E

WIPO

WCT-WPPT/IMP/3.
ORIGINAL: English
DATE: December 3, 1999

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

WORKSHOP ON IMPLEMENTATION ISSUES OF THE WIPO COPYRIGHT TREATY (WCT) AND THE WIPO PERFORMANCES AND PHONOGRAMS TREATY (WPPT)

Geneva, December 6 and 7, 1999

TECHNICAL PROTECTION MEASURES: THE INTERSECTION OF TECHNOLOGY, LAW AND COMMERCIAL LICENSES

by Dean S. Marks[*] *and Bruce H. Turnbull*[**]

[*] Senior Counsel Intellectual Property, Time Warner Inc., Burbank, California
[**] Partner, Weil, Gotshal & Manges LLP, Washington, D.C.

TABLE OF CONTENTS

Introduction[1]

Advances in both analog and digital technology offer content owners new opportunities for distributing their works and offer consumers new means for receiving and enjoying these works.[2] Such advances, however, also pose a serious challenge: how can works be protected in a world where: (i) duplication is easy and inexpensive, (ii) every copy made (whether from the original or another copy) is perfect, and (iii) distribution to users around the world can be accomplished virtually cost-free and immediately over the Internet? This challenge is particularly acute in today's world where an individual consumer no longer simply receives works, but can also send and re-distribute such works to others. Further complicating the challenge of protecting works is the fact that copyrighted works now flow in an environment that encompasses consumer electronic devices, computers, satellites and global networks such as the Internet.

As lawmakers, content owners, and consumer electronics and computer (both hardware and software) manufacturers have struggled to meet this challenge, several issues have become clear. First, neither technology alone nor legal measures alone can provide a viable solution. Second, the development and implementation of copy protection technologies and structures requires co-operation and compromise among the content, consumer electronics, computer and other relevant industries. Third, copy protection must address two key issues: (i) the treatment of works within devices (e.g. individual players, recorders, or computers), and (ii) the treatment of works as they move among devices (e.g. from a set-top box to a television set to a recording device) and over wired or wireless networks (e.g. the Internet). Fourth, the implementation of copy protection must take into account reasonable consumer expectations and cost considerations. Fifth, copy protection technologies and structures need to take account of the innovation, speed and openness that has marked the computer and Internet revolution. The challenge of providing adequate protection for works is both difficult and complex; similarly the solutions are neither simple nor one-dimensional.

Current efforts at building copy protection structures have demonstrated the need for a three-pronged approach. The first prong involves the development of technical protection measures and the making available of such measures on reasonable terms. The second prong consists of laws that support protection technologies and prohibit the circumvention of such technologies. The third prong involves cross-industry negotiations and licenses of technical protection measures. These licenses impose obligations to ensure that when access is granted to works protected by the technical measures, appropriate copy control and usage rules are followed. This paper will examine all three prongs and describe why all of these elements are necessary.

---

1 The authors have participated actively in the legislative and technology licensing issues discussed in this paper. Mr. Marks has participated on behalf of Time Warner from the perspective of the content owning industries and Mr. Turnbull on behalf of his client, Matsushita Electric Industrial Co., Ltd., from the perspective of the consumer electronics industry. The views expressed in this paper, however, are strictly those of the individual authors and do not necessarily reflect their respective companies' or clients' positions.

2 The focus of this paper is on audiovisual works and sound recordings. Similar concerns, however, exist for text and literary works (including computer software) and some of the general principles discussed in this paper may apply in those contexts.

In order to give context to these issues, we will briefly describe some of the developments that have given rise to the challenge in the first place. We will then examine the three prongs on a general level. In our discussion of the second prong, we will set forth our views as to how the anti-circumvention provisions of the two WIPO treaties should be implemented. Thereafter, we will describe in some detail a number of copy protection technologies and structures that have recently emerged or are under development and negotiation. Although many policy, technical and even legal issues remain unresolved, the work accomplished to date has yielded some concrete results as well as guideposts for moving forward.

BACKGROUND: TECHNOLOGY DEVELOPMENTS THAT POSE THE CURRENT CHALLENGE TO PROTECTING WORKS

Developments in technology often prove to be a double-edged sword to creators and content owners. On the one hand, they provide more sophisticated tools for the creation and legitimate dissemination of works. On the other hand, these same technologies often facilitate unauthorized reproduction and distribution of works in violation of content owners' rights. This dilemma is not new; it began with the introduction of the printing press. In recent years, however, certain advances in technology have added a dramatic new dimension to this dilemma. These advances include the following:

Digital Copying: Analog copies of audio and video works degrade in quality with each generation. Thus if a person makes a copy of an analog videocassette and gives it to a friend, that copy will not be as good as the original. A further copy made from that copy would be of even poorer quality. Analog technology thus contains an inherent bar against multi-generation copying that serves as an obstacle to massive unauthorized consumer copying. Digital copying, however, involves bit-for-bit replication. This means that every copy is perfect and perfect copies can be made from other copies through endless generations. Moreover, digital copying can be done at very high speeds with no loss of quality. The threat of unauthorized copying is therefore much more dangerous with the advent of digital copying. Currently, the ease with which an analog signal can be converted into digital format and then disseminated rapidly means that analog delivery also presents challenges and must be taken into account in copy protection efforts.

Compression: Audio and video works when converted to full-resolution digital form comprise vast amounts of data. Prior to digital compression technology, such works required substantial bandwidth or very long periods of time to deliver across a network. Compression technologies, such as MPEG-2 for video and MP-3 for music, have altered this situation. Some compression technologies currently allow perfect "lossless" copies to be created that are less than 25% of the original digital size. This means that these copies can be delivered in one quarter of the time it took to deliver the uncompressed originals. New compression techniques are predicted to allow for nearly lossless copies at 5% of the original size. More importantly, some compression methods make a slightly degraded "lossy" copy. These copies, while not perfect replicas of the original, usually have flaws that are imperceptible to the viewer or listener. Today, typical lossy compression provides copies that are less than 2% of the original digital size, with future projections running at 0.5% of the original. These vast advances in compression technology mean that it will become increasingly easier, faster and more convenient to transmit full-length high quality audio and video works over networks such as the Internet.

Bandwidth: Increases in bandwidth mean greater capacity for delivering more data more quickly. Cable modem and high-speed DSL phone lines are becoming available to consumers for their Internet connections. These services provide delivery of data that is roughly 9 times faster than that provided by the common 56K-baud telephone modem. Some predict that bandwidth capacity will eventually increase to the point of providing speeds that are several hundred times greater than today's common modem. These advances in bandwidth will make it vastly easier to distribute works in high quality to many people with little time or cost factor.

Networking: As more and more people go "online" and get connected to the Internet, they experience two-way links from the external world to the home and out again. Networking of personal devices in the home (such as personal computers, televisions, recorders, and music systems) is increasing as users demand more interactivity in the devices that they purchase. This allows users both to receive and to send works from home as well as move works among the different devices in their home (e.g. from a personal computer to a digital recorder). Such networking makes it easy for non-professionals to make and distribute multiple, high-quality copies of audio and video works. Indeed, every consumer that is hooked up to the Internet can become an unauthorized re-publisher and syndicate works.

The above advances in technology mean that content piracy no longer requires dedicated pirates using expensive equipment to reproduce works and physical distribution channels (from flea markets and street corner sales to retail shops) to distribute such unauthorized copies. Today an individual consumer with a few thousand dollars of home equipment can make and distribute an unlimited number of high quality unauthorized copies of works.

FIRST PRONG: TECHNICAL PROTECTION MEASURES: MEETING THE CHALLENGE POSED BY TECHNOLOGY WITH TECHNOLOGY AND THE LIMITS OF COPY PROTECTION TECHNOLOGIES

A phrase, coined by Charles Clark, that has often been repeated in policy forums is that "the answer to the machine is in the machine." Indeed a variety of technical measures have been developed to assist in the protection of works. These measures are briefly described on Annex A. While it is true that existing technical measures and new ones under development can be used to address some of the concerns posed by the advances in digital and analog technology described above, copy protection technology alone is not the answer for several reasons.

First, technical protection measures—no matter how strong—will always be vulnerable to attack by dedicated hackers, especially because the processing capabilities of computer hardware and software continue to increase rapidly. Therefore, there must be legal safeguards against the circumvention of copy protection technology. Moreover, there are real economic constraints on the strength of technical protection measures that can be implemented in copyrighted works and playback devices. Technical protection measures therefore cannot prevent piracy by resourceful individuals or organizations. Rather, they can serve basically just "to keep honest people honest"—to facilitate respect of rights in works—and to pose an obstacle to those who seek to violate such rights.

Second, content owners reap value by having their works seen, heard and read by audiences. Creators generally want people to experience their works and investors and creators alike depend upon wide audiences of legitimate, paying consumers to support the creation and distribution of works. Creative works are not like gold; there is no value in locking them away in a sealed vault. Therefore, copy protection technology must be implemented so as not to interfere with the legitimate distribution and communication of works to the public. This imperative vastly increases the complexity of developing and using copy protection technology. It means that for all practical purposes copy protection measures cannot be unilateral. Sound recordings and audiovisual works can only be enjoyed by the use of receiving and playback devices, such as television sets, CD or record players, videocassette players, personal computers, etc. Content owners thus cannot apply technical measures to their works that will cause all receiving and playback devices to be unable to receive or play the works. Equally important, the goal of protecting works cannot be achieved if receiving, playback and recording devices do not recognize and respond to copy protection technologies, but simply ignore them. Therefore, to work properly copy protection technologies must be bilateral–the technologies applied by content owners need to function with consumer electronics and computer devices used by consumers and these devices need to respect and respond to the technologies applied. This bilateral requirement means that solutions are not simply a matter of technological innovation. Rather, effective copy protection technology requires a high level of agreement and implementation by both content providers and manufacturers of consumer electronics and computer products. This can be achieved by legislation, whereby certain types of devices are required to respond to a particular copy protection technology, or by negotiated cross-industry agreements.

Third, implementation of protection technologies can be limited severely by the problem of an already existing and installed base of consumer devices that cannot function with such technologies. For example, music on CDs is not encrypted. If record companies began to encrypt the music on CDs, they would not play on the CD players that consumers currently own. The ideal time to implement copy protection technologies is with the introduction of new formats or delivery systems, such as DVD or digital broadcasts.

Fourth, content that is already out in the market place without copy protection technology cannot be protected retroactively with technology. Yet, this unprotected content can be manipulated fairly easily to take advantage of advances in copying and delivery technology. Thus, for example, consumers can now record music from CDs onto blank discs or upload it to the Internet. Obviously, such activity violates laws related to copyright and related rights. The point, however, is that there is little—if anything—that technology can do to solve this particular problem.

In addition to the limitations described above, it is unlikely that technical protections will be implemented in all environments and with respect to all formats. Therefore, strong legal regimes of copyright laws and related rights laws backed up by effective enforcement and remedies remain indispensable. The Global Business Dialogue on Electronic Commerce ("GBDe") recently acknowledged this imperative[3]. In the principles and consensus

[3] The Global Business Dialogue on Electronic Commerce (GBDe) constitutes a worldwide collaboration among companies engaged in the field of electronic commerce. Several hundred companies and trade associations have participated in the GBDe consultation process; the representation is both geographically and sectorally diverse.

recommendations issued by the GBDe in Paris in September 1999 with respect to intellectual property, the GBDe urged the following:

"Electronic commerce will not develop to its fullest potential until problems with enforcement of copyright laws are resolved.

Government action required:

- providing rightholders with effective and convenient means of pursuing copyright enforcement actions in each jurisdiction where infringement occurs;
- encouraging the improvement of judicial proceedings, remedies, and workable liability rules for copyright infringement in all countries, in order to achieve effective enforcement and deter infringement; and
- promoting a copyright awareness program among public, industrial and educational organizations to educate users on the importance of copyright protection and compliance with copyright laws, which together foster creative activities."

We have established that technology alone cannot answer the challenge of protecting works from massive unauthorized copying and distribution in the new environments. We have also established some of the difficulties involved in implementing copy protection technologies. These limitations indicate that particular legal safeguards must be provided to support copy protection technologies.

SECOND PRONG: LAWS THAT SUPPORT PROTECTION TECHNOLOGIES: THE NEED FOR EFFECTIVE ANTI-CIRCUMVENTION LAWS AND IMPLEMENTATION OF THE WIPO TREATIES

Technological protection measures require appropriate legislative and legal support: (i) to ensure that these measures are respected, and (ii) to deter the defeat of such measures by parties that might otherwise violate the rights of content owners. This imperative was recognized in both the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. Article 11 of the WIPO Copyright Treaty provides:

"Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

Article 18 of the WIPO Performances and Phonograms Treaty contains a parallel provision.

While the WIPO Treaties set forth the general prohibition against the circumvention of technological protection measures, debate has ensued over how this general principle should be implemented in national law. Much of this discussion has focused on three issues: (i) whether the prohibition should extend to devices as well as conduct, (ii) whether equipment should be required to respond to particular protection measures, and (iii) what are the appropriate exceptions to the prohibition on circumvention. We believe that in implementing the anti-circumvention provisions of the two treaties, the Digital Millennium Copyright Act of

1998 ("DMCA") adopted in the United States resolved each of these issues in an appropriate manner. We do not intend to describe the DMCA in great detail here; rather we will draw on the DMCA's concepts and solutions in our discussion of the three issues and our views as to the elements necessary for effective and balanced anti-circumvention laws.

Conduct vs. Devices

The anti-circumvention provisions of the two WIPO treaties are silent as to whether they apply just to circumvention conduct or also to devices and services that are designed or distributed to defeat protection technologies. For several reasons, a "conduct only" approach is insufficient. Circumvention conduct is generally not public; individuals usually undertake it in the privacy of their homes or workplaces. While the results of such activity, such as a software utility program that "hacks" a copy protection measure, may be made public, the conduct leading up to the cracking of the protection system is usually private. It is neither feasible nor desirable to undertake systematic monitoring of private conduct to deter circumvention activity. In any event, most people will not undertake the time and effort to crack a copy protection measure on their own. If, however, people can legally purchase (or receive for free) devices or services that defeat these measures, then it becomes much more difficult to maintain the integrity and fulfill the purpose of protection technologies. This concept is not novel. Many countries, for example, prohibit the manufacture, sale or distribution of pirate "smart cards" or black boxes that are used to decrypt and receive conditional access satellite or cable television broadcasts without authorization or payment. Therefore, to provide effective remedies against circumvention, the law needs to proscribe devices and products that are produced or distributed for the purpose of circumventing protection technologies.

The GBDe has also recommended that national legislation implementing the two WIPO treaties should "prohibit harmful circumvention related activities by regulating both conduct and devices, while providing appropriate exceptions . . . that would maintain the overall balance between rightholders and users." (emphasis added)

While effective anti-circumvention laws need to apply to devices and services, setting the boundaries as to what devices and services should be prohibited is not simple. The cases at the extremes are relatively straightforward. So-called "black boxes" that serve solely, for example, to decrypt television signals without authorization (i.e. circumvent encryption access control) or to strip out copy protection measures are devices that should clearly be illegal. General personal computers, at the other extreme, are sometimes used by hackers to crack copy protection measures that are implemented in software. Despite the fact that such computers are sometimes put to such an illicit use, the computers themselves should not be prohibited as circumvention devices because they generally serve overwhelmingly legitimate purposes and functions. The problem is where to draw the line between these two extremes.

Most people would agree that incorporating a clock into a "black box" should not legitimize the device simply because the time keeping functions of the clock portion of the device are legitimate. However, many would argue that a device that permits analog video content to be playable through a computer which device also results in the elimination of copy control flags from the content should be permissible. We believe that the DMCA achieves the appropriate balance in this difficult area. It does so by first establishing three alternative tests for determining whether a service or device should be prohibited as circumventing. Further it provides that this test may be applied to parts or components of a device or service, and not

just to the service or device as a whole. Hence, a service or device—or part or component thereof—that falls into any one of the following categories is prohibited:

- it is primarily designed or produced to circumvent;
- it has only limited commercially significant purpose or use other than to circumvent; or
- it is marketed for use in circumventing.

A device, service, part or component that falls into any of the three above categories is prohibited and may not be manufactured, imported, sold or otherwise distributed. The second part of the balance comes in the "no mandate" provision discussed below. This approach can serve as a useful model for other countries as they implement the WIPO treaty anti-circumvention provisions in their national laws. We believe that an approach along these lines to anti-circumvention law is necessary to provide adequate legal support to technical protection measures.

Response to Particular Protection Technologies

Copy protection technologies currently fall into two general categories: measures that control access to content, such as encryption, and measures that control the copying of content, such as SCMS or Macrovision.[4] Access control technologies, such as encryption, generally pose clear-cut situations for the application of anti-circumvention laws. If content is encrypted, a playback or record device can either pass along the content in encrypted form without descrambling it, or the device can decrypt the content to make it viewable or accessible to the end user. Such decryption cannot occur by accident. Decryption requires affirmative action by the device to "unlock" the controls on the content and make it accessible. Therefore, decryption without authorization constitutes circumvention.[5]

Technologies that control the copying of content, such as copy control flags, pose more complex questions with respect to the application of anti-circumvention laws. This is because the successful operation of such technologies generally depends upon a response from the playback or record device. With encryption, if the playback device does not affirmatively respond to unlock—decrypt—the content, then the content remains encrypted and protected. With copy control flags, however, if the device does not affirmatively look for and respond to the flags, then the content is not protected and subject to unauthorized copying.

Some of the leading copy protection technologies in use today, such as SCMS and Macrovision, are not effective with personal computers. It is not so much that computers override or remove these protections, rather it is more that they do not "look for" and respond

---

4 See Annex A for descriptions of encryption, SCMS and Macrovision.

5 All of the copy protection structures described below that have been recently implemented or are under negotiation across the industries rely on encryption of the content as the foundation. This is precisely because content that is encrypted cannot be decrypted "by accident". Manufacturers of legitimate products that choose to participate in the copy protection structures "sign up", get a license and agree to follow copy protection rules as a condition for obtaining the keys to decrypt the content. Decrypting the content without authorization (i.e. without a license) clearly constitutes the type of activity that anti-circumvention laws must, in general, prohibit.

to them. The computer industry has strongly resisted the idea of any legislative mandate that would require personal computers to be designed so as to look for and respond to particular flags or copy control bits. The computer industry particularly objects to the notion of a computer being obligated to screen all incoming streams of data for such flags or bits. This concern is amplified by the possibility that computers might need to respond to any and all copy protection technologies that any content owner might choose to adopt. This latter concern is also shared by the consumer electronics industry.

Hence a key issue that has emerged in the debate over the scope and requirements of appropriate anti-circumvention laws is whether failure to respond to a particular copy protection technology constitutes circumvention. Equipment manufacturers understandably do not want to be responsible for ensuring that their devices are able to respond to a variety of known (and even unknown) copy protection technologies. Content owners, on the other hand, justifiably believe that equipment manufacturers should not be permitted to design their products purposefully so as to avoid or ignore copy protection technologies. This thorny issue was resolved in the DMCA by enactment of the so-called "no mandate" provision. This provision clarifies that the prohibition on circumvention devices does not require manufacturers of consumer electronics, telecommunications or computing equipment to design their products or select parts and components affirmatively to respond to any particular technological measure, so long as the product or part does not otherwise fall within the prohibitions of the three alternative tests described above (i.e. primarily designed or produced to circumvent; only limited commercially significant purpose other than to circumvent; marketed for use in circumventing).[6]

Appropriate Exceptions

National laws generally provide for certain limitations and exceptions to the rights of authors and related rightholders, such as for fair use/fair practice. The Berne Convention and the two WIPO treaties adopted in 1996 set forth parameters for exceptions to and limitations of rights. In general, these exceptions and limitations may only be provided for "in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author" or related rightholders.[7]

A concern has been frequently expressed that the development of technical protection measures will lead content owners to "lock up" their works and prevent users from exercising legitimate exceptions to the rights of content owners. This concern may be alarmist for several reasons. First, content owners generally depend upon wide public consumption of their works. Thus, even if certain versions or formats of those works are secured with protection technologies, these technologies must be transparent enough to permit easy access for authorized uses. Second, ensuring the availability of works for public purposes, such as libraries, archives and schools can be readily addressed through licensing arrangements or even particular laws. Restrictions on technical protection measures are not a necessary (or

---

6 Our discussion here relates only to anti-circumvention laws. In some cases, other laws will require that equipment be designed to respond to particular copy control technologies. The DMCA, for example, contains a provision that requires analog VCRs to respond to Macrovision.

7 See Articles 9(2), 10 and 10 bis of the Berne Convention, Article 10 of the WIPO Copyright Treaty and Article 16 of the WIPO Performances and Phonograms Treaty.

even a very effective) method for addressing such issues. Moreover, technical measures can work with whatever economic model is applicable to the content and a particular user. Thus, for example, libraries may obtain low cost or even free licenses of content where technical measures actually help to accommodate such licenses by allowing the library use but preventing unauthorized copying and re-distribution of the content. Third, it is unlikely that technical protection measures will be applied to all formats. Finally, technical measures can actually facilitate certain exceptions and limitations to the rights of content owners, through, for example, "copy once" technology that allows consumers to make a single copy of a work. It would seem prudent to exercise restraint with respect to permitting exceptions for the circumvention of technical measures until the market for technical measures is better developed and unless specific problems arise.

The WIPO treaties do not specifically provide for exceptions to the obligation to provide adequate legal protection against circumvention. Any possible exceptions to anti-circumvention law should be narrowly crafted and restricted to special cases that do not defeat the normal functioning and application of protection technologies and do not unreasonably prejudice the legitimate interests of content owners in employing such protection technologies. Because devices and services, by their very nature, cannot be restricted to particular uses, exceptions to anti-circumvention laws do not appear well suited to devices and services. Rather, they are better considered in relation to certain types of individual conduct and subject to a set of reasonable conditions. Legislators should be cautious and use parameters such as: (i) the general availability of works (not of individual formats), (ii) the impact that any possible exception to anti-circumvention rules may have on the value of works and the efficacy of protection technologies, and (iii) the existence of licensing agreements between rightholders and public libraries and archiving institutions, when considering possible exceptions. Finally, legislators should also look at copying opportunities that are in practice being built into copy protection structures under development. Technical measures may be useful in facilitating certain exceptions and limitations to the rights of content owners. If this works out in practice, then there is little need to provide for exceptions to the general rule against circumvention of such measures.

The DMCA provides for some narrowly drafted limitations of and exceptions to the general prohibition on circumvention. First, the prohibition on individual circumvention conduct only applies with respect to access protection technologies and not to technologies that prevent copying. Other limitations and exceptions are provided for: (i) law enforcement and other governmental activities; (ii) non-profit libraries, archives and educational institutions solely to determine whether they wish to obtain authorized access to works; (iii) reverse engineering solely to achieve interoperability; (iv) encryption research and security testing; and (v) protection of privacy and minors. The foregoing exceptions are narrowly tailored and contain conditions that aim to maintain a balance and prevent the exceptions from nullifying the general rule against circumvention.

Each country has its own particular concerns regarding exceptions and limitations. We believe that such concerns need to be considered carefully. Technical measures and circumvention devices are blind as to whether the circumventing purpose is lawful or unlawful. Any possible exceptions and limitations to the anti-circumvention rule should apply to certain types of defined, individual conduct. Prohibitions against circumvention devices and services need to remain firm and cannot be undercut. To date technical protection measures have not prevented fair use or fair practice with respect to works and there has been no demonstration that such measures will have this effect in the future. Our work in the area of technical protections has led us to conclude that anti-circumvention laws must provide

effective deterrence against and sufficient remedies to redress circumvention. Strong and effective laws in this area are essential because technical measures can do no more than serve as obstacles to unauthorized use and such measures will always be subject to defeat.

The copy protection structures described below in this paper depend upon technologies and license agreements. Effective anti-circumvention laws are essential for ensuring that these structures and agreements are not undermined by parties that either choose not to participate in the agreements or to breach such agreements. The laws should encourage participation and adherence to these structures and agreements and avoid permitting those who choose not to participate to compete unfairly by defeating technical protection measures. Because works and protection technologies cross borders with increasing frequency, correct and rapid implementation of the WIPO anti-circumvention provisions by as many countries as possible is vital.[8]

THIRD PRONG: CROSS-INDUSTRY NEGOTIATIONS AND LICENSES: THE DEVELOPMENT OF COPY PROTECTION STRUCTURES

While technical protection measures serve as the first prong of copy protection structures, we have described how a variety of real world limitations prevent technical measures from providing a complete solution. We then discussed the second prong of copy protection, namely legal measures and in particular anti-circumvention laws. We explained why strong and effective anti-circumvention laws are necessary to support the efficacy of technical measures. Now we turn our attention to the third prong of copy protection: cross-industry agreements and structures whereby technical protection measures are implemented and rules for the proper treatment of content are established through the use of commercial licensing arrangements.

Early Efforts

Early attempts at implementing copy protection measures were somewhat narrow in scope. One example is the SCMS[9] system developed for digital music, which allows unlimited first generation copying of digital recordings, but prevents second generation or serial copying (i.e., unlimited copies made from the original permitted, but no further copying from those copies allowed). Worldwide implementation of SCMS emerged from negotiations and eventual agreement between record companies and consumer electronics manufacturers in 1989. In some countries, such as the United States, laws were eventually enacted that required consumer electronics devices to respond to SCMS. Nevertheless, the agreements and laws concerning SCMS failed to include the computer industry. Thus, personal computers that today are capable of playing and recording digital music are not obligated to adhere to SCMS.

---

[8] A recent example justifies this urgency. The encryption system for protecting DVDs was recently hacked in Norway and posted on a website from a server located in Norway. Yet, Norway—along with many other countries—has not yet enacted anti-circumvention laws as prescribed in the WIPO treaties.

[9] See Annex A for description of SCMS.

Another example is the encryption of certain television broadcasts, notably cable and satellite broadcasts. Encryption was developed for such broadcasts to help ensure that only those consumers who are authorized (i.e. pay for their subscriptions) are able to decrypt the broadcasts and view the programming. As currently applied by satellite and cable companies, the encryption technology protects the programming only until it reaches the authorized consumer's set-top box. Once the signal is decrypted, the content is available to the consumer with no further technical protections against unauthorized copying or re-distribution.

Current Realizations and General Principles

Current attempts at devising and implementing copy protection structures seek to address some of these shortcomings. Content owners realize that it is important to provide some measure of protection across environments: physical media, broadcast, Internet, etc. They also understand the need to work with the consumer electronics industry, computer industry, broadcast industry and eventually the telecommunications industry to develop and implement protection technologies and content use rules. These realizations have led to the following set of general goals and principles that guide current copy protection efforts:

Voluntary participation in the copy protection structure. Content providers should not be required to use copy protection technology. In general, device manufacturers should be free to choose whether to participate in a copy protection structure. If, however, they decide not to participate, then their products must neither circumvent nor interfere with copy protection technology.

Content needs to be encrypted. Encryption of content is key for distinguishing clearly between authorized uses and unauthorized uses, especially in computer environments. No individual or device can decrypt content "by accident". Hence, encryption of content is the keystone of current copy protection efforts.

Copy protection rules imposed by encryption/decryption license. Encryption of content and decryption of content requires a license of the relevant encryption technology. This license will include obligations concerning what copy protection rules must be followed (e.g. no copies allowed, one copy allowed, etc.) as a condition for decrypting the content and making it accessible to the user. Copy protection rules need to strike a balance between the rights of content owners and reasonable consumer expectations. Once content has been encrypted, any licensed device that decrypts the content takes on the contractual obligations established by the license to respect the copy protection rules. Ideally, content should be watermarked with the copy protection rules and terms of use of the content. Any unlicensed device may transmit or pass on encrypted content without restrictions, provided such device does not decrypt or otherwise make the content accessible. Any unlicensed device that decrypts the content violates anti-circumvention law (as well as any proprietary rights of the owners of the encryption technology).

Application to devices and systems. Effective copy protection requires application of technology and copy protection obligations to all devices and services that are capable of playing back, recording and/or transmitting protected content. Given the realities of the networked environment and the Internet, all devices and "way stations" of delivery systems must maintain content as securely as it was received and neither circumvent protections nor release content to the next device or component in the clear. This means that such devices and systems may not pass content which has been legitimately decrypted through either

analog or digital connections to other devices and systems without the appropriate protections.

Record and playback control. Devices and systems should not read back (i.e. play or display), from recordable media, content that is watermarked as "no copy."[10] If a "no copy" watermark is present on recordable media, this means that the recording was unauthorized in the first place. Similarly, there should be no read back from any copy of content that is marked "copy once" beyond the single authorized copy. Ideally, recording devices should read and respond to watermarks and refuse to copy content that is marked "no copy".

Availability of technologies on reasonable and non-discriminatory terms. Technical protection measures need to be made widely available on fair and non-discriminatory terms for implementation by all relevant parties (e.g. hardware manufacturers, content owners, and system operators)

Sustain meaningful protection. Copy protection systems and technologies need to provide meaningful protection for works on an on-going basis. Therefore, such systems should allow for the revocation of compromised or cloned devices. Further, the technologies embodied in these systems should be renewable so that a single hack does not destroy the efficacy of the system.

While stating the above goals and principles is relatively straightforward, implementing them into real life copy protection structures has been far from easy. We now examine in some detail the development and implementation of some of these structures, beginning with DVD (Digital Versatile Disc) video.

Introduction of DVD Video

The introduction of DVD video set the stage for some of the current approaches to implementing copy control technologies. DVD video provides high quality video on a convenient 5-inch disc format that is resistant to wear and damage and allows for attractive consumer features, such as multiple foreign language versions. The DVD was developed and designed to be playable by both consumer electronics devices and personal computers. Both the consumer electronics and computer industries were eager for the introduction of this new format for motion pictures. On the consumer electronics side, the analog VCR market was fairly mature and DVD offered a new generation of players that could gain wide popularity with consumers and generate substantial equipment sales. On the computer side, DVD represented an opportunity for the personal computer to get into the home entertainment market as a playback device for movies. Film studios, however, were not prepared to release their movies on this new digital format without protections against unauthorized copying and distribution—particularly digital copying and distribution. Because DVD was a new format, it provided the ideal opportunity to build in copy protection technology. There was no existing installed base of DVD players or DVD drives for personal computers; copy protection therefore could be designed and built into these new devices from the outset.[11]

---

[10] See Annex A for description of watermark.

[11] Even at this ideal stage of introduction of a new format, limitations still exist. For example, to succeed in the marketplace DVD players needed to be compatible with the existing installed

[Footnote continued on next page]

Origins of CPTWG and DVD Video Copy Protection

The need for a group to facilitate copy protection discussions among these three disparate industries became evident in the spring of 1996, when the trade association representing the major motion picture studios and the trade association representing the consumer electronics manufacturers presented to the computer industry a joint proposal for legislation. This proposed legislation would have required all devices capable of digital recording of motion picture content to look for, read, and respond to certain copy protection information to be contained in the content, whether from DVD discs, other physical formats, or transmissions, such as broadcasts. The computer companies responded unanimously, immediately, and forcefully that such an approach to copy protection was contrary to their view of the appropriate role of government (i.e., not involved in the design of computer products), unworkable as a technical matter without crippling the functioning of computer products, and too insecure to warrant any special effort by the computer companies to accommodate the system.

Faced with the impending release of DVD players by various consumer electronics companies, the desire of those companies to have prerecorded DVD discs containing motion picture content, the insistence of the motion picture companies that adequate copy protection be afforded any content placed on such DVD discs, and the impasse over the legislative proposal, the three industries formed two working groups. One group focused on policy issues and one focused on technical issues, the technical group adopting the name of the Copy Protection Technical Working Group ("CPTWG"). The policy working group met a number of times but failed to make any meaningful progress on legislative approaches that would be acceptable to the computer industry and sufficient for the copy protection goals of the motion picture industry. Hence, the main action focused on the technical group.

From the first week in May through the middle of July 1996, the CPTWG and its DVD task force met nearly weekly, drawing participants from the United States, Japan, and Europe to nearly every meeting. The computer industry insisted that content be encrypted as the starting point for any copy protection structure. The consumer electronics industry initially resisted this approach, out of a concern that encryption would be very taxing to its devices, adding complexity and cost. After several meetings, however, two companies – Matsushita Electric Industrial Co., Ltd. ("MEI," manufacturer and distributor of products under the Panasonic, Quasar, and National brands) and Toshiba Corporation – stepped forward with a proposal for a copy protection method that: (i) was designed specifically for the DVD format, (ii) met the design needs of the consumer electronics industry, (iii) met the computer industry's basic criterion for encryption of the content to be protected, and (iv) would impose legally enforceable rules against unauthorized copying and transmission at a level acceptable to the motion picture industry through a private commercial licensing agreement.

The basic "design goals" that were required for this copy protection technology and licensing structure were:

[Footnote continued from previous page]

base of television sets. Therefore, the copy protection technology adopted had to provide that DVD discs played on legitimate players would be viewable on existing television sets.

Sufficient technical and legal protection to "keep honest people honest," i.e., to make it difficult for an ordinary consumer to make a copy of protected content by consumers using normal home-type products;

Sufficient technical and legal protection to prevent the easy creation of widely available and usable means of avoiding the technical and legal protections afforded by the technology and related licensing;

Implementation in both computer and consumer electronics products such that the effect is insignificantly burdensome in complexity and cost in both environments;

Technology licenses that are both sufficient to provide the necessary legal protections and low in burdens on product manufacturers and distributors; and

Transparent operation to consumers, except where consumers attempt to make unauthorized copies of content protected using the system.

Finally, a fundamental starting principle was that the technology and related licenses were not required to be used by movie or product companies. Alternative copy protection technologies for DVD video can and have been developed and deployed into the market.[12]

The technology proposal developed by MEI and Toshiba was discussed in close coordination with other CPTWG participants and was initially presented to the DVD Consortium to ensure that the developers of the DVD format would support its adoption as "friendly" to this new format. MEI and Toshiba then presented the proposal to the full CPTWG in mid-July and there ensued another three months of intense work to refine the technology and discuss the rules for its usage to ensure that the protection was both adequate from the perspective of the motion picture companies and reasonable from the perspective of the companies that would implement the technology in their products.

The technical refinements included careful evaluation of the technology by computer companies to ensure that the implementation of the decryption functions in computer software was reasonable in terms of processing power required. Since MEI and Toshiba were oriented to production of semiconductor chips and other hardware solutions for product design, the system had been initially optimized for hardware implementation. The core computer companies saw very quickly that this approach was not optimal for software decryption and that a then-standard personal computer would not be able to do the decryption in software without consuming all or virtually all of such computer's processing capabilities. Several computer companies obtained the very confidential description of the technology under confidentiality and non-disclosure agreements and set to work finding a means of adapting the technology for acceptable computer implementation. These revisions were presented to the CPTWG for discussion. The result was consensus agreement that the revised version contained sufficient protection against consumer copying. This revised version of the technology, called the Content Scramble System ("CSS"), thus became the technology upon which protection of DVD video would be built. A more detailed description of the CSS technology and how it operates is set forth on Annex B.

---

[12] The most visible of the alternatives that have been introduced was the DIVX system sponsored by Circuit City and a group of private investors.

Having agreed to use CSS to encrypt video content on DVD discs, the industries then needed to negotiate the terms upon which the content on the discs could be decrypted and played. It must be emphasized that the purpose for distributing video on DVD is so consumers may watch and enjoy the films. No consumer or business interests would be served if the content remain encrypted and not accessible for viewing. Therefore, the negotiations centered on how the content of DVD discs should be treated by playback devices (both consumer electronics and computer devices) once it is decrypted. The industries agreed, in principle, that the video content on DVD discs should not be subject to unauthorized: (i) copying, or (ii) transmission, including making the content available over the Internet.

The discussion of these principles, along with rules under which CSS might be used, was conducted within the CPTWG. The result of these discussions was that a consensus was achieved on a set of principles. The CPTWG itself had no authority to "adopt" such principles or to force anyone to use them, but they served a very important function. The open discussion leading to a consensus among all those participating in the discussion provided a roadmap for MEI[13] in producing the license for use of the CSS technology.

Before describing the particular contractual obligations of the license, it is important to understand why a license is necessary in the first place. The CSS system developed by MEI and Toshiba is proprietary; these companies engineered the technology and hold certain intellectual property rights with respect to it. Therefore, any party that wants to use the CSS technology—either to encrypt content or decrypt content—must obtain a license. The license not only gives the party the right to use the technology, but also provides the party the relevant necessary technical "locks" and "keys". Because a license is necessary to use the CSS technology, this license can impose obligations as to how the technology is used and how content should be treated once it is decrypted. To ensure that content owners, consumer electronics manufacturers and computer manufacturers would actually use the CSS technology, it was crucial that a consensus be reached by all three industries as to the obligations imposed by the license.

Because of the consensus reached in the CPTWG on certain principles, MEI was assured that there was a reasonable likelihood that a license for this technology based on these principles would be accepted by participants in the new DVD video marketplace. Within days after the CPTWG meeting at which consensus was achieved, which was itself days after the final consensus that the revised encryption technology was acceptable, MEI produced the initial "interim" license document, and companies were able to produce both DVD discs containing encrypted movies and products that would both play the movies for consumer enjoyment and protect that content from unauthorized consumer copying.[14]

The CSS Technology License

Two features of the license for this technology made it unique – first, it is offered on a royalty free basis, with a small administration fee collected to offset the actual costs of managing the license system; and second, the long-term licensing of the technology will be

---

13 MEI has acted as licensing agent for both itself and Toshiba in licensing the CSS technology.

14 Although the initial interim license was produced very quickly, the longer-term interim license took many months of negotiation to achieve agreement among the affected parties on a final set of usage and copy protection rules.

turned over to an organization owned and governed by the licensees of the technology, including content owners, computer product implementers, and consumer electronics product manufacturers. While it has taken substantial time and negotiation to finalize the governance procedures under which this multi-industry body will operate and the terms and conditions of the final license to be offered through this organization, the corporate and licensing documents are nearly finalized, and the long-term licensing through the multi-industry licensee owned body is expected to start in the near future.

Copy Protection Functional Requirements. The CSS license issued by MEI imposes a series of obligations on licensees with respect to how content encrypted with CSS must be protected once it is decrypted. Companies producing licensed playback products are required by the license agreement and related specifications to employ certain defined techniques to maintain the protection of the content as follows:

The first task is to keep consumers from accessing the decrypted content during the playback process.

In the computer playback environment, decrypted content may not be placed on user accessible busses while it is in the MPEG encoded form. As a future requirement, content will not be permitted on user accessible busses even after MPEG decoding, due to the ready availability of MPEG encoders for consumer applications. In the short term, the idea is that an MPEG encoded stream of content could be manipulated within a consumer computer such that a copy could be made of the content – hence, the requirement that MPEG encoded content not be readily available on busses normally accessible to consumers. MPEG decoded data streams are sufficiently large and cumbersome for a normal consumer to manipulate that at the time the license was negotiated, there was no need to forbid normal consumer access to these data. At the point—rapidly approaching—at which MPEG encoders are readily available to, and easily used by, consumers and at which it is non-burdensome to keep the decoded content off of consumer accessible busses within the computer environment, the specifications require that computer manufacturers keep this content off of consumer accessible busses.

Equivalent requirements were not initially required in the consumer electronics environment, due to the fact that consumers do not normally modify the functioning of consumer electronics devices from that which is set by the manufacturer. To prevent possible modifications, however, the requirements will be amended in the near term to require even consumer electronics products from having MPEG encoded, decrypted content on consumer accessible busses that may exist within such devices and to forbid such devices from being manufactured in a manner such that the MPEG encoded, decrypted content could be accessed by consumers using readily available tools.

Connections between playback devices and other products are also closely regulated by the license. Only specific connections are permitted, as follows:

Standard consumer electronics connections must incorporate specified analog copy protection technologies – the proprietary Macrovision systems where applicable, and the analog version of the Copy Generation Management System copy protection information flags for certain connections;

Digital connections have been prohibited entirely, due to the lack of consensus-agreed copy protection systems. This is expected to change in the near future, with the general

acceptance of the Digital Transmission Copy Protection technology and related license agreements.

Because computer monitor connections were already widespread in the market based on the general RGB technology, these connections have been allowed by the license agreement, notwithstanding the lack of an accepted copy protection.

Related function requirements

Regional playback control. There was a consensus that regional playback control could be implemented in the DVD video environment, and the CSS license has served as the vehicle for this particular requirement. A more detailed discussion of regional playback control is set forth on Annex C.

Recordable media playback control. As a back-up to the requirements related to preventing consumer access to data streams in an environment in which copies can be made, the CSS license prohibits performing CSS playback functions (decryption, etc.) with respect to any content contained in recordable media. In other words, CSS is technology to be used solely in relation to prerecorded content on media that is factory produced read only (DVD-ROM).

Playback control applicable to unencrypted content. While content providers are free to place their content in unencrypted form onto DVD discs of any kind, the CSS license also guards against content originally encrypted using CSS being recorded onto any type of disc in unencrypted form. Thus, if a consumer is able to access the data after decryption and record the content onto a DVD disc, the license requires that the playback system recognize the fact that this content was originally encrypted using CSS and is never to be presented in unencrypted form, regardless of the type of media involved. The initial technology for accomplishing this depends on the existence and setting of a single bit in the DVD format data, and is considered highly unreliable. The longer term system for preventing such content from being played back will rely on a watermark technology that content owners will be able to use to mark the content and that playback product licensees will be required to look for in any content presented in unencrypted form.

Robustness against attack. In order to ensure that implementations are not easily defeated by consumers, either using their own tools and methods or using programs or products created for the purpose of defeating the copy protections afforded by the technology and license requirements, the CSS license also requires that implementation of the decryption and copy protection-related functions be difficult to defeat. The precise definition of this requirement has been somewhat controversial, and there have been failures by particular licensees in their actual implementations. The easy defeat of some DVD players' implementations of the regional playback control system led to widespread flouting of the regional playback system in 1998 and early 1999. Renewed focus on the requirement by licensees, together with the availability of more prerecorded DVD movie discs coded for playback outside of the North American region, has led to better compliance with this requirement. Most recently, an insecure implementation of the decryption functions in a software playback program led to a widely publicized "hack" of the encryption technology itself, a situation that will be a challenge to this particular technology over the coming months.

Enforcement and other license terms. As indicated above, the CSS technology is currently licensed by MEI on an "interim" basis and will soon be turned over to the DVD Copy Control Administration ("DVD CCA"), as a multi-industry body controlled by licensees. As licensor, MEI has, and later the DVD CCA will have, direct rights to enforce the license and related specification requirements. As recognition that the purpose of the license is to protect content, that the technology is being offered royalty-free, and that the technology adds value to products only in relation to the availability of content that would otherwise not have been presented to this format, the content provider licensees have also been given special rights to enforce the license as "third party beneficiaries." This right has been limited to injunctive and other equitable relief (primarily oriented at keeping non-compliant implementations off of the market), but the threat of litigation from these companies has been viewed as adding a credible deterrent against non-compliance by licensees.

Further Work of the CPTWG

With the initial work completed on CSS for DVD video, the CPTWG turned to other problems. One issue concerns the protection of content being passed along digital connections between products in consumers' homes. A second issue involves the marking of content with copy protection information in a way that will securely survive normal transformations of the content in various standard ways (e.g., transforming content from digital to analog and back to digital formats).

Today, the CPTWG is an open forum for presentations concerning technologies related to the protection of digital audio and video content from unauthorized consumer copying. The group meets monthly in Burbank, California, and draws approximately 125-150 attendees to its monthly meetings. While there are regular reports on certain developments in related forums, the agenda is open, and any party wishing to make a presentation may simply show up and do so. By its nature, this is not an organization for decision-making, but rather for presentations and discussion. When its members choose to do so, the CPTWG has formed, and will presumably in the future continue to form, special working or discussion groups to focus on particular subjects. The regularity of the CPTWG meetings also serves to facilitate the scheduling of other meetings related to copy protection during the week in which the CPTWG meets. Participants in CPTWG come from all around the world, and include many smaller companies and inventors as well as the world's major companies in each of the motion picture, music, computer, and consumer electronics industries.[15]

The stated goal of the multi-industry efforts has been to come up with legal and technical means of "keeping honest people honest." These efforts have explicitly not aimed at stopping professional pirates from gaining access to copyrighted content or from producing illegal copies of works. Rather, the goal has been to devise means to cause ordinary consumers difficulty in making unauthorized copies or transmissions of protected works.

In response to the two issues of: (i) protecting content over digital connections, and (ii) marking content with survivable copy protection information, CPTWG formed two

---

[15] The music industry has participated less than the others and, as described in more detail elsewhere in this paper, has sought to rely on its own separate organization, the Secure Digital Music Initiative, to address music-specific copy protection concerns.

working groups – the Digital Transmission Discussion Group ("DTDG") and the Data Hiding Subgroup ("DHSG") – to seek technical proposals from various parties and to conduct certain tests and analyses of the proposals received. Both groups discussed among interested parties the methods they would use to evaluate proposals, drafted and issued calls for proposals, and conducted testing and other analyses on the proposals received. Neither group had the legal ability to make any kind of "selection" of proposed technologies, but both had sufficient prestige and technical capabilities that the testing, analysis, and evaluation processes achieved considerable interest and support among the various industries and companies offering solutions.

Digital Transmission Copy Protection

Formed by the merging of two technical approaches originally proposed to the CPTWG's DTDG, the Digital Transmission Copy Protection ("DTCP") system is designed to protect content during digital transmission from one consumer device to another consumer device. The system relies on a combination of authentication – device to device communication on a bi-directional digital interface to establish that each device is an acceptable "partner" in the DTCP "family" – and encryption of the content to protect it against unauthorized interception as it travels across the interface.

The system is licensed through a limited liability corporation established by the five companies that developed the technology – Hitachi, Intel, Matsushita, Sony and Toshiba. The license shares many of the features of the CSS video license – with the basic license authorizing the use of the intellectual property in the algorithm, keys and other technology owned by the LLC. The royalty and fee levels are set at essentially the levels necessary simply to recover the costs of operating the system. Finally, the basic copy protection carried forward through compliance rules requires that the content be protected securely throughout the transmission process.

Two features of the licensing for this technology are somewhat different and have caused a certain amount of controversy – the usage rules applicable to content owners desiring to use the technology to protect their content; and the secure means that must be used to protect any authorized copies that are made of content protected using DTCP.

With respect to usage rules, the DTLA has proposed a set of rules to ensure that consumers can continue to make copies of certain types of broadcasts, such as free television and basic cable programming. Potential content owner licensees of the technology are in negotiations with the DTLA to resolve issues concerning the number of copies that should be permissible and the rules that should apply to pay and other conditional access broadcasts. The DTLA and content owners agree that DTCP may be used to prevent consumer copying of content on physical media (such as DVD video), pay-per-view broadcasts and video-on-demand. Final resolution of the usage rules issue is expected soon.

Because a certain amount of copying is allowed by the DTCP system, it is recognized that any authorized copy must be protected against further copying. Otherwise, there would have been little point in protecting the content up to the stage at which an authorized copy is made. Accordingly, the DTCP rules require any authorized copy to be encrypted or part of a "closed system" to ensure that further copying can be restricted by additional license requirements applicable to the playback of the copy.

While some issues remain unresolved, including to what extent DTCP can be used to prevent unauthorized uploading of content to the Internet, it appears likely that the industries will reach an accommodation. The DTCP system has been available for license in the market for over a year and is being adopted in an increasing number of products. It has also been accepted as an ITU (International Telecommunications Union) standard and is being included in the Open Cable standard for set-top boxes. Final endorsement of the technology and its licensing terms will have a significant positive effect on its actual use in the marketplace.

Conveying Copy Protection Information – Secure Digital Information and "Watermark" Technologies

Because there is authorization for some content to be copied, it is very important that the information concerning the copy protection status of a particular piece of content be conveyed accurately, securely, and conveniently.

Initial proposals for conveying copy protection information as "associated information" (i.e., information that is associated with a particular piece of content but is not itself a part of the content or otherwise required in order to view or listen to the content) is insecure against unauthorized modification (and, hence, may be inaccurate at any particular point) and is inconvenient for at least some devices to look for. Accordingly, there has been substantial opposition, especially from companies in the computer business, to this form of conveying copy protection information.

Two approaches to conveying copy protection information have been developed to meet these challenges.

Secure Digital Data. An element of the DTCP technology is that the copy protection information concerning each piece of content that is sent through a DTCP protected interface is conveyed as a part of the encryption system itself. That is, if someone attempts to manipulate the copy protection information, the keys for the content will be altered, and the content itself will be inaccessible to the receiving device. This approach addresses all three concerns – the information is secure from attack by someone desiring to modify the information, the information is reliable when received (so long as it has not been tampered with), and the information is convenient, in that it is part of the security system itself. Content not using DTCP simply does not carry this copy protection information, and a computer is free not to look for copy protection information in such content. Computers must specially handle content protected with DTCP in any event, due to the need to decrypt it, and the copy protection information is no more burdensome than the protection system itself.

Watermarks. The second method for conveying copy protection information solves the security and reliability problems but cannot, by itself, solve the convenience problem. "Watermark" technologies convey information by hiding certain codes within the content itself. For those who know where to look and how to interpret the codes, the information can be extracted and responded to. However, it is also essential that the information not disturb the normal viewing or listening experience of the consumer. Therefore, it must be invisible except to a specially designed detector. This means that detection of the information is "inconvenient" in the sense that the product through which the content is flowing or on which it is being viewed or listened to must know to look for the watermark in that particular piece of content. Since many devices do not distinguish types of content, it provides no protection in non-participating systems.

The focus of our discussions so far has been primarily on the protection of video content (i.e. audiovisual works). We now turn our attention to recorded music. In this area, there have been two important initiatives: DVD audio disc copy protection, and the Secure Digital Music Initiative.

DVD Audio Disc Copy Protection

While DVD video discs and related playback products have now been on the market for nearly three years, the DVD audio format has not yet been commercialized. Copy protection for this format is being offered by the 4C Entity, LLC, a limited liability corporation established to offer and administer licenses for copy protection technologies developed by four companies – IBM, Intel, Matsushita, and Toshiba. Although initially it had been proposed that a minor variant of the CSS video encryption system would be offered as the base encryption for content recorded on DVD audio discs, the recent "hack" of the video technology has caused a reconsideration of this proposal. It is now likely that the encryption system used for DVD audio discs will be based on a wholly new encryption technology, not susceptible to the same hack or even the same type of hack that occurred with regard to CSS for DVD video.

The copy protection rules will be somewhat different in the case of DVD audio, as well. In recognition of the fact that consumers use audio material in a different way than they do video material, some copying will be permitted as a routine matter. The nature and extent of the copying to be permitted was the subject of careful discussion among the 4C companies and the five major recording companies. The approach to be used was announced in February 1999 at the CPTWG meeting and includes the following basic rules:

Three types of outputs will be permitted from DVD audio playback equipment – two legacy outputs (analog and IEC 958) and protected digital outputs (likely to be initially configured as IEEE 1394 outputs).

In relation to legacy outputs, copy protection will be provided by a combination of watermarks containing copy protection information and, for IEC 958 outputs, the Serial Copy Management System (required in the United States under the Audio Home Recording Act of 1992 and part of the International Electrotechnical Commission standard that is observed in the European Union, Japan, and other countries). In such outputs, the content must be delivered, in general, in "real time" (i.e. must be conveyed at the normal listening speed for the material).

In relation to other forms of digital outputs, copy protection will be required, with the DTCP technology serving as one possible form of such protection. Whatever technology is used must (1) limit the content to "CD quality" or lower sampling rates and bits lengths for the content; (2) convey the range of copy protection information necessary for the full "menu" of content provider options (see below); and (3) ensure protection of the content adequately in both the transmission and the authorized copy that is made. The protected digital interface may convey the content at whatever speed is supported by the interface (i.e., it may be at rates greater than real time and, thereby, may support recording capabilities at very high speeds).

When playing back any unencrypted disc, the playback product must search for the watermark to determine whether the copy that is made is an unauthorized one. If it finds a

watermark indicating that the content was originally encrypted using the 4C system, then the playback product must refuse to play back any disc containing unencrypted content.

Recording devices will be licensed to record using an authorized encryption system to protect the content on an authorized copy. As a condition of such license, the recording product must read and respond to copy protection information in the form of the watermark in any legacy interface and the digital information contained in any copy protected digital interface. In order to properly "respond," the recorder must determine whether the input signal itself originated from the original of the recording or from a copy of the content that was already made using the copy protection system (in which case the copy protection information would so indicate);

refuse to make a copy of any content where the input signal or information originated from a source that was itself already a copy of the material;

refuse to make a copy of any content received through a copy protected digital interface where that recorder had itself already made a copy of the material (i.e., the basic rule is that there may be one copy made per recording device where the content is sent through the copy protected digital interface); and

in any circumstance where it is permitted to make a copy of the in-coming material, up-date the copy protection information in both digital (if present) and watermark form, to indicate that the copy that is made is, in fact, a copy rather than the original recording of the material.

In allowing consumers to make copies under these rules, the 4C group intends to make the limitations on copying reasonable in terms of the normal consumer expectations and experience in relation to other audio environments. The group recognized, and the recording companies that advised the group also recognized, that consumers are accustomed to making at least one convenience copy of audio material in order to "place shift" – i.e., to have an extra copy for the car, jogging, other rooms in the home, or other locations where the consumer may be at any particular time. Any system that did not allow such a copy to be made would be faced with both considerable consumer opposition as a marketplace matter and with the constant threat of circumvention. Rather than face these problems, the group, and the recording company advisors, agreed to allow this type of convenience copying but then to use technologies in various ways to prevent additional copying.

Furthermore, the group understood the need to support legacy products and systems as a means of making its products attractive in the market. In this way, consumers would be brought more rapidly to the point of having "compliant" products that provide copy protection within the understood rules described above, rather than continuing to rely on non-compliant, legacy systems that provide no copy protection at all.

Secure Digital Music Initiative ("SDMI")

SDMI was created by the major recording industry trade associations and the major recording companies. In large part, it was a response to the MP3 "phenomenon" that swept the world in 1998. MP3 – a compression technology allowing audio content to be compressed into computer files that are small enough for easy transmission over the Internet – allowed consumers to become their own distributors of recorded music. With no protection – access or copy related – this technology created the "worst nightmare" scenario

for the music companies – that a single album would be sold once and then would be redistributed by individual consumers to everyone desiring the album, without the music company ever selling more than that single initial album.

The music companies responded by filing a lawsuit, ultimately unsuccessful, against the distribution of the product that first allowed consumers to store MP3 files in a portable manner. Even while this suit was pending, the music companies also sought to enlist the consumer electronics and computer industries in a voluntary process to develop standards and technology to restrict the unauthorized distribution of music over the Internet, while allowing authorized distribution to take place. Companies were invited to join SDMI for $10,000 each, for which the joining company was given a voice in the process of developing the standards and selecting the technologies. By late 1999, approximately 150 companies had joined SDMI, and many were sending representatives to most of the meetings.

While the "Plenary" – the body of the whole membership of SDMI – is open to all companies willing to pay the fee and sign the agreement with respect to the terms and conditions of participation, the organization is administered through the SDMI Foundation, comprised of a Board of Directors made up of representatives of recording companies (for the most part, although not entirely, the major recording companies). The power of the Foundation is limited, however, and does not extend to overriding determinations made in the Plenary with respect to the substance of the standard or the terms of any SDMI offered licenses.

The group's first priority was developing an interim standard to begin the process of regulating audio content flowing to portable devices. In order to accomplish this, SDMI formed the Portable Device Working Group ("PDWG") for the purpose of formulating an initial standard to be completed by June 30, 1999. The PDWG met an average of twice a month from February through early July and, in July 1999, issued version 1.0 of its Portable Device Phase I standard.

The standard contains three major types of protections. First, this standard requires conforming systems to be equipped with technology to detect three types of watermarked signals:

a signal that Phase I has been completed and that an up-grade to Phase II is required in order for the system to receive content marked for Phase II. The system would not have to be up-graded, so long as the consumer is willing not to receive Phase II content;

copy protection information in the watermark indicating that no copying is permitted of the content of which the watermark is a part; and

an indication that content is Phase II content, and may be permitted access to the system only if the system has been up-graded to Phase II.

Second, although all types of content (e.g., MP-3 files)—including unauthorized copies of works—are allowed to enter an SDMI compliant system during Phase I, once content has entered the Phase I compliant system, certain protections are required to be maintained. After an initial choice by a consumer that the content is to be retained within the SDMI compliant environment, any copy must be made in a protected manner (encrypted in some secure manner) and playback of the content is restricted to certain authorized outputs, essentially inhibiting the consumer from uploading the content to the Internet or sending it to devices by

means of a digital connection. The third type of protection is the promise of a more elaborate protection regime in Phase II.

SDMI has operated in general as an industry standards-making body, patterned after the techniques used to develop standards such as MPEG but not observing "full" standards-making procedures. Decisions are made when there is a "substantial consensus" of each affected industry group in support of the particular decision. The existence of such consensus is ultimately a matter determined by the Executive Director of SDMI, a person appointed by the SDMI Foundation.

In general, the SDMI standard is similar to many other standards used by industries to promote the development of certain products or systems. The only part of the SDMI standard that requires a specific technology license is the watermark. The reason for having only one technology for this purpose, and, therefore, a required license for a particular technology associated with the standard, is that inserting multiple watermarks into content is likely to result in a significant degradation of the quality of the music and detecting more than one watermark is considered to be overly burdensome on products and their manufacturers. Thus, both the content and product industries have a powerful incentive to restrict the watermark to a single technology that is uniformly used by the content companies and uniformly detected by the products receiving the content. These facts drove the SDMI PDWG to determine to select a single watermark technology to convey copy protection information for Phase I and to convey the signal that Phase I is over and that a product must up-grade to Phase II in order to receive Phase II content. The selection process involved a Call for Proposals, initial analysis of submitted technologies and licensing terms and conditions, development and implementation of a testing regime to determine which watermarks were most easily and reliably detected and to determine which watermarks had the least impact on the quality of the listening experience for the consumer.

The result was a rather longer process than had been anticipated. Nevertheless, the finalization of the watermark selection and the availability of a final standard mean that SDMI compliant products will be on the world markets shortly after the beginning of the year 2000, and the recording companies are hopeful that compliant products will then proliferate, essentially crowding out non-complying products in the process.

SDMI itself has now moved onto the longer-term effort to define a standard for Phase II (meaning essentially everything that comes after the conclusion of Phase I). This is supposed to be completed by April 2000, although the history of the Phase I process suggests that this may be optimistic. The main substantive goal of Phase II is to select a long term means of determining what content is "SDMI compliant" and of doing so on a basis that is reliable, secure, and reasonable to implement. The Phase I watermark technology will not automatically be carried forward into Phase II, although some continued use of this technology seems certain to be necessary, if only to continue to signal consumers that they should move to Phase II.

The Phase I watermark technology is a proprietary technology, developed by a particular company and licensed by that company (using the 4C Entity, LLC as it licensing agent). The costs associated with this license are a mixture of the administrative cost-recovery fees associated with the other major copy protection systems described above and the normal commercial royalties associated with a commercial technology product. The license itself also imposes certain restrictions in terms of the use of the technology – essentially designed to preserve the normal consumer practices of place shifting music that

were described above in relation to the DVD audio copy protection approaches. As a practical matter, what this means is that prerecorded commercial music for sale to consumers is not allowed to be encoded as "never copy" material, but must allow consumers at least one copy.

Conclusions

As this paper has attempted to explain, development and implementation of technical measures for copy protection is complex. Innovation of protection technologies is an ongoing process that requires a significant investment of research and development. Implementation of technical measures requires cooperation across industries. The licensing of technical protection measures for use by content owners and equipment manufacturers involves detailed negotiations to reach consensus on appropriate copy control and usage rules for content that makes use of the measures. Our descriptions of some of the current copy protection structures have demonstrated that technical measures can and are being implemented in a manner that fulfills reasonable consumer expectations and permits some consumer copying. Far from denying all opportunities to exercise legitimate exceptions to the exclusive rights of content owners, technical measures can actually help facilitate the proper use of such exceptions and limitations. Development of technical protection measures and their implementation by commercial licensing arrangements, however, are only two parts of the copy protection equation. Strong legal protections—both in terms of copyright and related rights laws and laws against the circumvention of technical protection measures—are required.

Without adequate legal protection against the circumvention of copy protection measures, those who "play by the rules" are put at an unfair competitive disadvantage. For example, manufacturers of DVD playback devices that want their devices to be able to play DVD discs encrypted with CSS must enter into a license agreement for decryption. As explained above, this license agreement imposes obligations on how the devices must operate in order to protect the content once it is decrypted. If, however, parties are free to hack and defeat CSS, then products can be made without a license that decrypt CSS and do not comply with the copy protection obligations. Unless this type of circumvention activity is clearly illegal, legitimate equipment manufacturers will have little incentive to enter into a technology license in the first place and the entire copy protection structure will collapse. The key role played by strong and effective anti-circumvention laws clearly demonstrates the need for all countries to implement the two WIPO treaties and provide for effective anti-circumvention provisions in their national laws.

[Annexes follow]

ANNEX A

BRIEF DESCRIPTIONS OF SOME EXISTING PROTECTION TECHNOLOGIES AND METHODS

Copy Control Flags: Digital bits which immediately precede or are embedded in the content that indicate whether copying is authorized. These flags can become elaborate in defining numbers of copies or length of time for viewing, etc. For flags to be effective, equipment manufacturers must look for and respond to such flags. Flags can be easily identified by content pirates and are easily stripped or ignored. The computer industry to date (at least in the United States) has not been required to look for flags and has resisted doing so.

SCMS (Serial Copy Management System): A specific method of using copy control flags that allows digital copies to be made from a master, but not from a copy of that master. Thus, second generation copies and beyond are precluded. This is accomplished by having a set of control flags on the master that are changed by the copying device during the copying process. If the copy is used for an attempted copy, the control flags are incorrect and the copy device will reject it as a master for copying. SCMS is used primarily on music CDs. Computer systems have not been obligated to comply with SCMS. Further, the use of control flags has proven to be easily compromised.

Macrovision: A signal within an analog video signal that disrupts the ability of consumer VCRs from recording. Macrovision Type I disrupts recording circuitry of analog VCRs. Macrovision Type I is compatible with NTSC and PAL video signals. With DVD, Macrovision Type II and III (two line and four line colorburst respectively) were introduced. These signals create additional degradations of the video signal. Type II and III Macrovision are compatible with the NTSC video standard only.

Encryption: Digital scrambling of the bits that make up content to prevent the content from being seen clearly until it is descrambled (i.e. decrypted). The keys necessary to decrypt are delivered only to authorized users and/or authorized equipment. This technology is widely used for all satellite broadcasting of content, including conditional access channels. Early systems relied on one repeatable encryption method, which once compromised was compromised forever. Later systems employed keys with renewable and changing encryption methods. Smart cards were provided to consumers to identify who had paid for the service and who had not. Encryption protects the content until it is decrypted (usually at a set-top box) at which point it can be copied onto other digital media (e.g. computer disc) or analog media (e.g. VCR) that may be connected to the set-top box directly or indirectly via another device, such as a television.

Identification: Unique way of identifying devices and classes of devices to facilitate Authentication and Revocation**.**

Authentication: The act of verifying a device to determine whether such device complies with a particular copy protection structure/technology and should receive protected content. If the device is verified, then authentication permits the transfer of data (content) from the sending device to the verified receiving device along a secure channel. This is usually accomplished through the use of various cryptographic techniques**.**

Authorization: Access rights given to a device once it has been successfully identified and Authenticated.

Revocation: When tampering or illegal cloning has compromised a device or class of devices, digital revocation disallows any further access rights for that device. This is accomplished by providing a list of all revoked devices to compliant devices. Compliant devices then will not Authenticate and Authorize the revoked devices. This list is updated electronically via networks and physical media to the trusted devices and does not require any physical modifications.

Watermarking: Bits embedded into the content that cannot be audibly nor visually detected, but which can be read by a detection device so that it knows whether the content being played is authentic and where the source of the content was originated. Such information can provide data on the author, rights, distribution, etc. It can also contain copy control information and instructions. A watermark can only be effective if compliant detectors that read and respond to the watermark are embodied in the playback and record devices; otherwise, the watermark will pass undetected. One of the difficulties in watermarking is that it must survive compression methods without becoming visible or audible when uncompressed.

[Annex B follows]

ANNEX B

DESCRIPTION OF CSS TECHNOLOGY AND ITS APPLICATION TO DVD VIDEO

The CSS technology itself is a combination of a private algorithm and a series of keys associated with the individual work being protected, the disc onto which the work is placed, and the manufacturer of a decryption product. In the computer application, the relationship between the DVD drive and the host computer decryption system is regulated by an authentication protocol and an additional layer of encryption of the keys as they are carried from the disc to the playback decryption module. Copy protection information is placed into the data using locations defined by the DVD format book and then utilized by the encryption program.

On the encryption side, when a movie company wishes to have one of its works protected using this system, the movie company instructs one of the companies preparing the content for the DVD format to encrypt the work. Where the movie company itself is integrated such that a unit of that company is doing the content formatting and then encrypting, the movie company itself needs to be a licensee, but where the movie company contracts with another party to do the encrypting, the movie company itself need not be a licensee. The movie company or its designee can choose unique disc and title keys, varying them as often or infrequently as they wish. The title key is used to encrypt the content, and the disc key is used to encrypt the title key. MEI retains the ox" module that encrypts the disc key. The content owner or its designee sends the disc and title key set to MEI for encrypting the key "set" using the module. These are exchanged by secure means, and the resulting information is placed onto the disc in an area that is not normally accessible to a drive not licensed for this system.

On the playback product side, any company using any of the confidential or highly confidential information in making its product must be a licensee and must take out a license for each category of the CSS specification that it requires for its product. Companies that are making the decryption product itself are assigned keys for that product. These are the keys used by MEI in the process of encrypting the key set.

[Annex C follows]

ANNEX C

REGIONAL PLAYBACK CONTROL FOR DVD VIDEO

While the introduction of DVD video was a very exciting prospect, the effect was that the distribution systems of the motion picture companies could be dramatically disrupted. DVD technology was truly global, in a format that would not change according to local differences in television standards and that would allow easy viewing of movies on televisions and computer monitors in multiple languages as chosen by the consumer. Therefore, a motion picture DVD disc released in one location would be immediately playable, and playable in a consumer friendly way, in all parts of the world. The problems with this capability were: first, that different companies often controlled the relevant rights for movie distribution in different countries; and second, that motion picture companies frequently timed the releases of the same motion picture to be different in different parts of the world. That is, a movie deemed to be a "summer movie" would be released in the Northern Hemisphere in July but held for release in the Southern Hemisphere for the following January. However, by the time the movie was released in theaters in the Southern Hemisphere, the movie was likely to be released on DVD disc for sale and rental to consumers in the Northern Hemisphere. The movie companies were greatly concerned that the effect would be that the discs released in the Northern Hemisphere would be shipped to the Southern Hemisphere and the theatrical release in the south would be greatly harmed by the influx of DVD discs playable in consumers' homes.

For these two reasons – the legal issue of control over distribution rights, and the release "window" structure of the movie business – the movie companies insisted that DVD somehow adopt a regional playback system, such that a disc released in one region would not play on playback systems used in other regions. The structure, again, would be aimed at keeping honest people honest, rather than devising a perfect regime to prevent anyone from playing a disc coded for one region on playback products sold in other regions. The situation was further complicated by the distribution mechanisms used by the product companies – that is, a manufacturer of a DVD drive for a computer or of the CPU used for a computer would not know at the time of manufacture of that product where the drive or CPU would ultimately be sold. Many computer companies have worldwide distribution and commonly ship products from one market to another as demand dictates. They argued that they could not be required to unalterably designate a given drive or CPU unit for a given region at the time of manufacture. So, the system would have to be flexible enough to accommodate this problem. Again, the CPTWG met for weeks to discuss various means of accomplishing the dual goals of the movie industry and the computer industry.

The final result was a compromise that was then recommended to those devising the legal regime to require compliance with various rules. The compromise was that computers could be reset by consumers, effectively up to 25 times by the same consumer. This approach was going to be a bit complex to design and implement, however, so an alternate approach was to be allowed for the first phase of computer DVD playback systems. In the first phase, computers could be set for a given region through a software tool that could be set at the time of set-up of the computer by the consumer, accommodating the computer companies' distribution concerns. Again, the CPTWG lacked any means of implementing or requiring the implementation of this approach. The requirements for regional playback control were therefore implemented by the CSS license. Equipment manufacturers that take a license so

that their products are able to play DVD discs encrypted with CSS are obligated by the license to provide for regional playback control in their products.

[End of Annex C and of document]