Chicago-Kent Journal of Intellectual Property

Volume 3 | Issue 2 Article 3

4-1-2004

The Digital Millenium Copyright Act: Provisions on Circumventing Protection Systems and Limiting Liability of Service Providers

Francisco Castro

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/ckjip

 Part of the Intellectual Property Law Commons

Recommended Citation

Francisco Castro, *The Digital Millenium Copyright Act: Provisions on Circumventing Protection Systems and Limiting Liability of Service Providers*, 3 Chi. -Kent J. Intell. Prop. (2004).
Available at: https://scholarship.kentlaw.iit.edu/ckjip/vol3/iss2/3

This Article is brought to you for free and open access by Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in Chicago-Kent Journal of Intellectual Property by an authorized editor of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact jwenger@kentlaw.iit.edu, ebarney@kentlaw.iit.edu.

Copyright © Chicago-Kent Journal of Intellectual Property

THE DIGITAL MILLENNIUM COPYRIGHT ACT: PROVISIONS ON CIRCUMVENTING PROTECTION SYSTEMS AND LIMITING LIABILITY OF SERVICE PROVIDERS

Francisco Castro

The World Intellectual Property Organization (WIPO) held a Diplomatic Conference on Certain Copyright and Neighboring Right Questions in Geneva, Switzerland, on December 1996. The goal of the meeting was to develop the appropriate international response to the challenges placed on intellectual property protection by the rapid technological advances of the digital age. At the end of the month-long negotiations, two separate treaties were adopted: the Copyright Treaty ("Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works") and the Performances and Phonographs Treaty ("Treaty for the Protection of the Rights of Performers and Producers of Phonographs"). Both treaties contained obligations concerning technological measures, rights management information and provisions on enforcement of rights.

Less than two years later, on October 28, 1998, Congress passed the Digital Millennium Copyright Act (DMCA). This comprehensive piece of legislation was intended to implement the WIPO treaties and to respond to a variety of pressing copyright issues affecting the entertainment industry, especially the increased ease of music and video piracy on the Internet. Omitted from legislative piece during the House-Senate Conference was a controversial title establishing protection for databases and a provision concerned with the unauthorized importation and resale of copyrighted material. In its final form, the DMCA comprised five different titles: (1) the "WIPO Copyright and Performances and Phonographs Treaties Implementation Act of 1998"; (2) the "Online Copyright Infringement Liability Limitation Act"; (3) the "Computer Maintenance Competition Assurance Act"; (4) a series of miscellaneous amendments to the Copyright Act of 1976, including amendments which facilitate Internet broadcasting; and (5) the "Vessel Hull Design Protection Act."

Among the vast number of issues addressed by the DMCA, two key sets of provisions have particular importance in the protection and access to artistic material on the Internet: the prohibition of unauthorized access to copyrighted works by technologies that circumvent protection systems and the limitation of copyright infringement liability of online service providers.

I. CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS

The main purpose of Title I of the DMCA is to amend U.S. copyright law to comply with the Copyright Treaty and the Performances and Phonographs Treaty adopted by WIPO in 1996. The WIPO provisions relating to access controls to copyrighted material as implemented in 17 U.S.C. §1201 do not alter U.S. law but instead are intended to supplement the rights of copyright owners by imposing further limitations on how users can obtain copyrighted material. Under the DMCA, protection is given to

technological measures used to limit access of copyrighted works by prohibiting the use and distribution of techniques, tools, or devices that can circumvent security controls in order to gain access to copyrighted material. It is a federal offense to bypass security measures even when done as a part of a research project or in order to use copyrighted work in a manner permitted by law.

Enforcement of the DMCA provisions relating to access controls has already been tested. In 2001, Dmitry Sklyarov, a Russian doctoral candidate who came to the United States to present his dissertation in encryption research at an international conference was arrested for sharing his work to conference participants.[1] Although the charges were eventually dropped and he was able to return to Russia, the incident confirmed concerns held by critics that certain aspects of the DMCA are unfair. However, while there may be concerns with the enforcement of the law, the DMCA does allow for various activities, including encryption research, to be performed without violation of the statute.

The following paragraphs provide a brief summary of the most important prohibitions, rights, limitations, defenses, and exemptions described in Section 1201.

A. Prohibition of Technologies to Circumvent Access Controls

The basic prohibition of circumvention states that no person shall circumvent a technological measure that effectively controls access to copyrighted material. The law does not impose any standards or requirements on the manner or purpose of technical measures used to control access.[2]

B. Prohibition of Use or Distribution of Technologies to Circumvent Access Controls

The manufacture, import, or traffic of any technology, service, or device for the purpose of circumventing access controls to copyrighted works is prohibited. This provision limits access to permitted copyrighted material if a device is needed to get around access controls.[3]

C. Prohibition of Use or Distribution of Technologies to Circumvent Protection of Copyrighted Works

There are additional prohibitions on the use or distribution of technologies, products, services, or devices primarily intended to circumvent measures that protect the rights of a copyright owner. This section pertains to the copyrighted works or materials themselves rather than access controls.[4]

---

[1] L. Frederick, *Criminalizing Decryption in the United States: The Digital Millennium Copyright Act*, E-COMMERCE L. REP., vol. 4, no. 11, 13-16 (2002).

[2] 17 U.S.C. §1201(a)(1)(A).

[3] 17 U.S.C. §1201(a)(2).

[4] 17 U.S.C. §1201(b).

D. Rights, Limitations, and Defenses

Rights, remedies, limitations, or defenses to copyright infringement are not affected by these provisions. Because copyright violations and circumvention violations are distinct and separate offenses, defenses to copyright violations do not serve as defenses to violations of Section 1201.[5]

E. Recognized Exemptions

Congress provided for a number of exceptions since it recognized that there are several legitimate reasons for circumventing technical measures used to control access to copyrighted works.

> *(a) Nonprofit Libraries, Archives, and Educational Institutions.* Nonprofit libraries, archives, or educational institutions are allowed to gain access to a commercially exploited copyrighted work to decide whether to purchase it for a legal purpose. This exception is only available when a copy of an identical work cannot be obtained by other means and does not preclude restrictions to circumventing access controls previously discussed. In order libraries or archives to qualify for this exemption, their collections must be available to the public and also to persons doing research in the field covered by the protected work.[6]
>
> *(b) Law Enforcement and Intelligence Activities.* Agents or employees at the local, state, or federal level are not prohibited from carrying out lawfully authorized investigative, information security or intelligence activity. By "information security" is meant any activities carried out to identify vulnerabilities of government computer systems.[7]
>
> *(c) Reverse Engineering.* Software developers are granted the limited ability to reverse engineer a lawfully obtained copy of a computer program in order to identify elements necessary to achieve interoperability of an independent computer program. This is possible only if the interoperability elements are not readily available to the person engaging in the circumvention.[8]
>
> *(d) Encryption Research.* An exception for activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies is provided in order to advance the state of knowledge in the field and to assist in the development of encryption products. Circumvention is permitted if the copyrighted work was lawfully obtained, circumvention was necessary for encryption research, the researcher made a good faith effort to obtain authorization prior to the circumvention, and circumvention does not constitute infringement violation of applicable law. Other factors to consider in support of the exemption are: whether

[5] 17 U.S.C. §1201(c).
[6] 17 U.S.C. §1201(d).
[7] 17 U.S.C. §1201(e).
[8] 17 U.S.C. §1201(f).

results from the research effort were disseminated to advance the development of encryption technology; whether the researcher is appropriately trained or experienced in encryption technology; and whether researcher notifies the copyright owner of the findings of the research.[9]

(e) Exception Regarding Minors. Parents would not be in violation of the DMCA when attempting to protect their children from harmful material on the Internet. This section permits a component or part to be incorporated in a technology, product, service or device which has the sole purpose to prevent the access of minors to material on the Internet.[10]

(f) Security Testing. Accessing a computer, computer system, or computer network, is allowed solely for the purpose of good faith testing of security flaws and vulnerabilities with the authorization of the owner or operator. Factors in determining whether a person qualifies for this exemption are: whether the information derived from the security testing was used solely to improve the security of the owner or operator or shared directly with the developer of the computer, computer system, or computer network; and whether the information derived was used or maintained in a fashion that does not constitute infringement. This section also permits the development, production, distribution, and usage of technological means for the sole purpose of security testing. [11]

*(g) Certain Analog Devices and Certain Technological Measures***.** The protection of prerecorded movies and analog television programming as it relates to consumer analog video cassette recorders is addressed. This provision prohibits tampering with analog copy control technologies and requires manufacturers to conform to either the automatic gain control or the four-line colorstripe copy control technologies.[12]

II. LIMITATIONS ON LIABILITY RELATING TO ONLINE MATERIALS

Title II of the DMCA limits monetary liability of online service providers (OSPs) for copyright infringement in the event that others place infringing material on web sites hosted by the OSP or in the case that the OSP provides a link or networking connection to a web site containing infringing material. These new provisions were implemented in 17 U.S.C. §512 and provide legal protection to an OSP as long as it follows certain guidelines. These guidelines define various "safe harbors" or exemptions based upon the type of OSP activity. The exemptions offered by the DMCA are in addition to any defense that an OSP might have under copyright law or any other applicable law.

In *Hendrickson v. eBay, Inc.*, a movie owner had brought a copyright infringement case against eBay because it had listed offers to sell allegedly infringing

[9] 17 U.S.C. §1201(g).
[10] 17 U.S.C. §1201(h).
[11] 17 U.S.C. §1201(j).
[12] 17 U.S.C. §1201(k).

copies of the movie.[13] In its defense, eBay was able to gain protection under one of the limited liability provisions or "safe harbors" provided by Section 512 of the DMCA. However, in order to gain this protection, eBay had to meet a series of very strict requirements and definitions set forth by Section 512.

The following paragraphs provide a brief summary of the requirements for eligibility, definitions of a service provider, safe harbor requirements, and limitations described in Section 1201:

A. Requirements for Eligibility

The OSP must establish several requirements in order to qualify for the exemptions provided by the DMCA.

> *(a) Termination Policy*. An OSP must adopt, reasonably implement, and inform its subscribers and account holders of the service provider's system or network of, a policy that provides for the termination of those who are repeat infringers.[14]
>
> *(b) Accommodation of Technical Measures*. An OSP cannot interfere with standard technical measures. "Standard technical measures" is defined in Section 512(i)(2) as measures used by copyright owners to protect and identify copyrighted works. These technical measures do not impose a substantial cost or burden on the OSP and have developed from a broad consensus in an open, fair, and voluntary industry standard process.[15]
>
> *(c) Monitoring or Access*. For an OSP to qualify for the exemptions offered by the DMCA, it is not required to monitor its service or affirmatively search for facts that show infringing activity. Moreover, the OSP does not have to gain access, remove, or disable access to material in cases where such actions are prohibited by law.[16]

B. Definition of Service Provider

Where the OSP acts as a transitory digital network, a "Service Provider" is defined as an entity offering the transmission, routing, or providing connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received. For any other cases, "Service Provider" is defined as a provider of online services or network access, or the operator of facilities therefor.[17]

---

[13] 165 F. Supp. 2d 1082 (C.D. Cal. 2001)
[14] 17 U.S.C. §512 (i)(1)(A).
[15] 17 U.S.C. §512(i)(1)(B).
[16] 17 U.S.C. §512(m).
[17] 17 U.S.C. §512(k).

Copyright © Chicago-Kent Journal of Intellectual Property

C. Safe Harbor When OSP Acts as a Transitory Digital Network

An OSP is not liable for monetary relief, and is only subject to limited injunctive or equitable relief, for transmitting, routing, or providing connections for material through a system or network controlled or operated by the OSP, or for the intermediate and transitory storage of that material in the course of thereof.[18] The OSP qualifies for this exemption if the following conditions are met:

> (i) the transmission of material was initiated by or at the direction of a person other than the OSP;
>
> (ii) the activities covered by the exception are carried out through an automatic technical process without the OSP selecting the material;
>
> (iii) the OSP does not select the recipients of the material except as an automatic response to another person's request;
>
> (iv) no copy of the material made by the OSP in the course of intermediate or transitory storage is maintained on the system in a manner ordinarily accessible to anyone other than the recipient and is not maintained for a period longer than necessary for transmission, routing, or to provide connection; and
>
> (v) material content is not modified in the course of transmission through the system or network.

D. Safe Harbor When OSP Temporarily Stores Material

An OSP is not liable for monetary relief, and is subject only to injunctive or equitable relief, for infringement of copyright by reason of intermediate or temporary storage ("system caching") of material on a system or network controlled or operated by an OSP in a case where the material was made available online by a person other than the OSP. The storage is carried out through an automatic technical process for the purpose of making the material available by the originator to another person.[19] To qualify for this safe harbor the OSP must:

> (i) not modify the content of the cached material;
>
> (ii) comply with all rules concerning the refreshing, reloading, or other updating of the material in accordance with accepted industry standard data communication protocols, provided that the such rules are not used by the originator to prevent or unreasonably impair the system caching;
>
> (iii) not interfere with any technology associated with the material that returns information to the originator that would have been obtained by subsequent users

[18] 17 U.S.C. §512(a).
[19] 17 U.S.C. §512(b).

directly from that person;

(iv) if the originator has placed conditions, such as payment of a fee or entry of a password, that a person must meet to have access to the material, the OSP provides access to those who have met those conditions; and

(v) the OSP responds expeditiously to remove or disable access to any unauthorized material in intermediate or temporary storage upon notification that such material has been removed or disabled from the originating site by a copyright owner alleging infringement.

E. Safe Harbor When Information Resides on System at Direction of Users

An OSP is not liable for monetary relief, and it is subject to only injunctive or equitable relief, for infringing by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by the OSP.[20] To qualify for this exemption the OSP must:

(i) not have knowledge that the material is infringing;

(ii) not be aware of facts or circumstances from which infringing activity is apparent;

(iii) upon obtaining knowledge or awareness, acts expeditiously to remove or disable access to the material; and

(iv) does not receive financial benefit directly attributable to any infringing activity, if it has the right and ability to control such activity.

Under Section 512(c)(2), the limitation on liability established by this safe harbor applies only if the OSP has designated an agent to receive notifications of claimed infringement. The OSP must make this agent available through its service, including on its website in a location accessible to the public, and by providing the Copyright Office with the person's name, address, phone number, electronic mail address, and any other contact information that the Register of Copyrights may deem appropriate.

Elements of proper notification of infringement are specified in Section 5129(c)(3) and include identification of the copyrighted work, identification of the infringing material in sufficient detail to allow the OSP to locate it, complaining party contact information, a statement signed electronically or physically by the complaining party which shows it has the authority to enforce the rights that are claimed to be infringed, and a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. If a notice complies with at least the first three elements of proper notification, the OSP is required to promptly contact the complaining party in order to take advantage of the safe harbor provisions of

[20] 17 U.S.C. §512(c)(1).

the DMCA.

F. Safe Harbor When OSP Provides Information Location Tools

The final safe harbor states that an OSP is not liable for monetary relief, and it is subject to only injunctive or equitable relief, for infringement by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link. This exemption is available to an OSP if it meets similar requirements to those needed when establishing a safe harbor for the case when information resides on the OSP at the direction of users.[21]

G. Limitation on Liability of Nonprofit Educational Institutions

Section 512(e) contains an additional liability limitation for public or other institutions of higher education that act as an OSP. This Section provides that online infringement activities by faculty members or graduate students that take place when performing teaching or research functions will not be attributed to the institution if:

> (i) the infringing activities do not involve the provision of online access to instructional material that are or were required or recommended within the preceding three-year period, for a course taught at the institution by a faculty member or graduate student;
>
> (ii) the institution has not, within the three-year period, received more than two notifications of claimed infringement by such faculty member or graduate student; and
>
> (iii) the institution provides all users of its system with informational materials that accurately describe and promote compliance with, the laws of the United States relating to copyright.

III. CONCLUSION

Courts and law enforcement agencies have just begun to face and enforce the provisions of the DMCA, for that reason, it is important that individuals, companies and nonprofit organizations working with copyright protection technologies or hosting third-party content become aware of the prohibitions and safe harbors granted by the DMCA under Section 512 and Section 1201. While the DMCA allows for a great number of exemptions and limitations to those activities, there are still many critics in the international and technological communities, and in free speech advocates, who believe that the benefits awarded by the DMCA are overshadowed by the restraints it enforces.

[21] 17 U.S.C. §512(d).