E

WIPO/CR/RIO/01/5
ORIGINAL: English
DATE: September 3, 2001

COORDENAÇÃO DE DIREITO AUTORAL
MINISTÉRIO DA CULTURA

WORLD INTELLECTUAL
PROPERTY ORGANIZATION


ASSOCIACÃO BRASILEIRA DOS
PRODUTÓRES DE DISCOS

# NATIONAL SEMINAR ON THE WIPO INTERNET TREATIES AND THE DIGITAL TECHNOLOGY

organized by
the World Intellectual Property Organization (WIPO)

and
the Copyright Coordination of the Ministry of Culture of Brazil

with the support of
the Brazilian Recording Industry Association

**Rio de Janeiro (Brazil), September 17 to 19, 2001**

PART I: TECHNOLOGICAL MEASURES FOR PROTECTION OF COPYRIGHT AND RELATED RIGHTS ON THE INTERNET–PRESENT AND FUTURE TECHNOLOGIES
PART II: ENFORCEMENT OF COPYRIGHT AND RELATED RIGHTS IN DIGITAL NETWORKS, THE TECHNOLOGY AND ITS POSSIBILITIES FOR INFRINGEMENT AND SURVEILLANCE. THE ENFORCEMENT RULES UNDER THE WCT AND THE WPPT

*Paper prepared by*
*Mr. Michael Keplinger*
*Office of Legislative and International Affairs*
*United States Patent and Trademark Office*
*Washington D.C.*

Overview

1. The development of globe-spanning communications networks with their potential for electronic commerce requires us to reflect and plan if we are to avoid major impediments in the 21st century. Every six seconds, somewhere on the planet, another person logs onto the Internet for the first time. For many of you in this room, the Internet is already a tool of your daily life – e-mails that connect you to friends and colleagues in different countries, the World Wide Web which gives you instantaneous information about everything from the current political scene to access to on-line music.

2. For the intellectual property community–for artists, publishers, filmmakers, musicians, and software producers–the technological developments of the past decade have opened up a whole new world of economic opportunities – *and a whole new world of challenges and potential problems.* But I think that in some quarters, there is a perception that these changes, opportunities, and challenges are occurring far away and that they do not have much impact on developing countries with rapidly developing economies such as Brazil. Indeed, these new technologies may exacerbate the view of some that intellectual property rights only benefit developed countries, that intellectual property is not important to emerging economies,[1] and that international intellectual property norms involve some kind of North/South struggle.[2]

3. For example, a recent World Bank seminar on Brazil's science and technology sector considered that while Brazil has the largest science and technology sector in Latin America, its science agencies need to shift their emphasis "toward the encouragement of the productive use of scientific output." This World Bank conference also concluded that "strong respect for patents and intellectual property" is needed to "permit diffusion of knowledge, while protecting knowledge producers' rights."[3]

4. Again and again, the economic evidence shows that intellectual property protection promotes local innovation. For example, a 1986 study of the farm machinery industry in Brazil demonstrated that protection of utility models was instrumental in allowing local Brazilian producers to win away from foreign producers a dominant share of the work in adapting farm machinery to local conditions.[4] Another study has demonstrated econometrically that Japan's utility patent system contributed positively and significantly to the building of its post-war industries through local inventions.[5]

---

1 For example, C. Niranjan Rao of the Indian Council for Research on International Economic Relations, New Delhi, spoke of the view that the developing world is "overwhelmed by foreign patents" and copyrights on April 28, 1998, participating in the World Bank's IPRSTEAM Think Tank. www.vita.org/technet/iprs/iprsarch/0006.html.

2 *See* Michael P. Ryan, *Knowledge Diplomacy: Global Competition and the Politics of Intellectual Property* (1998) 91-124 (discussing the TRIPS negotiations and the initial opposition of the "Group of Ten" to the inclusion of intellectual property in the WTO negotiations).

3 Lauritz Holm-Nielsen, Michael Crawford, and Alcyone Saliba, *Institutional and Entrepreneurial Leadership in the Brazilian Science and Technology Sector: Setting a New Agenda*, World Bank Discussion Papers No. 325, pp. 16-17, The World Bank (1996)

4 S. Dahab, *Technological Change in the Brazilian Agricultural Implements Industry* (unpublished PhD dissertation, Yale University, 1986).

5 Keith E. Maskus and Christine McDaniel, *The Impact of the Japanese Patent System on Post-War Productivity Growth*, JAPAN AND THE WORLD ECONOMY, Vol.11, No. 4, (November 1999) 557-574.

5. The second point I wanted to mention on the issue of technology transfer is how the international intellectual property system can help developing countries gain technical know-how in the digital era. WIPO has an ambitious project to "wire the world," that is, to connect patent offices around the globe so that they can share data and information. It's only a small step from that information reaching a country's intellectual property office to that information being more widely diffused to the engineers and technologists of a developing economy.

6. Similarly, since March 1999, the USPTO's website–www.uspto.gov–has been offering the full text of all patents issues in our country since 1976 along with full-page patent images –drawings and schematics–to complement the patent text database. The patent images are a massive file. Indeed, all totaled, in the first half of 1999 our office put on the Internet a 2 tera-byte database system of *21 million* documents–roughly the size of 1 and 1/4 million copies of *Dona Flor and Her Two Husbands*. This means that enormous amounts of highly detailed technological information is now available to any Brazilian engineer, scientist or researcher who has a computer, a modem, and a reasonable telephone connection. Thousands, tens of thousands, of these patents describe technology now in the public domain. More importantly, all of the patents provide teaching – technical know-how that is valuable for further innovation. When you think of the limitation that university libraries (all over the world) have in their acquisition budgets, this is an online database that can be a tremendous resource for spreading technological education.

7. What I would like to do today is talk of the emergence of the Internet and its relationship to international intellectual property norms including the enforcement of rights, in the context of the importance of the international intellectual property legal system for economic development in Brazil. To this end, this paper summarizes the international legal situation and the relationship of technology to the enforcement or rights.

*Substantive International Standards*

8. These questions, raised in the United States and internationally, led to the adoption of two "Internet" Treaties in December 1996 in Geneva at the World Intellectual Property Organization (WIPO). The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) respond to the challenges of protecting works in cyberspace and bring international copyright and neighboring rights standards up to the digital age. Both treaties include norms for standards of protection, provisions on technological protection measures and enforcement requirements that will assure appropriate protection of intellectual property in the digital future.

9. Specifically, the WCT includes provisions on the copyright protection of computer programs and databases and provisions on the rights of distribution, rental, and communication and making available to the public. The Treaty also increases the minimum term of protection for photographic works from 25 years to 50 years.

10. The WPPT includes provisions on the minimum rights granted to performers and producers of sound recordings, including the rights of reproduction, distribution, rental and making available to the public. The Treaty also creates a new minimum term of protection of these rights of 50 years, rather than 20 years as under the Rome Convention.

11. Both treaties contain provisions ensuring that the right owner has the exclusive right to make his or her work available over interactive digital networks and that also permit members

to provide for exceptions to rights in certain special cases for scientific, research and educational activities that do not interfere with the normal, commercial exploitation of the work (e.g., "fair use"). Both treaties also include provisions on technological measures of protection and electronic management information, which are indispensable for an efficient exercise of rights in the digital environment. It is these provisions on technological measures and enforcement that will be the focus of this paper. In discussing these issue, I will draw on the experience of my own country in implementing the treaties and in applying in our national legislation.

The Digital Millennium Copyright Act (DMCA)

12. The U.S. DMCA made the changes necessary in the United States Copyright Law to permit adherence to the treaties. It was necessary to recognize the WCT and the WPPT as points of attachment for protection, but no changes were needed to substantive rights as the United States law already met the requirements of the treaties. The reproduction right in United States law is consistent with the treaties; the making available right, the distribution right and the right of communication to the public are fully implemented by the United States law's provisions on distribution, the reproduction and public performance.

13. However, that was not the case with respect to the provisions related to copyright management information and anticircumvention. Here the DMCA amended the copyright law to prohibit the circumvention of effective technological protection measures that control access to, and prevent the exercise of the exclusive rights in, protected works and the manufacturing or trafficking in technology designed to circumvent measures that control access to such works. The DMCA:

(a) prohibits actions aimed at pirating digitized copyrighted works while still permitting legitimate activities like encryption research and computer security testing;

(b) protects copyright management information – the kind of information attached to a work that identifies the author or the owner as well terms and conditions for the use of the work or phonogram. It forbids removing such information and bars the provision or distribution of false rights management information with the intent to induce or conceal infringement.

Anticircumvention Provisions

14. The anticircumvention provisions of the DMCA cover both the act of circumvention[6] and manufacturing, importing, offering to the public, providing, or otherwise trafficking in circumvention tools.[7] After extensive debate on this issue, Congress concluded that it was appropriate to include both categories of prohibitions. The resulting legislative package was supported by the content industries and also, importantly, by the consumer electronics and computer hardware sectors.

---

[6] 17 U.S.C. § 1201(a)(1).

[7] 17 U.S.C. § 1201(a)(2) and § 1201(b)(1).

15. The DMCA includes separate provisions on circumvention of effective technological protection measures that control access to works[8] and circumvention of technological protection measures that control the exercise of any of the exclusive rights in works.[9] It is important to note that these acts are not limited to copying but include all of the exclusive rights of the copyright owner.

16. The DMCA differentiates between copyright infringement and unauthorized circumvention of technological protection measures. The statute section makes it clear that the anticircumvention provisions have no impact on rights, remedies, or defenses under copyright.[10] It further provides that the copyright liability, if any, of producers or distributors of circumvention products and services is unchanged.

17. As a result, it is not necessary to prove infringement to establish a violation of the anticircumvention provisions. A violation of the anticircumvention provisions is an offense that must be proved on its own. Such an action may be brought by one whose technological protection system is compromised as in the cases involving the encryption system used to protect DVDs – the DeCSS cases, discussed later. Consequently, ordinary copyright defenses do not apply.[11] Thus, the DMCA makes circumvention a separate civil and criminal offense.

18. This distinction is also important in dealing with the circumvention of controls on the exercise of rights in copyrighted materials. For example, when technologies to control copying of protected materials are circumvented, the act of circumvention will typically comprise the unauthorized exercise of an exclusive right – unauthorized copying for example. For this reason, the DMCA does not prohibit the act of circumvention of copy control technology because enforcement of the exclusive right of reproduction would be sufficient to provide "adequate and effective" protection. However, the DMCA includes a prohibition on trafficking in devices or services for the circumvention of technologies that control the exercise of exclusive rights since the copyright law alone would not be fully "adequate and effective" to prevent the making or distributing such devices or services.[12]

19. The DMCA does not specify the technologies covered because to do so would doom the Act to rapid technological obsolescence. *Any* technology is covered if "in the ordinary course of its operation, [it] prevents, restricts, or otherwise limits" the exercise of exclusive rights.[13] Any measure that ordinarily "requires the [authorized] application of information, or a process or a treatment ... to gain access" to a work is protected.[14] Similarly, "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure" is also "circumvention." The DMCA precludes trafficking in circumvention technologies, regardless whether by hardware or software, or a good or a service.

20. The DMCA prohibits only devices or services that are developed or distributed with the purpose of enabling circumvention of technological protection measures. This may be established by: (a) the way that devices or services are designed or produced; (b) the way

---

8 17 U.S.C. § 1201(a).
9 17 U.S.C. § 1201(b).
10 17 U.S.C. § 1201(c)(1).
11 17 U.S.C. § 1201(c)(2).
12 17 U.S.C. § 1201(b).
13 Id.
14 17 U.S.C. § 1201(a)(3).

they are marketed; or (c) the fact that a device or service has only a limited commercially significant purpose or use other than to circumvent.[15] These criteria are intended to apply to those in the business of providing the means to defeat technological protection measures while permitting the manufacture and sale of legitimate consumer electronics and computer equipment that are not intended to circumvent. The DMCA also covers components in the same manner as other products. Those components with commercially significant legitimate uses other than circumvention, and that have not been designed for a circumventing purpose, will fall outside the scope of the anticircumvention provision.

21. It is clear that there is no requirement to design a device to respond to a particular technological protection measure.[16] This "no mandate" provision is important to spell out to the designers and manufacturers of multi-purpose devices, like computers, what the anticircumvention obligation does and does not cover.

22. The treaties provide general guidelines that any exceptions or limitations must be focused narrowly enough to preserve the adequacy and effectiveness of the anti-circumvention prohibitions. The exceptions in the DMCA fall into these categories. For instance, in a situation in which a copyright owner might totally deny access to prospective customers from the non-profit sector, and the work is not reasonably available in any other form, the DMCA includes a limited exception to permit such institutions to circumvent access controls.[17] Similarly, for the purposes of law enforcement, national security, encryption research and the maintenance of computer security circumvention is also permitted.[18] A key feature of all the exceptions in the DMCA is that they are tailored to address specifically the reasons that justified their inclusion in the DMCA – i.e. encryption research, security testing, etc. Exceptions to the anti- circumvention provisions of national law, as in the case of other exceptions, should not be so broad that they undermine the treaty obligations such laws are intended to implement.

23. The DMCA includes both civil and criminal remedies in order to provide an effective deterrent to the manufacture and trafficking in circumvention devices and services. The civil remedies include injunctions, impoundment, actual or statutory damages, costs and attorneys' fees, and destruction of prohibited devices; these may be invoked by any injured party.[19] The criminal penalties apply to willful commercial violators, and include both fines and imprisonment.[20]

## PART I
## TECHNOLOGICAL MEASURES

24. Of course, legal provisions alone are not sufficient to provide meaningful protection in the marketplace.[21] Content providers have repeatedly endorsed the importance of

---

15 17 U.S.C. § 1201(a)(2) and (b)(1).
16 17 U.S.C. § 1201(c)(3).
17 17 U.S.C. § 1201(d).
18 17 U.S.C. § 1201(e),(g) and (j).
19 17 U.S.C. § 1203.
20 17 U.S.C. § 1204.
21 Alan Weintraub and James Lundy, The Gartner Group, Best Bet for Copyright Protection Lies with Your Strategy, July 20, 2001.

technological security measures in ensuring the security of electronic commerce in their products on the Internet. What are the sorts of technological protection measures available to them?

A. Server and File Level Controls

25. Distribution of digital works can be regulated by controlling access to the source of copies of the works – information or data servers. Access to these servers can vary from completely uncontrolled access in which the full contents of the server are available without restriction, to partially controlled access in which unrestricted access is granted to only certain data on the server, to completely controlled access in which no uncontrolled access in any form is permitted. Access control is effected through user identification and authentication procedures that deny access to unauthorized users to a server or to particular information on a server.[22]

26. Nearly all service providers, including commercial on-line services such as America Online, provide private dial-up bulletin board systems, and servers accessible through the Internet, in order to control access to their systems. For example, via the Internet, users today can connect to a bewildering array of public servers using the World Wide Web. Some information providers grant full unrestricted access to all the information contained on their servers, and use control simply to comport with physical limitations of their servers in order to limit the number of concurrent users. Other information providers restrict access to users with accounts or grant only limited access to unregistered users. For example, using ftp a user can often log on to a remote server through the Internet as an "anonymous" user for whom no account has been created in advance; however, such a user will normally only be able to access specific or limited information on the server. An example is a typical airline site like UAL.com the website for United Airlines.

27. Of course, an information provider can elect not to provide uncontrolled access, and permit only those with pre-established accounts to access the server. This is more common with commercially-oriented on-line service providers such as the New York Times website in which access to articles requires registration. Control over access to a server containing

---

[22] The most common elements of such systems involve authentication of the user desiring access to the server. Typically, the server will require entry of a user name and a password. More elaborate mechanisms, however, have been developed. For example, some servers do not grant access once a user is verified, but rather, they terminate the connection and reestablish it from the server to the registered user's site. Such call-back systems tend to govern fully controlled server environments (*e.g.*, where access will only be granted to known and verified users). Other systems are being implemented that use more elaborate authentication systems. For example, a number of companies are developing hardware key systems that require the user, after establishing a preliminary connection, to verify that connection by inserting a hardware device similar to a credit card into the user's computer system. That device then sends an indecipherable code to verify the identity of the user.
Protection of works by means of access control mechanisms assumes that the system in question is in a physically secure environment and is not vulnerable to external means to circumvent access control. Several instances have been reported where the security of a supposedly secure server system was compromised, for example, through passive monitoring during the exchange of unencrypted passwords. As a consequence, many are currently pursuing efforts to improve security at the access control level.

protected works will typically be the first level of protection a content provider will look for before making their protected works accessible through the server.

28. A second level for controlling access to and use ofprotected works can be exerted through control measures tied to the electronic file containing the work.

29. Restrictions on access at the file level can be implemented using features in "rendering" software. An example of a system providing such services is Adobe Acrobat. For example, a content provider may develop specialized software products or implement features in general purpose software products that would control by whom, and to what degree, a protected work may be used. Such restrictions could be implemented using features in the rendering software, a unique file format or features in an established file format, or a combination of both. "Control" measures could also be implemented to determine if the content provider had authorized certain uses of the work, as well as some means to control the degree to which a user would be able to subsequently "manipulate" the work. For example, the rendering software could preclude a user who had not obtained the appropriate authority from the content provider or who enters an unauthorized or expired password from using the data. Rendering software can also be written to deny general access to the work if the file containing the work is not a properly authenticated copy – one in which the file has been altered from the version as distributed by the content provider. Such features are possible provided that sufficient information regarding authorized use can be associated with the file containing the information product through inclusion in a file header, packaged and sealed in an "electronic envelope" sealed with a digital signature, embedded through steganographic means,[23] etc.[24]

B. Encryption

30. In its most basic form, encryption amounts to a "scrambling" of data using mathematical principles that can be followed in reverse to "unscramble" the data. File encryption thus simply converts a file from a manipulable file format such as a word processor document or a picture file that can be opened or viewed with appropriate software to a scrambled format.[25] Authorization in the form of possession of an appropriate "key" is required to "decrypt" the file and restore it to its manipulable format.

31. Encryption techniques use "keys" to control access to data that has been "encrypted." Encryption keys are actually strings of alphanumeric digits that are plugged into a mathematical algorithm and used to scramble data using that algorithm. Scrambling means that the original sequence of binary digits–the 1s and 0s that make up a digital file–that constitute the information object is transformed using a mathematical algorithm into a new sequence of binary digits – a new string of 1s and 0s. The result is a new sequence of digital

---

23 *See* discussion of stenography *infra*.

24 For example, the software may deny access to a work if the electronic file containing the work has been altered or information stored in the file does not match data supplied by a user necessary to open and use the file. *See* discussion of digital signatures *infra*.

25 Rendering or viewing software may integrate encryption and file manipulation into a single software package. In other words, the rendering software, after getting a password, will decode the file and permit the user to manipulate the work (*e.g.*, view it or listen to it), but only with the provided rendering software.

data that represents the "encrypted" work.[26] An example of this type of protection is the encryption used to protect DVD copies of motion pictures. Anyone with the key can decrypt the work by plugging it into a program that applies the mathematical algorithm in reverse to yield the original sequence of binary digits that comprise the file. Although most commonly thought of as a tool for protecting works transmitted via computer networks, encryption can be and is used with virtually all information delivery technologies, including telephone, satellite and cable communications. Of course, once the work is decrypted by someone with the key, there may be no technological protection for the work if it is stored and subsequently redistributed in its "decrypted" or original format.

32. A widely discussed technique for sending secure transmissions of data is "public key" encryption. This technique can be used to encrypt data using an algorithm requiring *two* particular keys – a "public" key and a "private" key. The two keys are affiliated with the recipient to which the information is to be sent. The "public" key is distributed publicly, while the private key is kept secret by recipient. Data encrypted using a person's public key can only be decrypted using that person's secret, private key. For instance, a copyright owner could encrypt a work using the public key of the intended recipient. Once the recipient receives the encrypted transmission, he could then use his private key to decrypt that transmission. No secret (private) keys need to be exchanged in this transaction. Without the private key of the intended recipient, the work cannot be read, manipulated or otherwise deciphered by other parties. Of course, if a decrypted copy is made and shared, then others could manipulate the work unless other means are used to protect it.

33. There may be instances where someone other than the communicating parties needs access to the encrypted data. A key escrow system is one way such access might be obtained. A key escrow system would hold the key needed to decrypt an encrypted transmission in "escrow." Such a system could be maintained by a private organization or the government, and anyone seeking access to an encrypted transmission would have to demonstrate their need for the key through a process, such as obtaining a search warrant, that ensures the legitimate privacy and security needs of users of encrypted transmissions or that certain contract terms have been met.

C. Digital Signatures

34. First, one should note that these digital "signatures" are not the kind of signatures covered by the legislation providing for the legitimacy of digitally represented copies of a signature. Mathematical algorithms can also be used to create digital "signatures" that, in effect, place a "seal" on a digitally represented work. Generating a digital signature is referred to as "signing" the work. The algorithms can be implemented through software or hardware, or both. The digital signature serves as means for authenticating the work, both as to the identity of the entity that authenticated or "signed" it and as to the contents of the file that encodes the information that constitutes the work. Thus, by using digital signatures one will be able to identify from whom a particular file originated as well as verify that the contents of that file have not been altered from the contents as originally distributed.

35. A digital signature is a unique sequence of digits that is computed based on (1) the work being protected, (2) the digital signature algorithm being used, and (3) the key used in digital

[26] An algorithm is a set of logical rules or mathematical specification of a process which may be implemented in a computer.

signature generation.[27] Generating a digital signature uses cryptographic techniques, but is not encryption of the work; the work may remain unencrypted so it can be accessed and used without decryption. In fact, digital signatures and encryption can be used simultaneously to protect works. Generally, a signature is computed for a copyrighted work first and then the work (including the seal) is encrypted. When the work is to be used, the work is decrypted, then the signature–the seal–is verified to be sure the work has not been modified either in its original or encrypted form. If the work is never changed, the seal need never be removed or changed. If the work is changed, a new seal must be computed on the revised information.

36. Typically, the digital signature is incorporated in some manner in the transmission that constitutes the work. Often, the sender will also distribute his public key as well. The signature serves as a "seal" for the work because the seal enables the information to be independently checked for unauthorized modification.[28] If the seal is verified by independently computing a signature matches the original signature, then the work is a bona fide copy of the original work in which nothing has been changed in the file that constitutes the work.

D. Steganography

37. Innovative new techniques are being developed to address security or management driven concerns relating to dissemination and use of digitally-encoded information. For example, methods have been developed that can encode digitized information with attributes that cannot be disassociated from the file that contains that information. This field of technology has been termed "steganography" and been conceptually referred to as "digital fingerprinting" or "digital watermarking."

38. In essence, using steganographic techniques, a party can embed hidden messages in digitized visual or audio data. The embedded information does not degrade or otherwise interfere with the audio or visual quality of the work. Instead, the embedded information can only be detected if specifically sought out. More advanced steganographic techniques based on statistical or entropically-directed encoding are proving to be difficult to defeat. For example, one system modulates a known noise signal with the information to be embedded and adds the "scaled" signal to the original data. Once encoded in this fashion, the steganographically encoded identification data is distributed throughout the work as subliminal noise and, like noise, cannot be fully eliminated from the work. Thus, one can ensure detection of an embedded message even after substantial corruption of the data, such as might occur through compression/decompression, encoding, alteration or excerpting of the original data. By providing a means to indelibly tag a work with specific information, steganography is likely to play a complementary role to encryption as well as authentication techniques based on digital signatures.

---

[27] The signature is generated using the binary digits of the work plus the value of the private key as inputs to the computation defined by the algorithm. Thus, the digital signature for an information object is a unique sequence of digits for that work. Specifically, a signature is not the same for different works using the same private key.

[28] Anyone who has access to an information object, in addition to having access to the work, also has access to the digital signature for the object. Consequently, the digital signature for the object may be recomputed and used to independently confirm the integrity of the object by comparing it to the digital signature appended to the object.

E. Controlling Use of Protected Works

39. Content providers will rely on a variety of technologies, based in software and hardware, to protect them against unauthorized uses of their information products and services.

40. One example can be found in the Audio Home Recording Act. This Act requires that manufacturers of digital audio recording devices and digital audio interface devices incorporate features that limit serial copying.[29] The hardware is programmed to read certain coding information contained in the "digital subcode channel" of digital sound recordings and broadcasts. Based on the information it reads, the hardware circuitry will permit unrestricted copying, permit copying but label the copies it makes with codes to restrict further copying, or disallow copying. The serial copy management system allows unlimited first generation copying – digital reproduction of originals (such as CDs distributed by record companies), but prevents further digital copying from those reproductions.[30]

41. Similar systems can be implemented through hardware, software or both, using the concepts discussed above such as rendering software and encryption technology. For example, files containing works can include instructions used solely to govern or control distribution of the work. This information might be placed in the "header" section of a file[31] or another part of the file. In conjunction with receiving hardware or software, the information, whether in the header or elsewhere, can be used to limit what can be done with the original or a copy of the file containing the work. It can limit the use of the file to view- or listen only. It can also limit the number of times the work can be retrieved, opened, duplicated or printed.

42. Just as legal provisions alone are insufficient to ensure effective protection of content moving in electronic commerce, technological measures must be backed up by legal measures to guard against their unauthorized circumvention.

## PART II
## TECHNOLOGY AND ENFORCEMENT

43. The employment of technology for enforcement of rights in copyright and related rights raises a number of issues that are sensitive to both content providers and to users. One only has to read the current press to note the reaction of various groups to the application of the enforcement provisions of the U.S. DMCA.[32] The use of the law to shut down free file sharing of music files through Napster,[33] the suppression of the distribution of software to

---

29 *See* 17 U.S.C. § 1002.

30 *See* H.R. REP. NO. 102-873(I), 102d Cong., 2d Sess., *reprinted in* 1992 U.S.C.C.A.N. 3578, 3579-80, 3583 n15.

31 A "header" is a section of a digital work where information, data, codes and permitted uses may be embedded. Such information may actually be embedded anywhere in the work, but for ease of reference, this paper refers to such information as embedded in a header. Terms such as "label" and "wrapper" are also used to refer to what this paper refers to as a "header."

32 See for example, *Confusion over copyright and free speech*, THE IRISH TIMES, Monday August 27, 2001.

33 *Defunct Seoul Music Site Hit hard*, WIRED NEWS, August 27, 2001.

decrypt encrypted motion pictures[34] and the criminal enforcement proceedings against the Russian hacker[35] who penetrated the Adobe security measures used for electronic books have all made the general public aware of this issue.

44. In Part I of this paper, we discussed the sorts of technological measures required by the WCT and the WPPT and the technologies for their implementation. In Part II, we will examine the level of enforcement required to properly implement the treaties taking into account the Agreement on Trade-Related Aspects of Intellectual Rights (TRIPS Agreement) enforcement regime and the use of technology in the enforcement process. Again, I will draw on the United States of America experience in the implementation of the treaties through the DMCA to illustrate my remarks.

Enforcement

45. Most disputes involving Internet piracy issues in the United States are resolved through civil litigation governed by TRIPS-compliant judicial procedures. Criminal penalties, however, may be imposed under various statutes, including the No Electronic Theft Act (NET Act) which criminalizes computer theft of copyrighted works, whether or not the defendant derived a direct financial benefit or commercial advantage from the acts in question. In addition, the United States Department of Justice has established a special section within its Criminal Division called the Computer Crimes and Intellectual Property Section (CCIPS) which handles the prosecution of federal crimes involving Internet piracy (among other computer and intellectual property crimes), including prosecutions under the NET Act.

46. There is currently no multinational treaty that addresses in detail all of the issues raised regarding enforcement of intellectual property rights on the Internet. Both the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) require that signatories ensure that enforcement procedures are available to permit "effective action" against covered acts of infringement, including Internet piracy. Such enforcement measures must include expeditious remedies to prevent infringement as well as remedies that deter future infringements.[36]

47. In addition, the enforcement provisions contained in Part III of the TRIPS Agreement, with its requirements of fair and equitable procedures, swift and effective enforcement actions and adequate compensation to the rights holder (among others), are not limited to enforcement of rights in a physical medium that is to say in connection with goods and services. Instead, they are equally applicable to infringing activities that arise in the digital universe, including infringing acts of piracy on the Internet. Thus, the legal framework for protecting copyrighted works against piracy via the Internet is established by the TRIPS Agreement in conjunction with the WCT and the WPPT.

---

34 C. Scott, *Criminal Code?,* Salon Technology , February 9, 2000.

35 See *U.S. Indicts Russian Programmer*, ZD Net News, August 28, 2001.

36 WCT, Article 14; WPPT, Article 23.

A. Coverage of Internet Piracy as an Infringing Act

48. Although neither the term "Internet" nor "digital" expressly appear in the language of the TRIPS Agreement or the relevant articles of the Berne Convention which are incorporated by reference in the TRIPS Agreement in Article 9,[37] the substantive protections which must be granted a copyright holder under the Treaty include protection against the reproduction and distribution of copyrighted works via the Internet without the copyright owner's approval. These substantive provisions require that a copyright owner be granted the exclusive right to authorize, *inter alia*, the reproduction, translation and adaptation of their works, as well as their public distribution, display and performance. [38] Numerous countries, including the United States of America, have recognized that reproduction and/or distribution of a copyrighted work, in whole or in part, without the copyright owner's permission on the Internet qualifies as copyright infringement.[39]

B. Remedies for Internet Piracy

49. The most comprehensive international provisions regarding the protection of copyrighted works from piracy in any medium of expression are contained in Part III of the TRIPS Agreement. These provisions**,** although adopted to deal with conventional piracy, are technologically neutral and equally applicable to Internet piracy. They require that countries establish a multi-disciplinary approach to IP enforcement. In other words, the TRIPS Agreement requires that countries establish civil, criminal and border enforcement measures that serve as an effective deterrent against intellectual property infringement. The TRIPS Agreement specifically requires that such measures be in place "to permit effective action against any act of infringement" of the rights granted under the Treaty.[40] These acts of infringement include acts of Internet piracy. To combat such piracy, the TRIPS Agreement requires that at a minimum:

(a) Procedures established to combat such piracy must be fair and equitable. They must not be unnecessarily complicated or costly. In addition, such procedures must not entail unreasonable time-limits or unwarranted delays in granting relief.[41] The absence of any such delays is particularly important in connection with Internet piracy where pirated copies of a work can be disseminated in seconds around the globe and files can be erased with the click of a mouse.

---

37 Article 9 of TRIPS incorporates by reference Articles 1 through 21 of the Berne Convention, with the exception of Article 6bis (the "moral rights" provision).

38 *See generally* Berne Convention, Articles 8, 9, 11, 11bis, 11ter, and 12.

39 *See, e.g, Playboy Enterprises Inc v. WebbWorld, Inc*., 991 F. Supp. 543 (N.D. Tex. 1997)(distribution of copyrighted photographs without permission on the Internet qualifies as copyright infringement); *Shetland Times Ltd. v. Wills*, [1997] FSR 604 (October 1996)(distribution of copyrighted headlines and articles without permission on Internet qualifies as copyright infringement).

40 TRIPS Article 41.

41 TRIPS Article 41(2).

(b) Copyright owners must be granted the right to seek relief against Internet pirates in civil (or administrative) proceedings.[42] In these proceedings:

(i) Defendants must be given timely written notice of such proceedings. In cases where the relief is sought ex parte (as is often the case in Internet piracy), such relief may be provided after provisional relief has been granted. (See below) Such notice must contain sufficient detail regarding the alleged infringement, including the basis of the claims.[43]

(ii) Parties must have the right to substantiate their claims and to present all relevant evidence.[44]

(iii) Decisions on the merits must be based on the evidence presented in the case by the parties. It should preferably be in writing, with the reasons for the decision explained.[45]

(iv) Judges must be authorized order the production of evidence necessary to substantiate a party's claim where the party has been unable to obtain such evidence from the opposing party.[46]

(v) Judges must also be granted power to do the following in connection with cases involving Internet piracy:

– Enjoin a defendant from committing further infringing acts on the Internet.[47]

– Order the payment of monetary damages by the defendant in an amount adequate to compensate the copyright owner for the injury suffered, including costs and, in appropriate cases, the recovery of profits and/or statutory damages.[48] The unauthorized dissemination of copyrighted works over the Internet has the potential to cause great harm to a copyright owner, even if the pirate does not charge for access to the pirated works, since such unauthorized dissemination may destroy the market value of the copyrighted work in question. Consequently, money damages awarded in the United States of America include both an award for the copyright owner's lost profits, as well as for the defendant's profits. In addition, United States law allows the copyright owner to seek statutory damages which may be as much as US$150, 000 per infringement for willful copyright infringement as an alternative to actual damages.

---

42 TRIPS Article 41.
43 Id.
44 Id.
45 TRIPS Article 41(4).
46 TRIPS Article 43(1).
47 TRIPS Article 44(1).
48 TRIPS Article 45.

– Order the seizure of infringing goods and materials and of the implements the predominant use of which has been the creation of the infringing goods.[49] Where there is no physical good per se, seizure of the website and other instrumentalities used to conduct the infringing activities may be required to avoid future infringing acts. Judges must also be granted the power to dispose of all seized goods, materials and implements outside the channels of commerce "in such a manner as to avoid any harm caused to the right holder" or, alternatively to destroy them, without compensation to the infringer.[50] Since Internet piracy does not usually involve physical copies of the goods "destruction" would usually entail the elimination of the offending website, as well as an injunction against any future infringing acts on any website. In the United States of America, such injunctions are enforced through the court's power to impose fines and penalties if the injunctions are not obeyed.

– Grant temporary restraining orders and provisional relief to prevent infringement and preserve evidence. Such relief must be available *inaudita altera parte* (*ex parte*, without notice to the defendant) in particular where any delay is likely to cause irreparable harm to the right holder or where there is a demonstrable risk of evidence being destroyed.[51] In the case of Internet piracy in the United States of America such injunctions are routinely granted due to the great harm that may be caused by the continued unauthorized dissemination of pirated materials via the Internet. In accordance with the TRIPS Agreement requirements,[52] the plaintiff must, of course, indemnify the defendant against harm caused if the provisional relief in question was improvidently granted.

– Require the complaining party to indemnify the defending party against harm if a decision on the merits finds that the ordered provisional relief was unjustified.[53]

– Where the relief is granted *inaudita altera parte* (*ex parte*), affected parties must be given notice, without delay, of such action and must be granted a right of review and to be heard within a reasonable period after such notice regarding whether the relief granted should be modified, revoked or confirmed.[54]

(vi) In the United States of America, all such civil enforcement proceedings are conducted by judicial personnel. Where, however, civil enforcement of

---

49 TRIPS Article 46.
50 Id.
51 TRIPS Articles 50(1) and (2).
52 TRIPS Article 50(3)
53 Id.
54 TRIPS Article 50(4).

intellectual property rights is conducted by administrative (as opposed to judicial) proceedings, all of the above requirements apply.[55]

C. The WIPO Copyright and WIPO Performances and Phonograms Treaties

50. In addition to the enforcement provisions of the TRIPS Agreement, the United States of America is convinced that implementation of the provisions of the WCT and the WPPT also assist in combating Internet piracy. Both the WCT and the WPPT require members to provide adequate legal protection and effective legal remedies against any act of infringement rights covered by the treaties which would include providing for sanctions against the circumvention of "effective technological measures" and the removal or alteration of rights management information. The WCT requires members to provide "adequate legal protection and effective legal remedies" against the circumvention of effective technological measures used by authors in the exercise of their rights, or used by authors to restrict acts which are not authorized by the author, such as, for example, copy technology that prohibits the unauthorized reproduction of a copyrighted work.[56] The WPPT contains a similar provision with regard to technological measures used by performers or producers of phonograms.[57]

51. The WCT also requires members to provide "adequate and effective legal remedies" against the unauthorized removal or alteration of "rights management information" where such removal is done knowing (for criminal remedies) or with reasonable grounds to know (for civil remedies) that such act will induce, enable, facilitate or conceal an infringement of any copyright. Distribution, importation, broadcast and communication to the public of the work knowing that the "rights management information" has been removed or altered without authority must also be prohibited.[58]

52. The WPPT contains similar provisions prohibiting the unauthorized alteration or removal of rights management information from copies of fixed performances and phonograms, as well as the distribution, importation, broadcast or communication to the public of such copies and phonograms containing management rights information which has been altered or removed without authorization.[59] Both treaties define "rights management information" as information identifying the work or performance in question, the author or performer, the owner of any right in the work, information about the terms or conditions of any use of the work in question, and any "numbers or codes that represent such information."

53. Strong prohibitions against the circumvention of copy technology and other technological measures used by copyright owners to protect their works from unauthorized use are particularly helpful in combating Internet piracy since many pirates must necessarily circumvent such measures in order to reproduce software, and other optical media products. Rights management information also helps copyright owners track Internet piracy by allowing them to track unauthorized copies of their works. Thus, strong protection against the removal or alteration of rights management information serves a useful function in protecting another tool which copyright owners have to protect their works.

---

55 TRIPS Article 49.
56 WCT Article 11.
57 WPPT Article 18.
58 WPPT Article 12.
59 WPPT Article 19.

54. As noted above, both the WCT and the WPPT include a general article on enforcement that requires member countries to establish effective enforcement measures against any infringing acts in violation of the rights granted under the respective treaties.[60] These infringing acts include violations of the anti-circumvention and rights management integrity measures discussed above. They also include, among others, violations of the copyright owner's exclusive right of public distribution and communication to the public of his work or performance,[61] violations of which are often involved in cases of Internet piracy. The intent of these enforcement provisions was to assure that the TRIPS Agreement remedies would be available for the subject matter of the WCT and WPPT.

55. Again, in order to emphasize the importance of these standards, I will turn to the law of the United States of America for examples of our approach to the provision of adequate and effective enforcement in the digital environment.

D. The U.S. Digital Millennium Copyright Act

56. The DMCA amended the United States domestic law to give force to its obligations under the WCT and the WPPT. The Act established both civil and criminal remedies for violations of the anti- circumvention and rights management integrity provisions of the statute. The full range of remedies is available in civil proceedings, including temporary and permanent injunctive relief, impoundment of "any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in the violation." The DMCA also provides for the remedial modification or destruction of such device, or any device that has not been impounded but which was involved in the violation and was in the custody or control of the violator. Last, but not least, the DMCA provides for money damages.[62] These damages may include costs, reasonable attorney's fees, actual damages, including the damages suffered by the copyright owner as a result of the violation and any profits of the violator that are attributable to the violation and not taken into account in computing the actual damages, or at the complaining party's election, statutory damages.[63]

57. Statutory damages for a violation of the anti-circumvention provisions discussed previously are not less than US$200 or more than US$2,500 "per act of circumvention, device, product, component, offer, or performance of service, as the court considers just."[64] For violations of the rights management integrity provisions also previously discussed, statutory damages are not less than US$2,500 or more than US$25,000 for each violation. In the event that a person violates the anti-circumvention or rights management integrity provisions within three years after a final judgment was entered against that person for another such violation, the court may increase the award of damages up to triple the amount it would otherwise award. The statute provides an exemption for nonprofit libraries, archives and educational institutions which prove that they had no reason to believe their acts were a violation.[65]

---

60 WCT Article 14 and WPPT Article 23.
61 *See generally* Articles 6 and 8 of the WCT and Articles 7-15 of the WPPT.
62 17 U.S.C. § 1203.
63 Id.
64 17 U.S.C. § 1203.
65 Id.

58. Persons who violate the anti-circumvention and rights management integrity provisions of the DMCA "willfully and for purposes of commercial advantage or private financial gain" are subject to criminal penalties under the Act. For first time offenders, penalties range from fines up to US$500,000 or imprisonment for not more than five years, or both. For repeat offenders, penalties are increased to fines up to US$1,000,000 and imprisonment for not more than 10 years or both.[66]

(e) The No Electronic Theft (NET) Act

59. The No Electronic Theft Act ("NET Act") established criminal penalties for willful infringement of copyright through electronic means even where there is no purpose to obtain a commercial advantage or private financial gain. Under the Act, persons who willfully infringe a copyright by the reproduction or distribution, "including by electronic means," of one or more copyrighted works, or one or more copies or phonorecords which have a total retail value of more than US$1,000 during any 180-day period face criminal penalties.[67] These penalties include fines of up to US$100,000 (US$200,000 if the defendant is an organization) and imprisonment for up to one year, or both. Where at least 10 copies of one or more copyrighted works are distributed within a 180-day period, and the retail value of the copyrighted works is more than US$2,500, the penalties are increased to fines up to US$250,000 (US$500,000 where the defendant is an organization) and imprisonment for not more than three years, or both.[68] For repeat offenders, the penalties are increased to fines up to US$250,000 (US$500,000 where the defendant is an organization) and imprisonment for not more than six years, or both.[69]

60. Where works are willfully infringed for purposes of commercial advantage or private financial gain, no threshold number of copies is required for criminal penalties to apply. Under United States law, "financial gain" is defined to include "the receipt or expectation of receipt of anything of value, including the receipt of other copyrighted works."[70] A defendant does not have to expect to make money in order for criminal penalties to apply. Just swapping music files could trigger the NET Act. Consequently, those who aid in stealing copyrighted works, but do not profit financially from the theft, may still be prosecuted. Criminal penalties for willful infringement for purposes of commercial advantage or financial gain are relatively severe. Any one who reproduces or distributes, including by electronic means, at least 10 copies or phonorecords or one or more copyrighted works with a retail value of more than US$2,500 within a 180-day period faces fines up to US$250,000 (US$500,00 if the defendant is an organization), imprisonment up to 5 years, or both. Penalties for repeat offenders increase to fines up to US$250,000 (US$500,000 if the defendant is an organization) and imprisonment up to 10 years, or both.[71] All other acts of willful infringement for commercial gain are punishable by fines up to US$100,000 (US$200,000 if the defendant is an organization) and imprisonment up to one year, or both.[72]

---

66 17 U.S.C. § 1204.
67 17 U.S.C. § 506(a).
68 17 U.S.C. § 506 (a); 18 U.S.C. § 2319.
69 17 U.S.C. § 506(a); 18 U.S.C. § 2329.
70 17 U.S.C. § 101.
71 17 U.S.C. § 506(a); 18 U.S.C. § 2319.
72 17 U.S.C. § 506(a); 18 U.S.C. § 2329.

F. Statutory Damages

61. In addition to the statutory damage awards described above that may be awarded for violations of the DMCA, United States copyright law also provides for statutory damages in civil cases for any infringement of a copyright owner's rights. Under United States law, the copyright owner is always entitled to an award of actual damages. These damages include the harm suffered by the copyright owner as a result of the infringement, as well as any of the defendant's profits that have not been taken into account in computing the owner's actual damages.[73] In addition, before a final decision has been rendered, the copyright owner is entitled to elect to receive statutory damages instead of actual damages. Statutory damages range from a minimum of US$750 to US$30,000 per infringement (for non-willful infringement) up to US$150,000 per infringement for willful infringement of a copyrighted work. Courts are also empowered to award costs and reasonable attorney's fees to the prevailing party.

G. The Role of Technology

62. Just as technology is essential to the protection of the rights of copyright and neighboring rights owners on the Internet, it is as well important to the effective enforcement of those rights. The recent example of the Napster Case will illustrate the importance of using technology in enforcement.

63. One of the most pressing issues confronting the world of copyright is the set of legal consequences that arise from the intersection of advances in Internet file sharing technology and copyright and related rights law. Internet peer-to-peer file sharing–p2p technology–permits individuals to provide access to files stored on their computers to others in a timely and efficient manner. Coupled with file compression technology like MP3 that permit digital files of copyrighted information to be packaged in volumes that allow their internet transmission in an efficient manner, these p2p technologies have lead to the rapid growth of the exchange of files of information – much of it copyrighted - over the Internet. Services established using these technologies–Napster, Gnutella, Scour, etc.–make the newspapers and on-line news sites daily.[74]

64. Everyone is aware that the file sharing services provided by Napster to over 50 million users in the United States of America and abroad have been the subject of intense scrutiny in the United States, in the press, in legal seminars, in the Congress and in the courts. As John Perry Barlow, champion of the digerati, put it, "[t]he great cultural war has broken out at last. Long awaited by some and a nasty surprise to others, the conflict between the industrial age and the virtual age is now being fought in earnest, thanks to the modestly conceived but paradigm-shifting thing called Napster."[75] Others took a more circumspect view of these developments.

65. File sharing systems like Napster were still in the future when the United States Congress adopted the DMCA in 1998, however the practice of "sharing" MP3 music files by

---

[73] 17 U.S.C. § 504.

[74] Napster Finds Old Space Crowded, Wired News, June 26, 2001, reporting on the upsurge of new file sharing websites after the injunction to prevent Napster from trading copyright protected music was enforced.

[75] Wired Magazine, October 2000.

e-mail was widely practiced at a level that was annoying to right holders, but not yet demonstrably detrimental to conventional systems for the distribution of music. That was all to change in a short time when Napster burst onto the scene.

66. Napster is an example of what is called a "peer-to-peer" system on the Internet or World Wide Web. Instead of computer files being stored on, and distributed from, large, centralized "server" computers, Napster allows individuals to ask for and obtain copies of files from others' personal computers if those individuals are using the Napster system. The computer file travels from a "peer" (a person's PC) to another "peer" without having to reside in an intervening storage facility.

67. Napster became increasingly popular with Internet users as a way to download free music – at its peak some 20 - 50 million people used Napster each month. The major record labels and various musicians – including Metallica and Dr. Dre – sued Napster, arguing that Napster users were committing copyright infringement and, that because Napster knew what was going on, Napster should be held liable for contributory and/or vicarious infringement. The major suit against Napster, *A & M Records, et. al v. Napster* was started on December 6, 1999.

68. The record companies moved for a preliminary injunction against Napster. At the hearing for that injunction, evidence established that at least 70% of the music files being copied and transferred on Napster belonged to the plaintiffs and were being copied and transferred without authorization.

69. On July 26, 2000, Judge Patel in the Northern District of California issued a preliminary injunction against Napster, ordering Napster to stop "from engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound records..." After Judge Patel issued her opinion supporting the preliminary injunction on August 10, 2000, Napster appealed. Pending the appeal, the Ninth Circuit Court of Appeals issued a stay of the injunction pending the hearing of the appeal.

70. The Ninth Circuit decision on February 12, 2001, affirmed most of Judge Patel's analysis as to infringement.[76] The Ninth Circuit affirmed the trial court analysis on the following points:

(a) that Napster users are not engaged in "fair use" when making thousands of unauthorized copies;

(b) that Napster is not protected by the *Sony v. Universal City Studios*[77] defense of "time shifting" because Napster, unlike the VCRs at issue in *Sony*, involves not only copying a work, but also public distribution of the work;

(c) that Napster has both actual and constructive knowledge that its users were engaged in widespread copyright infringement; that Napster materially contributes to the infringing activity, therefore, making it liable for contributory infringement;

---

[76] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[77] 464 U.S. 417 (1984).

(d) that Napster probably has a "direct financial interest in the infringing activity" and that Napster has the ability to "control" and "patrol" its users activities, at least as to identifying the names of music files to know that they are copyrighted works. Therefore, the Ninth Circuit agreed that Napster was likely to be found to be vicariously liable.

71. As to the DMCA, the Ninth Circuit said that this issue needed to be developed further at trial and that, in the interim, the balance of hardships tipped in favor of the record companies and musicians, that is to say, in favor of the preliminary injunction. The Ninth Circuit ordered that the injunction be narrowed to take account of Napster's technology, and the issue was returned to Judge Patel for further proceedings. As a result of those further proceedings Judge Patel ordered Napster to use filtering technology to prevent the trading of copyright protected recordings over its system. This filtering technology, in effect, checks the names of files traded through the system against a list of protected titles and will not allow their transmission. The record companies have periodically raised concerns over the effectiveness of the technology used by Napster and Judge Patel has ordered Napster to improve the technology. In this case, Judge Patel has appointed a technology consultant to advise the court on the technology issues and to work with the parties to ensure the effectiveness of the blocking.

72. The music swapping phenomenon is by no means limited to the United States of America. At its peak, nearly 40% of Napster users were from other countries. As well, other countries have had their own versions of Napster. The International Federation of Phonographic Industries (IFPI) reports that they have been successful in the courts in Belgium Denmark, France and Sweden in pursuing remedies against such operations. In those countries courts have held that such systems amount to the "unauthorized communications" of works. In the Republic of Korea, the court recently held a Napster-like service liable for damages.

73. More troubling is the proliferation of file-sharing systems that do not rely on central servers to distribute the files sharing software or that rely on off-shore servers. In order to pursue these actions, IFPI relies on a variety of technological measures – an advanced Web crawler that identifies unauthorized files, and "fingerprinting" technology which can identify a song by its audio characteristics.[78]

74. The Internet remains a tremendous tool for performing artists to bring their music directly to audiences. Nothing in the Ninth Circuit's decision prevents musicians from developing their own websites and freely distributing their own music in order to build fans or indeed from permitting fans to use Napster or Napster-like services to distribute their music. The Napster opinion affirms a simple truth: the decision to distribute a musician's music free on the Internet is a decision that should be made by the musician and his or her record company.

75. The interesting issue raised by this decision is of course where do the music industry and Napster go from here? As the initial quote from John Perry Barlow indicated, Napster and its progeny have changed the landscape. Music companies and musicians need to come to grips with the commercial implications of the new technologies. I, personally, do not believe that the traditional distribution models will continue to be the sole or perhaps even the dominant form of music distribution. The preliminary deals struck between MP3, Napster

---

[78] *Pirated music battle spreads overseas*, ZD NET NEWS, August 23, 2001.

and some music publishers–most notably Bertelsmann–as well as the launches of music sites the major labels by seem to point in this direction.[79]

76. In order to protect their copyrights, over the years, motion picture studios have used copy a variety of methods to protect their works distributed on videocassettes such as Macrovision. Similarly, satellite television services use encrypted signals to prevent their signals from being received by non-subscribers. The motion picture industry has pursued vigorously those who distribute, devices that break such copy protection including illegal "black boxes" to defeat Macrovision and illegal "smart cards" that allow illegal access to satellite television.

77. However, Macrovision does not work on digital recordings, so the industry was faced with the need to develop a protection mechanism of the digital environment. CSS is the copy protection system adopted by the motion picture industry and consumer electronics manufacturers to provide security to copyrighted content of DVDs and to prevent unauthorized copying of that content. CSS is the kind of access control mechanism protected by the anticircumvention provisions of the WCT and the WPPT as well as the U.S. DMCA. Because it controls access to the DVD content, it may be viewed as akin to the lock on a video rental shop. The motion picture industry has created the DVD Copy Control Association (DVD CCA), a not-for-profit corporation, in order to license the CSS (Content Scramble System) to manufacturers of DVD hardware, discs and related products. They have licensed owners and manufacturers of the content of DVD discs; DVD replicators, creators of encryption engines, hardware and software decryption devices, and manufacturers of DVD players and DVD-ROM drives.

78. Anticipating the potential of digital technology for facilitating piracy, the film industry relied on the security provided by CSS in manufacturing, producing and distributing to the public copyrighted motion pictures in DVD format. Those motion pictures, many of which involved investments of tens and even hundreds of millions of dollars, were distributed on CSS-protected DVDs. CSS allows consumers to enjoy the benefits of digital entertainment because the motion picture industry is able to issue their films on DVD while at the same time preventing massive piracy of their copyrighted works. De-encryption destroys this protection, which is why distribution of de-encryption devices were prohibited in the DMCA.

79. In late 1999, a small group of hackers in Europe worked to "crack" the CSS encryption system for DVDs and created an unauthorized software utility commonly referred to as DeCSS. A computer that has the DeCSS utility can use it to break the CSS code on DVDs making it possible for motion pictures in DVD format to be decrypted and illegally copied onto a computer's hard-drive. Some argue for the purposes of viewing on a different platform such as a Linux-based machine. However, many of the decrypted films were made available for further distribution over the Internet or otherwise, in perfect, digital format.

80. The development and distribution of DeCSS may lead to widespread digital video piracy. Currently, the impact of hacks such as DeCSS is limited by the amount of time needed to download a full-length motion picture over the Internet. However, as the bandwidth of the Internet increases rapidly, the ability increases for pirates to create perfect, illegal digital copies of movies from DVDs using the DeCSS utility and to post those copies

---

[79] P. J. McNealy and Mike McGuire, The Gartner Group, Digital Content Sales Hinge on Standardized Protection, 29 August 2001.

on websites for download by Internet users all over the world. Consequently, in order the protect its legitimate interests, the motion picture industry has actively sought to suppress the distribution of the DeCSS software by bringing suit to enjoin the distribution of DeCSS under the DMCA.[80] The court granted the preliminary injunction, and in further proceedings, it made the injunction permanent. The judgment has been appealed but no decision has yet been rendered.

Conclusion

81. Internet piracy poses a severe threat to the global copyright industry and to the continuing growth of e-commerce on the Internet. As the specialized problems in dealing with copyright piracy in a digital environment become clearer, it is expected that additional international standards for dealing with these problems will develop. United States law is also evolving in this rapidly changing area to meet the demands posed in assuring that the valuable intellectual property rights of copyright owners are protected against the rapacious acts of Internet pirates.

[End of document]

[80] Shortly after the commencement of the action, the Court granted plaintiffs' motion for a preliminary injunction barring defendants from posting DeCSS. *Universal City Studios, Inc. v. Reimerdes,* 82 F. Supp.2d 211 (S.D.N.Y. 2000).