THE DIGITAL MILLENNIUM COPYRIGHT ACT

Jonathan Band
Taro Isshiki
Anthony Reese
Morrision & Foerster LLP
Washington, D.C.
jband@mofo.com

On October 12, 1998, Congress passed the Digital Millennium Copyright Act (DMCA), a complex piece of legislation which makes major changes in U.S. copyright law to address the digitally networked environment. The President is expected to sign the DMCA shortly. This memorandum discusses the law's five titles which: (1) implement the WIPO Internet Treaties; (2) establish safe harbors for online service providers; (3) permit temporary copies of programs during the performance of computer maintenance; (4) make miscellaneous amendments to the Copyright Act, including amendments which facilitate Internet broadcasting; and (5) create *sui generis* protection for boat hull designs. A controversial title establishing database protection was omitted by the House-Senate Conference, as was a provision which would have reversed the Supreme Court's decision in *Quality King v. L'anza*, 118 S. Ct. 1125 (1998), which concerned parallel imports.

TITLE I: WIPO TREATIES IMPLEMENTATION

Title I of the DMCA amends U.S. copyright law to comply with the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty, adopted at the WIPO Diplomatic Conference in December 1996.

Two major provisions in the WIPO treaties require contracting parties to provide legal remedies against circumventing technological protection measures and tampering with copyright management information. To comply with these provisions, the DMCA adds a new chapter, Chapter 12, to Title 17 of the United States Code.

Circumvention of Copyright Protection Systems — New Section 1201

The DMCA prohibits gaining unauthorized access to a work by circumventing a technological protection measure put in place by the copyright owner where such protection measure otherwise effectively controls access to a copyrighted work.[1] This prohibition on unauthorized access takes effect two years after enactment on the DMCA. Over this two year period, the Librarian of Congress is to conduct a rulemaking proceeding to determine appropriate exceptions to the prohibition.[2]

---

[1] 17 U.S.C. § 1201(a)(1) (1998). To "circumvent a technological protection measure" means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate, or impair a technological protection measure." A technological protection measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or process or treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201(a)(3) (1998).

[2] The Library of Congress is required to conduct additional rulemakings every three years after this initial rulemaking.

To facilitate enforcement of the copyright owner's right to control access to his copyrighted work, the DMCA also prohibits manufacturing or making available technologies, products and services used to defeat technological measures controlling access.[3] Similarly, the DMCA prohibits the manufacture and distribution of the means of circumventing technological measures protecting the rights of a copyright owner, *e.g.*, measures which prevent reproduction. But to ensure that legitimate multipurpose devices can continue to be made and sold, the prohibition applies only to those devices that:

(1) are primarily designed or produced for the purpose of circumventing;

(2) have only a limited commercially significant purpose or use other than to circumvent; or

(3) are marketed for use in circumventing. *Id.*

Unlike the prohibition on acts of circumvention, which takes effect in two years, the prohibition on the manufacture and distribution of circumvention devices takes immediate effect.

The DMCA does not affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, nor does it alter the existing doctrines of vicarious and contributory liability.[4] However, a defense to copyright infringement is *not* a defense to the prohibition established in Chapter 12. The DMCA also does not require manufacturers of consumer electronics, telecommunications, and computing products to design their products to respond to any particular technological protection measure.[5] (However, as discussed below, manufacturers of certain analog recording devices will be required to respond to two known analog copy protection technologies.)

Congress recognized that there may be legitimate reasons for engaging in circumvention. In addition to the rulemaking noted above, Congress specifically provided for a number of exceptions to the prohibition on circumvention and circumvention devices.

Reverse Engineering Exception. Section 1201(f) allows software developers to circumvent technological protection measures of a lawfully obtained computer program in order to identify the elements necessary to achieve interoperability of an independently created computer program with other programs. A person may reverse engineer the lawfully acquired program only where the elements necessary to achieve interoperability are not readily available and reverse engineering is otherwise permitted under the copyright law.[6] Furthermore, a person may develop and employ technological means to circumvent and make available to others the information or means for the purpose of achieving interoperability.

---

[3] 17 U.S.C. § 1201(a)(2), (b) (1998).

[4] 17 U.S.C. § 1201(c)(1), (c)(2) (1998).

[5] 17 U.S.C. § 1201(c)(3) (1998).

[6] 17 U.S.C. § 1201(f) (1998).

EXCEPTIONS TO SECTION 1201

	1201(a) – Access Controls		1201(b) - Copy Controls
	Circumvention	Devices	Devices
Reverse Engineering	X	X	X
Encryption Research	X	X	
Security Testing	X	X	
Law Enforcement	X	X	X
Monitoring Children		X	
Privacy	X		
Libraries	X		
Rulemaking	X		

Exception for Law Enforcement and Intelligence Activities. The DMCA permits circumvention for any lawfully authorized investigative, protective, or intelligence activity by or at the direction of a federal, state, or local law enforcement agency, or of an intelligence agency of the United States.[7]

Encryption Research Exception. Recognizing the need to improve the ability of copyright owners to prevent the theft of their copyrighted works, Congress provided an encryption research exception intended to advance the state of knowledge in the field of encryption technology and to assist in the development of encryption products.[8] Circumvention in the course of a good faith encryption research may be allowed if the following conditions are met;

(1) the researcher lawfully obtained the copyrighted work;

(2) circumvention is necessary for the encryption research;

(3) the researcher made a good faith effort to obtain authorization from the copyright owner before the circumvention; and

(4) circumvention is otherwise permissible under the applicable laws.[9]

In addition to the above factors, the DMCA directs the court to consider three other factors:

[7] 17 U.S.C. § 1201(e) (1998).

[8] 17 U.S.C. § 1201(g) (1998).

[9] 17 U.S.C. § 1201(g)(2) (1998).

(1) whether the information derived from the research was disseminated to advance the knowledge or development of encryption technology or to facilitate infringement;

(2) whether the researcher is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology; and

(3) whether the researcher timely notifies the copyright owner with the findings and documentation of the research.[10]

Furthermore, a person may develop and employ or provide to his collaborator technological means to circumvent for the sole purpose of performing acts of good faith encryption research.

Security Testing Exception. In addition to the encryption research exception, the DMCA provides another exception for information security activities. The security testing exception permits circumvention conducted in the course of security testing if it is otherwise legal under applicable law.[11] Security testing is defined as obtaining access, with proper authorization, to a computer, computer system, or computer network for the sole purpose of testing, investigating or correcting a potential or actual security flaw, or vulnerability or processing problem.[12] In determining whether this exception is applicable, the DMCA requires the court to consider whether the information derived from the security testing was used solely to improve the security measures or whether it was used or maintained so as not to facilitate infringement.[13] The DMCA also permits the development, production or distribution of technological means for the sole purpose of performing permitted acts of security testing.[14]

Exception Regarding Minors. To alleviate concern that the DMCA might inadvertently make it unlawful for parents to protect their children from pornography and other harmful material available on the Internet, the DMCA permits the manufacture of a circumvention component whose sole purpose is to assist parents in preventing access of minors to objectionable material, provided that the component is included in a product which does not itself violate the provisions of Title I.

Protection of Personally Identifying Information. The DMCA addresses personal privacy concerns by permitting circumvention for the limited purpose of identifying and disabling as technological means such as a "cookie" which collects or

[10] 17 U.S.C. § 1201(g)(3) (1998).

[11] 17 U.S.C. § 1201(j) (1998).

[12] 17 U.S.C. § 1201(j)(1) (1998).

[13] 17 U.S.C. § 1201(j)(3) (1998).

[14] 17 U.S.C. § 1201(j)(4) (1998).

disseminates personally identifying information reflecting the online activities of the user.[15] This exception is only applicable if the user is not provided with adequate notice and the capability to prevent or restrict such collection or dissemination, and if the circumvention has no other effect on the ability of any person to gain access to any work. Interestingly, this provision permits acts of circumvention to protect privacy, but does not specifically permit the development and distribution of the means of effectuating that circumvention.

Exemption for Nonprofit Libraries, Archives, and Educational Institutions. The DMCA provides an exemption for nonprofit libraries, archives, and educational institutions to gain access to a commercially exploited copyrighted work solely to make a good faith determination of whether to acquire such work.[16] A qualifying institution may gain access only when it cannot obtain a copy of an identical work by other means and access may not last longer than necessary. Such an entity is not allowed to use this exemption for commercial advantage or financial gain. Here, too, the provision does not specifically permit the development and distribution of the devices necessary to effectuate the permitted circumvention.[17]

Certain Analog Devices and Certain Technological Measures. Title I contains a provision which specifically addresses the protection of analog television programming and prerecorded movies in relation to recording capabilities of ordinary consumer analog video cassette recorders. It requires analog video cassette recorders to conform to the two forms of copy control technology that are in wide use in the market today — the automatic gain control technology and the colorstripe copy control technology.[18] The provision prohibits tampering with these analog copy control technologies to render them ineffective by redesigning of video recorders or by intervention of "black box" devices or "software hacks."

As an essential element of this provision, Congress included specific encoding rules to preserve long-standing consumer home taping practices. Copyright owners may use these technologies to prevent the making of a viewable copy of a pay-per-view program or a prerecorded tape, for example, but cannot limit the copying of traditional over-the-air broadcasts or basic and extended tiers of programming services, whether provided through cable or other wireline, satellite, or future over-the-air terrestrial systems. In addition, copyright owners may only utilize these technologies to prevent the making of a 'second generation' copy of an original transmission provided through a pay-television service.

This provision becomes effective in eighteen months. Professional devices and Beta and 8mm VCRs, however, are exempt from its requirements.

---

[15] 17 U.S.C. § 1201(i) (1998).

[16] 17 U.S.C. § 1201(d) (1998).

[17] Section 402 of the DMCA, discussed below, also provides broadcasters with an exception to the circumvention prohibition when necessary to make permitted ephemeral reproductions.

[18] 17 U.S.C. § 1201(k) (1998).

Copyright Management Information — New Section 1202

The DMCA prohibits tampering with copyright management information (CMI). Specifically, the DMCA creates liability for any person who intentionally provides or distributes false CMI.[19] Also, the DMCA prohibits intentional removal or alteration of CMI, and knowing distribution of illegally modified CMI is similarly proscribed.[20] To be covered by the DMCA, CMI must be conveyed in connection with a copyrighted work and CMI may constitute any of the following:

(1) information that identifies the copyrighted work, including the title of a work, the author, and the copyright owner;

(2) information that identifies a performer whose performance is fixed in a work, with certain exceptions;

(3) in case of an audiovisual work, information that identifies the writer, performer, or director, with certain exceptions;

(4) terms and conditions for use of the work;

(5) identifying numbers or symbols that accompany the above information or links to such information, for example, embedded pointers and hypertext links; or

(6) other information as the Register of Copyrights may prescribe by regulation, with an exception to protect the privacy of users.[21]

Limitations on Liability. The DMCA recognizes special problems that certain broadcasting entities may have with transmission of CMI. Such entities include radio and television broadcasters, cable systems, and persons who provide programming to such broadcasters or systems. Those entities which do not intend to induce, enable, facilitate or conceal infringement may limit their liability in certain circumstances.[22]

In the case of an analog transmission, a transmitting entity will not be held liable for violating the DMCA if it is not "technically feasible" to avoid the violation or if avoiding the violation would "create an undue financial hardship."[23] In the case of an digital transmission, the DMCA contemplates voluntary digital transmission standards for the placement of CMI.[24] Different standards are likely to be set for the placement of CMI in different categories of works. If a digital transmission standard is set in a voluntary,

---

[19] 17 U.S.C. § 1202(a) (1998).

[20] 17 U.S.C. § 1202(b) (1998).

[21] 17 U.S.C. § 1202(c) (1998).

[22] 17 U.S.C. § 1202(e) (1998).

[23] 17 U.S.C. § 1202(e)(1) (1998).

[24] 17 U.S.C. § 1202(e)(2)(A) (1998).

consensus standard-setting process involving a representative cross-section of the relevant copyright owners and relevant transmitting industry, a transmitting entity will not be held liable for a third party's placement of CMI that deviates from the standard, provided that the entity does not intend to induce, enable, facilitate or conceal infringement. Until such a standard is set for a category of works, a transmitting entity will not be liable for violation only if the transmission of the CMI would: (1) cause a perceptible visual or aural degradation of the digital signal; or (2) conflict with an applicable government regulation or a certain, applicable industry-wide standard for the digital transmission.[25]

Civil Remedies and Criminal Penalties

The DMCA creates civil remedies and criminal penalties for violations of Sections 1201 or 1202. A civil action may be brought in a federal district court.[26] The court has broad powers to grant injunctions and award damages, costs and attorney's fees.[27] The court may also order the impounding, the remedial modification or the destruction of the devices or products involved in the violation. The court may punish repeat offenders by awarding treble damage awards.[28] Generally, it is up to the court to decide whether to reduce damage awards against innocent violators. But, in the case of nonprofit library, archives or educational institutions, the court must remit damages if it finds that a qualifying entity had no reason to know of the violation.[29]

The DMCA prescribes significant criminal penalties for willful violations committed for commercial advantage or private financial gain.[30] Criminal penalties are inapplicable to nonprofit libraries, archives, and educational institutions.[31]

Technical Amendments

Title I also contains a variety of technical amendments. It amends the federal copyright law to grant copyright protection to: (1) sound recordings that were first fixed in a treaty party (a country or intergovernmental organization other than the United States that is a party to specified international copyright and other agreements); and (2) pictorial, graphic, or sculptural works incorporated in a building or other structure or an architectural work embodied in a building located in the United States or a treaty party. The DMCA treats works published in the United States or a treaty party within 30 days after publication in a non-U.S., non-treaty party as first published in the United States or a treaty party for purposes of conferring protection.

---

[25] 17 U.S.C. § 1203(e)(2)(B) (1998).

[26] 17 U.S.C. § 1203(a) (1998).

[27] 17 U.S.C. § 1203(b) (1998).

[28] 17 U.S.C. § 1203(c)(4) (1998).

[29] 17 U.S.C. § 1203(c)(5) (1998).

[30] 17 U.S.C. § 1204(a) (1998).

[31] 17 U.S.C. § 1204(b) (1998).

Title I provides that no works other than sound recordings shall be eligible for protection solely by virtue of U.S. adherence to the Geneva Phonograms Convention or the WIPO Performances and Phonograms Treaty. It revises the definition of "eligible country," for purposes of provisions regarding copyright in restored works, to include nations other than the United States that: (1) become World Trade Organization member countries after the date of enactment of the Uruguay Round Agreements Act; (2) are or become nations adhering to the Berne Convention; (3) adhere to the WIPO Copyright or Performances and Phonograms Treaties; or (4) become subject to a certain presidential proclamation of copyright restoration after such enactment date. It includes sound recordings in the definition of "restored work" if the source country for the work is an eligible country solely by its adherence to the WIPO Performances and Phonograms Treaty.

TITLE II: ONLINE SERVICE PROVIDER LIABILITY

Title II of the Act limits an online service provider's ("OSP") liability for copyright infringement in several important situations. Because the term "service provider" is defined extremely broadly in some instances — "a provider of online services or network access, or the operator of facilities therefor"[32] — many entities which are not in the business of providing online services may nonetheless take advantage of Title II's protection.[33]

The exemptions from liability that the DMCA creates are additional to any defense that an OSP might have under copyright law or any other law.[34] In essence, the Act creates certain "safe harbors" for specified OSP activity. If an activity falls within the safe harbor, then the OSP qualifies for the exemption from liability; if the activity does not come within the safe harbor, then the questions of whether the activity in fact constitutes infringement and whether the OSP has any defense are to be decided under traditional copyright analysis. In addition, whether an OSP qualifies for any particular exemption is determined independently of whether the OSP qualifies for any other exemption.[35]

General Conditions for Eligibility

Termination Policy. To be eligible for any of the exemptions, an OSP must adopt, reasonably implement, and inform its subscribers and account holders (its "Users") of, a policy providing for termination of Users who are repeat infringers.[36]

---

[32] 17 U.S.C. § 512(k)(1) (1998).

[33] The House Judiciary Committee Report explains that the definition includes "services such as providing Internet access, e-mail, chat room and web page hosting…." Thus, a company which maintains an Intranet for its employees may be a service provider under the statute. Similarly, a company which maintains a bulletin board where customers can post comments concerning the company's products may qualify as a service provider.

[34] 17 U.S.C. § 512(l) (1998).

[35] 17 U.S.C. § 512(n) (1998).

[36] 17 U.S.C. § 1203(i)(1)(A) (1998).

Accommodation of Technical Measures. In addition, an OSP must accommodate and not interfere with "standard" technical measures used by copyright owners to identify and protect copyrighted works. Such technical measures might include, for example, digital watermarks or technological means for preventing copying of a work. In order to qualify as "standard", such a measure must have been developed by a broad consensus of copyright owners and OSPs in a fair multi-industry process, must be available to anyone on reasonable and nondiscriminatory terms, and must not impose substantial costs on OSPs or substantial burdens on OSP systems.[37]

No Need to Monitor or Access. The Act makes clear that in order to qualify for the exemptions, an OSP does *not* need to monitor its service or affirmatively seek out information about copyright infringement on its service (except as part of the standard technical measures discussed in the previous paragraph). In addition, the Act states that an OSP does not have to access, remove, or block material in order to qualify for its exemptions if such action is prohibited by law (such as, for example, the Electronic Communications Privacy Act).[38] At the same time, the Conference Report states that the legislation is not intended to discourage OSPs from voluntarily monitoring their sites, and that OSPs do not lose eligibility for the safe harbors by virtue of such monitoring.

Safe Harbors for System Storage and Information Locating Tools

The most straightforward exemptions in the Act cover two common OSP activities: (1) storing material (such as a Web page or chat room, for example) on an OSP's system at the request of a User and (2) referring Users to material at other online locations by means of, for example, a search engine, a list of recommended sites, or a hypertext link.[39]

The Act limits an OSPs liability for copyright infringement based on the material stored or referred to if the OSP meets certain conditions:

(1) the OSP doesn't actually know that the material is infringing;

(2) the OSP isn't aware of information from which the infringing nature of the material is apparent;

(3) if the OSP acquires such knowledge or awareness, the OSP acts expeditiously to remove or block access to the material;

(4) the OSP doesn't get a financial benefit directly attributable to the infringing material (for example, a special fee paid by each party that accesses the material) while having the right and ability to control the material; and

[37] 17 U.S.C. § 512(i)(2) (1998).

[38] 17 U.S.C. § 512(m) (1998).

[39] 17 U.S.C. § 512(c), (d) (1998).

(5) the OSP complies with the "notice and take down" provisions of the Act (discussed below).[40]

Safe Harbors for System Caching

A third safe harbor in the Act limits an OSP's liability for system caching, in which an OSP makes a temporary copy of popular Internet material requested by a User so that the OSP can deliver that copy to subsequent Users, which can be done more quickly and efficiently than obtaining the original material for each subsequent User.[41]

This exemption applies to material (a) that is originally placed online by someone other than the OSP (the "Originator") and (b) that is transmitted from the Originator, through the OSP's system, to a third party at that third party's request. To qualify for the exemption from liability for the intermediate and temporary storage of such material, the OSP must meet the following conditions:

(1) the OSP's storage of the cached material must be made through an automatic technical process and must be for the purpose of providing the material to subsequent Users who request the material;

(2) the OSP must transmit the cached material to subsequent Users without modifying its content;

(3) the OSP must comply with any rules on updating the cached material that are specified by the Originator using a generally accepted industry standard protocol, as long as such rules are not used by the Originator to prevent or unreasonably impair system caching;

(4) the OSP must not interfere with technology associated with the cached material that returns certain information to the Originator, as long as such technology doesn't significantly interfere with the performance of the OSP's system and is consistent with generally accepted industry standard protocols;

(5) if the Originator has placed conditions (such as payment of a fee or entry of a password) on access to the cached material, the OSP must allow access to the cached material only to subsequent Users that have met such conditions; and

(6) if the original material from which the cached copy was made has been removed or blocked and a copyright owner provides notice to the OSP (pursuant to certain "notice and take-down" provisions discussed below), the OSP must act expeditiously to remove or block access to the cached material that the copyright owner alleges is infringing.[42]

---

[40] 17 U.S.C. § 512(c)(1), (d) (1998). The Committee Reports contain examples of what constitutes actual knowledge or awareness of circumstances from which infringing activity is apparent.

[41] 17 U.S.C. § 512(b) (1998).

[42] 17 U.S.C. § 512(b) (1998).

Safe Harbors for Transmission and Routing

A final safe harbor in the Act covers an OSP's transmission, routing, or providing connections for material through the OSP's system and for intermediate and transient storage of material in the course of such activity. In essence, this safe harbor covers an OSP's activities in acting as a conduit for material travelling between other parties.

To qualify for this exemption, several conditions must be met:

(1) the transmission of the material must have been initiated or directed by someone other than the OSP;

(2) the activities covered by the exemption must be carried out through an automatic technical process and not by any selection of material by the OSP;

(3) the OSP must not select the recipients of the material except as an automatic response to another person's request;

(4) the OSP must not make any copy of the material ordinarily accessible to anyone other than intended recipients and must not keep any copy for longer than reasonably necessary for the OSP's transmission, routing, or connection; and

(5) the OSP must not modify the content of the material as it transmits it through its system.[43]

Extent of Exemptions from Liability

The safe harbors of the Act provide somewhat different limitations on different types of remedies usually available for copyright infringement.

Monetary Relief. If an OSP's activity qualifies for any of the safe harbors in the Act, then the OSP is not liable for any monetary relief for claims of copyright infringement based on that activity. Monetary relief includes damages, court costs, attorney's fees, and any other form of monetary payment.

Injunctions. If an OSP qualifies for a safe harbor under the Act, then the possible injunctive relief against the OSP is limited. Under any safe harbor, a court may issue an injunction restraining an OSP from providing access to an identified User engaging in infringement by terminating the User's specified accounts. With respect to the safe harbors for system caching, system storage, and information location tools, a court can also issue an injunction restraining an OSP from providing access to infringing material residing at a particular online site on the OSP's system. Any other injunctive relief must be necessary to prevent infringement of specified material at a particular online location and must be the least burdensome to the OSP among comparably effective forms of relief. With respect to transmission and routing, a court can also issue an injunction ordering an OSP to take specific reasonable steps to block access to an identified online location outside the U.S.[44]

[43] 17 U.S.C. § 512(a) (1998).

The Act also sets forth several additional considerations, including the burden on an OSP's system, the technical feasibility, and the interference with noninfringing material, that a court must consider in the case of all the safe harbors in deciding whether to grant injunctive relief. The DMCA further limits the liability of nonprofit institutions of higher education that act as OSPs for the infringing acts of their faculty and graduate students when performing teaching or research functions.

Notice and Take-Down Provisions

Certain of the Act's exemptions apply only if an OSP complies with the notice and take-down provisions of the Act. These provisions allow copyright owners to notify an OSP of allegedly infringing material on the OSP's system and require the OSP to remove or block access to such material after receiving such notice.

Designated Agent of OSP. An OSP must designate, both to the Copyright Office and on its service, the contact information for an agent that will receive such notices.[45]

Form and Content of Notice. A notice from a copyright owner must be in writing and must be signed by such copyright owner or his or her agent and must include certain specified information, including an identification of the allegedly infringing material and information reasonably sufficient for the OSP to locate the material or the reference or link to it.[46] If the OSP receives a notice that substantially complies with the Act's requirements, then the OSP must act expeditiously to remove or block access to the material that is alleged to be infringing in order to remain eligible for the exemption from liability.

Misrepresentations. The Act provides that anyone who knowingly materially misrepresents under the Act that material is infringing is liable for any damages incurred by an OSP or a User as a result of the OSP relying on such misrepresentation in removing or blocking material.[47]

Subpoenas. The Act also provides a procedure by which a copyright owner can obtain from a court a subpoena directing an OSP to disclose to the copyright owner information sufficient to identify an alleged infringer of material as to which the owner has sent a notice to the OSP.[48]

"Take Down" Procedures

Exemption from Liability. If an OSP in good faith removes or blocks access to material that it has cached, stored at a User's request, or referred users to, either because the OSP has received notice from a copyright owner or because the OSP has become aware of

[44] 17 U.S.C. § 512(j) (1998).

[45] 17 U.S.C. § 512(c)(2) (1998).

[46] 17 U.S.C. § 512(c)(3) (1998).

[47] 17 U.S.C. § 512(f) (1998).

[48] 17 U.S.C. § 512(h) (1998).

information from which the infringing nature of the material is apparent, the Act exempts the OSP from any liability for such removal or blocking.[49]

Notice and Putback. In the case where an OSP removes or blocks material stored on the OSP's system at the User's request (such as the User's Web site) because the OSP has received a notice from a copyright owner alleging infringement, the OSP must take additional steps designed to protect the User's rights, and which may lead to putting the material back on the system.

(1) The OSP must take reasonable steps to promptly notify the User that the OSP has removed or blocked the material.

(2) The User may then send a "counter notification" to the OSP stating that the removal or blocking was a result of a mistake or a misidentification of the material. (The Act provides for liability to the OSP and the copyright owner for knowing material misrepresentation in such counter notification.[50])

(3) If the counter notification complies with the statutory requirements, then the OSP, to remain exempt from liability for the "take down", must provide a copy of the counter notification to the copyright owner that sent the original notice.

(4) Unless such copyright owner then notifies the OSP that the owner has filed a court action seeking to restrain the alleged infringement, the OSP must replace or unblock the material within 10 to 14 business days of receiving the counter notification.[51]

TITLE III: COMPUTER MAINTENANCE OR REPAIR COPYRIGHT EXEMPTION

Title III amends Section 117 of the Copyright Act to ensure that independent service organizations do not inadvertently become liable for copyright infringement merely because they have turned on a computer in order to service its hardware components.

Title III was proposed in response to the decision in *MAI Systems Corp. v. Peak Computer, Inc*.[52] *MAI* involved the limitation on the exclusive rights in computer programs contained in 17 U.S.C. § 117, which allows the "owner" of a program to load the program into the machine's random access memory, or "RAM." In *MAI*, an independent service organization (ISO) serviced a computer which used software licensed to, but not owned by, the customer. The court held that the ISO infringed the copyright in the program by loading the copyrighted software into the RAM of the customer's computer, thereby making a "reproduction" of the copy under 17 U.S.C. § 106. The *MAI* court ruled that Section 117

[49] 17 U.S.C. § 512(g) (1998).

[50] 17 U.S.C. § 512(f) (1998).

[51] 17 U.S.C. § 512(g)(2) (1998).

[52] 991 F.2d 511 (9th Cir. 1993).

only exempted "owners" of software and not "licensees." Title III amends Section 117 to effectively overrule *MAI* by allowing the owner or lessee of a machine to make or authorize the making of a copy of a computer program under certain conditions for the purpose of repair or maintenance of the computer hardware.

Specifically, the making of the copy is allowed (1) if the copy is made "solely by virtue of the activation of a machine that lawfully contains an authorized copy of the computer program, for purposes only of maintenance or repair of that machine," (2) if the new copy is used for no other purpose and is destroyed upon completion of the maintenance or repair, and (3) if "any computer program … that is not necessary for that machine to be activated … is not accessed or used other than to make such new copy by virtue of the activation of the machine." Significantly, the exception applies only to RAM copies made during the course of hardware maintenance, *not* software maintenance.

TITLE IV: MISCELLANEOUS PROVISIONS

Title IV of the DMCA contains miscellaneous amendments to the Copyright Act.

Provisions Relating to the Register of Copyrights. Section 401 of the DMCA provides parity in compensation between the Register of Copyrights and the Commissioner of Patent and Trademarks and clarifies the duties and functions of the Register of Copyrights.

Ephemeral Recordings. Section 402 of the DMCA amends section 112 of Title 17 to address two issues concerning the application of the ephemeral recording exemption in the digital age. The first issue is the relationship between the ephemeral recording exemption and the Digital Performance Right in Sound Recordings Act of 1995 ("DPRSRA"). Section 402 changes the existing language of the ephemeral recording exemption (redesignated as 112(a)(1)) to extend explicitly to broadcasters the same privilege with respect to digital broadcasts that they already enjoy with respect to analog broadcasts.

The second issue is the relationship between the ephemeral recording exemption and the anticircumvention provisions in the new section 1201 of the Copyright Act. Section 402 addresses the concerns that if use of copy protection technologies became widespread, a transmitting organization might be prevented from engaging in its traditional activities of assembling transmission programs and making ephemeral recordings permitted by section 112. Section 402 adds to section 112 a new paragraph that permits transmitting organizations to engage in activities that otherwise would violate section 1201(a)(1) in certain limited circumstances when necessary for the exercise of the transmitting organization's privilege to make ephemeral recordings.

Distance Education Study. Section 403 of the DMCA directs the Register of Copyright to consult with representatives of copyright owners, nonprofit educational institutions, and nonprofit libraries and archives and to submit to the Congress within six months recommendations on how to promote "distance education" through digital technologies.

Exemption for Libraries and Archives. Section 404 of the DMCA updates section 108 of the Copyright Act to allow libraries and archives to take advantage of digital technologies when engaging in specified preservation activities. The amendment to subsection 108(a)(3) is intended to ease the burden on libraries and archives of the current law's requirement that a notice of copyright be included on copies that are reproduced under section 108. Under this amendment, such notice would be required only where the particular copy that is reproduced by the library or archive itself bears a notice. The amendment to subsection 108(b) permits a library or archive to make up to three copies or phonorecords, rather than just one, for purposes of preservation and security or for deposit for research use in another library or archives, and permits such copies or phonorecords to be made in digital as well as analog formats. The amendment provides that any such copy in a digital format must not be otherwise distributed in that format and must not be available to the public outside the premises of the library or archives.

Scope of Exclusive Rights in Sound Recordings; Ephemeral Recordings. Section 405 of the DMCA contains various amendments to sections 112 and 114 of the Copyright Act. The amendments are aimed at achieving two purposes: first, to further a stated objective of Congress when it passed the DPRSRA to ensure that recording artists and record companies will be protected as new technologies affect the ways in which their creative works are used; and second, to create fair and efficient licensing mechanisms that address the complex issues facing copyright owners and copyright users as a result of the rapid growth of digital audio services. This amendment accomplishes both of these objectives by creating two statutory licenses for certain performances and reproductions of sound recordings in the digital environment.

Section 405 amends section 114 by creating a statutory license for certain nonsubscription and new subscription transmissions. Subscription transmissions by services providing service to customers on July 31, 1998, remain subject to the statutory license created by the DPRSRA, with certain exceptions. Section 405 also amends section 114 to clarify that certain types of programming practices should be considered interactive and therefore subject to a sound recording copyright owner's exclusive rights.

Section 405 also amends section 112 by offering a statutory license for certain types of reproductions made to facilitate transmissions subject to the statutory licenses in section 114 or which qualify for certain exemptions from a sound recording copyright owner's performance right. Section 112 refers to such reproductions as "ephemeral recordings." The statutory license created by section 112(f) facilitates the licensing that is necessary for the making of ephemeral recordings by Internet music services.

TITLE V: PROTECTION OF CERTAIN ORIGINAL DESIGNS

Title V of the DMCA, referred to as "Vessel Hull Design Protection Act," provides new *sui generis* protection for original boat hull designs for a 10-year term by adding a new chapter, Chapter 13, to Title 17 of the United States Code.

In *Bonito Boats Inc. v. Thunder Craft Boats, Inc.*,[53] the Supreme Court struck down, as preempted by federal patent law, a Florida statute that had protected the design of boat hulls against copying by means of making a mold from the finished hull. Title V was proposed to address the concerns raised by boat manufacturers and design firms in the wake of that decision.

An application for registration of the design would be a prerequisite to protection, and such application would have to be made within two years of the date the design was first made public.[54] The owner of a registered design would have the exclusive right to make, sell, import or distribute for sale or for commercial use any hull embodying the design.[55] The DMCA would, however, exempt from liability for infringement certain actions, including reproducing a protected design "solely for the purpose of teaching, analyzing, or evaluating the appearance, concepts, or techniques embodied in the design, or the function of the useful article embodying the design."[56] In addition, a distributor who sold a vessel hull embodying a protected design would not be liable if the distributor did not know the design was protected and copied.[57] Also, as with copyright, no liability would attach if the allegedly infringing hull was designed independently — *i.e.*, without copying the first hull. Further, whenever any vessel hull embodying a protected design was publicly exhibited or distributed, the hull would have to carry a notice of the design's protection, and omission of the notice would prevent the owner from recovering against a party who infringes before receiving notice of the protection.[58]

[53] 489 U.S. 141 (1989).

[54] 17 U.S.C. § 1310 (1998).

[55] 17 U.S.C. § 1308 (1998).

[56] 17 U.S.C. § 1309(g) (1998).

[57] 17 U.S.C. § 1309(b) (1998).

[58] 17 U.S.C. § 1306, 1307 (1998).