E

WIPO

SCCR/10/2 Rev.
ORIGINAL: English
DATE: May 4, 2004

WORLD INTELLECTUAL PROPERTY ORGANIZATION
GENEVA

STANDING COMMITTEE ON COPYRIGHT AND RELATED RIGHTS

Tenth Session
Geneva, November 3 to 5, 2003

CURRENT DEVELOPMENTS IN THE FIELD OF DIGITAL RIGHTS MANAGEMENT

Prepared by Mr. Jeffrey P. Cunard, Debevoise and Plimpton, Washington, D.C.;

Mr. Keith Hill, Senior Consultant, Rightscom Limited, London

and

Mr. Chris Barlas, Senior Consultant, Rightscom Limited, London

TABLE OF CONTENTS

Page

Page

Page

Page

Page

EXECUTIVE SUMMARY[*]

This study of digital rights management ("DRM") with respect to the technologies upon which it is based and the legal instruments that govern the technologies and processes in Australia, Europe, Japan and the United States of America (U.S.A.), is intended for anyone with an interest in the subject, especially those whose familiarity with digital rights management may be limited.

Although the study has been written by experts in the subject, it should be emphasized from the start that many aspects of digital rights management remain speculative. To date, there are no extensive implementations, though several types of content and content services are now using some DRM and content protection technologies. Furthermore, several of the laws governing the deployment and use of DRM technologies are recent and there is still comparatively little jurisprudence. It should be stressed, therefore, that the current study should be considered a snapshot in time and should not be taken as a definitive statement that can be relied on in future. However, it is hoped that the study will help anyone who wishes to gain some knowledge of the state of the art as it is in mid-2003.

The study opens with an introduction, providing a high-level functional description of DRM technologies, which breaks the subject down into the various functionalities a user–either a rights holder or a consumer of content–could expect to find in a DRM system. This brief description is followed by a short history of the Internet and the digital technologies that have been developed to support digital content, including technologies that enable the infringing exchange of content on networks. This leads to a brief assessment of the current situation for rights holders with respect to technology development.

The final part of the introductory section of the study sets out how traditional business models for content exploitation will be supplemented by new models, enabled by DRM technologies. These new models are exemplified by some scenarios. The section concludes with some observations about "trusted computing," which is likely to have a significant impact on the future of secure digital content transactions.

The second section provides a thorough description of DRM technologies at the present time. For the sake of simplicity, these technologies are presented as a set of components and tools, which together can be integrated into a coherent system. For the purposes of the study a distinction is made between "the management of digital rights" and "the digital management of rights." The former comprises the technologies of identification, metadata and rights languages, while the latter is concerned with encryption, watermarking, digital signatures, privacy technologies and payment systems.

This description of the component technologies of DRM is followed by a short subsection on standards and their importance to the deployment of DRM.

The third section of the study sets out the present legal framework in which DRM technologies are being deployed. Dealing first with the WIPO Copyright Treaty, and the WIPO Performances and Phonograms Treaty (hereafter the "WIPO Internet Treaties"), the

[*] The views expressed in this Study are those of the authors and not necessarily those of the Member States or the Secretariat of WIPO.

document describes the provisions on anti-circumvention technologies and copyright management information. Moving on to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), the study gives a description of the scope of the Agreement, followed by some explanation of the work of the World Trade Organization on electronic commerce. There follows analyses of the legal situations in Australia, the European Union, Japan and the United States of America. For the United States of America, the study reviews the Digital Millennium Copyright Act and other relevant legislation, including federal and state laws, as well as relevant regulatory proceedings. The discussion on the European Union reviews the Copyright Directive, including a brief summary of the state of implementation in the Member States, and other Directives, such as the Computer Program and Conditional Access Directives. In addition, some information about the European Commission sectoral workshops on DRM is provided. Each of these discussions on specific jurisdictional developments is followed by a review of the most relevant case law, if any.

The fourth section of the study opens with a quick review of the DRM stakeholders, from rights holders to consumer end users, taking in collective management societies, intermediaries and technology vendors in between. This is followed by a short subsection outlining various examples of DRM services for different content types available in the marketplace today. The section ends with a brief review of interoperability issues.

The fifth and last section reviews some of the policy issues raised by the use of DRM technologies, including those directly involving intellectual property. Other policy matters that are identified and discussed relate to privacy, questions of jurisdiction and applicable law, the role of government in standards setting and, finally, technology licensing practices.

The study concludes with a review of the role of international institutions and offers four recommendations for action that might be taken in the future.

1. INTRODUCTION

This paper describes current commercial, technical and legal developments in the field of Digital Rights Management ("DRM"). In large part, it is intended to demystify the technologies that have been developed for the management of rights and content in digital form and to help readers understand both the purpose and the application of those technologies in the real world. At the same time, the paper describes the various legal regimes that have emerged internationally and in several major jurisdictions to protect both DRM technologies themselves and the content that they manage. The paper concludes with an identification of significant current policy issues that may warrant further study.

This paper is not intended to provide an in-depth explanation of technical processes, though its authors hope that it will help non-technical people in their dealings with technical specialists. Nor is it intended to help people decide which proprietary technologies to choose, whether or not such proprietary technologies are based on standards.

In surveying the vast commercial and policy landscape, the paper neither can describe each technology available in the market for every type of content, nor can every applicable law and case be discussed.

1.1 A Functional Description of DRM

From a functional perspective, DRM means many things to many people. For some it is simply about the technical process of securing content in a digital form. To others, it is the entire technical process of supporting the exchange of rights and content on networks like the Internet. For convenience, DRM is often separated into two functional areas.

– The identification and description of intellectual property, rights pertaining to works and to parties involved in their creation of administration (digital rights management);

– The (technical) enforcement of usage restrictions (digital management of rights).

DRM may therefore refer to the technologies and/or processes that are applied to digital content to describe and identify it and/or to define, apply and enforce usage rules in a secure manner.

It is also important to distinguish between "access control," "copy protection" and "the management of intellectual property rights" highlighting their respective boundaries.

An access control system manages a user's access to content, usually achieved through some kind of password protection. However, once access to the content has been granted, no further protection is applied. Thus, once a user has access to the content, it is no longer possible to control what is done with that content. This type of protection is often employed on Websites where a simple access control mechanism suffices.

A copy protection system is designed to signal the extent of allowed copying and serial copying, if any, that is defined by the associated "usage information" with respect to any instance of delivered content, and to implement and enforce the signaled behavior in

consumer equipment. The notion of copy protection can be extended to control the movement of content within and outside the user domain, encompassing re-distribution over the Internet.

A fully enabled intellectual property rights management system covers the processing of all rights information for the electronic administration of rights, sometime including contractual and personal information, to enable end to end rights management throughout the value chain. By its nature, DRM may require access to commercially sensitive information (as opposed to copy information and usage signaling). The use of such a system will enable very granular control of content, enabling rights owners to apply sophisticated usage models.

This process of managing intellectual property rights inevitably involves the extensive use of DRM technologies. Such technologies can be embedded into many components, from those that reside on a single device, such as a Personal Digital Assistant ("PDA") to those to be found in commercial Internet Servers run by major companies and organizations.

It is the purpose of this paper to explain the range of tools that may be employed by DRM systems, show how they are applied and explain both the relevant legal principles and various of the public policy issues that are raised by their use.

1.2 Origins, Conceptual Basis and Purpose of DRM

1.2.1 The Birth of the Internet

The Internet and the World Wide Web, have roots in U.S.A. government computer research in the mid-1950s. The Advanced Research Projects Agency ("ARPA") was launched in 1950 and experienced the first networked computers in 1965. Later on, between 1967 and 1969, ARPA developed ARPANET. The project was commissioned by the U.S.A. Department of Defense ("DoD") for research into networking. A network of four computers was established, and in 1971, ARPANET was extended to 15 nodes. During the same year, Ray Tomlinson of BBN released the first email application, which was able to send and receive messages across a distributed network. In 1972, the @ sign was chosen for its "at" meaning and integrated into the BBN email application.

In 1972, a demonstration of ARPANET between 40 machines was performed at the International Conference on Computer Communications ("ICCC"). In the same year, the first computer-to-computer "chat" took place. In 1974, BBN launched the Telenet, a public packet data service that was a commercial version of ARPANET.

During the 1980s, Internet technology grew exponentially. Early in the decade, parallel networks to ARPANET were started. They included BITNET, CSNET and Minitel in France. At the same time many organizations adopted the newly introduced transport protocol, TCP/IP, which is the foundation of today's Internet. In 1983, the University of Wisconsin started to develop domain name technology. In 1984, the Domain Name System ("DNS") was introduced. This is another foundation stone of today's Internet. The first domain names were assigned in 1985.

In 1987, the number of Internet host computers reached ten thousand and in 1988, the Internet Assigned Numbers Authority ("IANA") was founded to administer the Domain Name System. In 1989, Reseaux IP Europeens ("RIPE") was formed by several European service providers, while the number of Internet hosts worldwide reached 100,000. In 1990,

"The World comes on-line (world.std.com)," became the first commercial provider of Internet dial-up access.

Perhaps the most important public milestone was the invention of the World Wide Web ("Web") in 1991. This technology was implemented by Tim Berners-Lee from the CERN laboratories in Geneva, using hyperlinks to make documents available through the Internet. The technology, originally designed for internal use by CERN, was shortly afterwards proposed to international standardization bodies. This led to today's World Wide Web standards, including HTML and HTTP, both of which are foundations of the Web as we know it today.

In 1992, the number of Internet hosts reached one million and in 1993 the first commercial Web browser, called Mosaic, was released. This was considered to be a major evolution, since it enabled non-technical people to use this new technology without any special training. During the same year, the Web was proliferating at a 341,634% annual growth rate of service traffic.

The first radio broadcast was performed over the Internet in 1994. In the next few years, technologies such as search engines and Internet phones began to appear as well as programming languages suited for the Internet, such as Sun Microsystems' JAVA.

The period between 1995 and 2003 has seen a tremendous growth of the Internet. The number of domains exploded, as did the number of Internet users. According to the Internet Software consortium, there were 162,128,493 Internet hosts in July 2002 advertised in the DNS, compared with 147,344,723 hosts in January 2002. According to OCCL, Alexa Internet and IDC, 4,400 new Websites are created every day.

1.2.2 Development of the Internet for eCommerce

In 1986, the first company operating a commercial service on the Internet was a stamp exchange, called the "International Stamp Exchange." The "electronic commerce" part of the stamp company was performed through telex terminals or personal computers. In 1996 the term eCommerce, appeared. 1998 is regarded by many as the year eCommerce really began, leading to today's wide consumer adoption of eCommerce. A recent report by research firm, Jupiter, estimates that online retail spending in the U.S.A. will increase by 28% in 2003 to US$52 billion. Jupiter also estimates that by 2007 online retail spending could reach US$105 billion and represent about 5% of U.S.A. retail spending. Online retail spending is also booming in Europe.

From a technology perspective, the use of encryption technologies, eventually released by governments for public deployment, enabled the development of secure transactions for eCommerce. The Secure Socket Layer protocol ("SSL"), developed by Netscape Communication, was the first important technology to provide security and privacy for financial transactions over the Internet, using encryption techniques. The SSL specification was introduced in 1994 with SSL version 1. In the same year, SSL version 2 was the first commercial application of the protocol. A substantially revised version was released in 1995 with SSL version 3.

1.2.3 Development of Digital Storage Media

Digital storage media (any support able to store Intellectual Property ("IP") digitally) is another fundamental technology that has been essential to the growth of eCommerce in digital goods. Digital storage media include hard drives, optical media, such as compact discs ("CDs") and digital versatile disks ("DVDs"), and various memory cards.

As the ability to store information in digital form has grown, mechanical storage, such as a physical library of audio CDs or a personal photo collection, has been increasingly replaced by digital storage. Personal computers, being very flexible in their ability to handle information, provide extensive opportunities to create individual compilations on their hard drives and writable CD-ROM drives. While this is not a problem as long as such compilations contain only the owner's personal information or creations, it becomes a real headache for rights owners when the technology is used to store large quantities of infringing intellectual property. The situation becomes even more problematic when the personal computer is linked to the Internet, because the owner's compilations can then be made available to anyone else on a file-sharing network.

1.2.4 Development of Ripping Technology

"Ripping" is a term commonly used to describe the process of extracting digital content (such as audio and video) from a CD or DVD to the owner's own media, such as a hard drive.

The development of ripping is associated with the advent of MP3, a compressed audio format (MPEG-1, layer 3 Standard), and allows users to store compressed high-quality music on a hard drive or any digital media. Originally, users ripped audio tracks from CDs to create a personal music compilation on their computers. However, as noted above, with the development of Web-based applications such as Napster, Kazaa and others, which enable users to share their collections online, the "ripping" phenomenon exploded, posing an increasingly significant danger to the owners of copyright.

Ripping is no longer limited to audio content. It is now relatively easy to copy a DVD movie onto a hard drive or one of the recently introduced DVD writers. If simple access control or copy protection has been applied to the original DVD, easily available tools exist which allow users to remove the copy protection and copy the content of a DVD onto other media. The video content can then be compressed using compression software, such as DiVX, (MPEG-4-based video compression technology), which dramatically reduces the size of a movie without losing too much quality.

1.2.5 Peer-to-Peer File Sharing

As noted above, the combination of powerful personal computers, digital storage media, network applications (such as the Web) and ripping technology provides an opportunity to transfer content from the original media to user controlled media. Once this has been done, the content can be made freely available by the user, despite the fact that it is legally protected by copyright.

The first file-sharing network to be adopted by a large number of Internet users was Napster, which started operating in May 1999. The company provided a service whereby

users were able to download software enabling them to exchange music files with other users free of charge. This was an early peer-to-peer service, in which music files were indexed on Napster's servers, allowing users to be directed to the source file. Napster was seen as the pioneer of such peer-to-peer services.

Napster was from the start exceptionally popular with users. However, shortly after it started operating, Napster was confronted with legal issues when it was discovered that its users were trading copyright files without the permission of the copyright holders. A phenomenon like this–a large community of users trading content over a file sharing network–had never previously been seen by the music industry.

Napster was sued by recording companies and music publishers for contributory copyright infringement. The court enjoined Napster and that ruling was affirmed by the appeals court. Napster went into bankruptcy and its assets were sold to Roxio, a software company.

Napster's demise did not stop other companies from providing file sharing services and software. Other peer-to-peer networks began to emerge, with technologies that did not require a central server, which made legal pursuit much more difficult. Kazaa, Morpheus and StreamCast are suppliers of software or services that enable peer-to-peer file sharing, attracting millions of users who are willing to share content on a daily basis and in huge quantities. It is currently estimated that over 2.6 billion music files are downloaded illegally every month, mainly through peer-to-peer services.[1] IFPI further estimates that 99% of all music files exchanged on the Internet are pirated files.[2] The recording industry has been litigating aggressively against these services and software suppliers, although in April 2003 a U.S.A. judge found in favor of Morpheus and StreamCast, concluding that aside from distributing software they were not contributorily liable because they did not actively and materially assist in the infringing activity of end users.[3] In early 2003, in the United States of America, the industry sued (and then quickly reached settlements with) individuals, so-called "super node" users responsible for enabling the distribution of vast quantities of content on university campuses. At the end of June 2003, it has announced that it is gathering information in support of filing possibly thousands of law suits against individuals involved in peer-to-peer file sharing.[4]

---

1 See *http://news.bbc.co.uk/1/hi/entertainment/music/2283072.stm.*

2 See *http://news.bbc.co.uk/1/hi/entertainment/music/2636235.stm.*

3 See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, CV 01-08541-SVW (April 25, 2003) (order granting defendants' (Grokster and StreamCast) motions for summary judgment and denying plaintiffs' motion for summary judgment), appeal pending No. 03-55894 (9th Cir. Filed May 29, 2003).

3 See *Recording Industry To Begin Collecting Evidence And Preparing Lawsuits Against File 'Sharers' Who Illegally Offer Music Online* (June 25, 2003 press release), available at *http://www.riaa.com/news/newsletter/062503.asp.*

1.2.6 The Situation for Rights Owners Today

The combination of powerful computers, content that can be ripped, very large storage media and file sharing has conspired to produce an extremely difficult situation for rights holders. All content is now vulnerable to illegal copying and distribution over the Internet, irrespective of media type. What began with the infringement of CD-Audio has now spread to films, books and any other type of content that can be digitized. The situation has become critical for many companies, as they see their revenue decline in the face of widespread, consumer piracy.

It is for this reason that the content industries are currently looking to digital rights management ("DRM"). Section 4 of this paper contains a generic description of such technologies, together with some information about specific initiatives supported by the content industries focusing on digital rights management and related legal and policy issues.

1.2.7 Legal Perspective–The WIPO Internet Treaties and More

Throughout the 1990s, rights holders increasingly focused on the threats, as well as the opportunities, posed by the digital technologies described above. Making content legitimately available through the Internet and other digital distribution means required security and protection for content, including DRM technologies. At the same time, the widespread use of peer-to-peer file sharing, ripping and the ease of copying and distributing content in digital files dramatically concerned rights holders and made them fearful of authorizing digital content distribution. For this reason, at the same time as rights holders and distributors considered possible technological approaches, they also focused more intently on legal mechanisms that could be used to safeguard legitimate content against unauthorized copying and dissemination.

The most commonly used legal approach, reflected in the Napster litigation described above, was to rely on copyright law to pursue those who facilitated or contributed to these practices. Rights holders generally had decided not to sue directly end users, the individuals who engaged in activities, such as peer-to-peer file sharing, that directly infringed copyright. Moreover, with respect to individuals, the status of some of their activities, such as ripping their own CDs, was legally ambiguous, at least in the United States of America, where making a copy of a work one had purchased arguably constituted a lawful fair use. Contributory infringement actions could be pursued against Napster and various other file sharing services, and rights holders–particularly the recording companies and the motion picture industry–litigated aggressively against what seemed to be an ever-increasing number of such service providers.

Starting principally in the early 1990s, rights holders, particularly in the United States of America, began to look to technology, as well as the law, to protect their works. As they considered whether and how they might develop and use technological approaches to protecting their content, they also recognized that those approaches would be ineffective unless the law itself provided enhanced protection for those processes and systems. As described below, in Section 3, legal protection for technological measures was not without precedent: various countries already gave legal protection to conditional access schemes that

were used in connection with cable and other pay television services.[5] Moreover, in the United States of America, the Audio Home Recording Act of 1992 already prohibited the circumvention of any device, program or circuit that implements a particular kind of technological measure–the Serial Copy Management System–which was used to protect digital music in digital recording and digital interface devices, such as the digital audio tape recorder.[6]

In September 1995, the United States of America Patent and Trademark Office issued a report, *Intellectual Property and the National Information Infrastructure*, which set out these themes in detail.[7] Drafted by a Working Group on Intellectual Property Rights, the report recommended that Congress enact into law an amendment to the U.S.A. Copyright Act of 1976 that would prohibit the import, manufacture or distribution of a device, product or component, or performing of a service, the "primary purpose or effect of which is to . . . circumvent, without the authority of the copyright owner or the law, any process, treatment, mechanism or system which prevents or inhibits the violation of any of the exclusive rights of the copyright
owner...."[8]

Note that this approach would have only prohibited the provision of a product, and not the actual act of circumvention. Moreover, the prohibition only applied to technological measures that would prevent unauthorized exercise of copyright rights, and not to access control measures.

In addition, the Working Group recommended that "copyright management information" be protected; any knowing removal or alteration, or knowing distribution of altered information, would be prohibited. "Copyright management" information was defined to include the "name and other identifying information of the author . . . [and] of the copyright owner, terms and conditions for uses ..."[9]

These provisions proved to be controversial. Although they were introduced in a bill, they were never enacted into law. Nevertheless, the report and these legislative proposals were the starting point for the negotiating position and draft treaty language proposed by the United States of America in the run-up to the Diplomatic Conference on Certain Copyright and Neighbouring Rights Questions (WIPO Diplomatic Conference of 1996). That Diplomatic Conference culminated in the adoption of the WIPO Copyright Treaty ("WCT") and the WIPO Performances and Phonograms Treaty ("WPPT") (together, the "WIPO Treaties"), which were signed in Geneva in December 1996. The WCT and the WPPT, and their implementation, are discussed below in Section 3.

---

5 The United States prohibits the manufacture and sale of devices that are used primarily to assist in unauthorized decryption of satellite cable programming. 47 U.S.C. § 605(c)(4). Similar provisions are found in the North American Free Trade Agreement ("NAFTA"), art. 1707(a).

6 17 U.S.C. § 1002(c).

7 Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (Patent and Trademark Office: 1995).

8 *Id.* at Appendix 1, 6.

9 *Id.* at Appendix 1, 6-7.

1.3 DRM as a Means of Enhancing Access to Online Content

In this section, the way in which the existence of the global network changes traditional models of access to intellectual property, and thus the business models of the "content industries," will be considered. From this will follow the means by which DRM technology might enable new business models, enhancing access to intellectual property in ways which are of benefit both to rights holders and to users.

1.3.1 Traditional Content Distribution Business Models

Traditional distribution value chains create value at points of scarcity. This is as true for the content industries as it is for any other producer. Intellectual property rights ("IPRs") create such a point of scarcity for their holders: creators of intellectual property (or their successors in title) are given the right, for a limited term, to control access to their content, creating a point of scarcity to the extent that the content (for whatever reason) is not effectively substitutable. If the consumer wants access to a particular piece of content, this is only possible to the extent that the rights holder has authorized the creation of points of access.

Infringements of copyright are as old as the legislation itself and the existence of copyright laws has never entirely stood in the way of people seeking to profit illicitly from others' intellectual property. Copyright has long been available to give rights holders the ability to prevent unauthorized uses of their content. Standing alone, the law cannot and could not completely prevent such uses, regardless of whether they are undertaken for illicit or legitimate ends. These include the know-how and investment necessary to create the physical media and entry to the supply chain (which is a significant barrier to, for example, piracy of books in countries with a well-developed book trade).

1.3.2 New Business Models for Networked Delivery

The development of the Internet has, as noted above, created significant challenges to any distribution model which depends on scarcity. Although there are many different ways of interpreting the statistics, by the end of 2002 there were around nine million distinct sites on the World Wide Web. It has also been estimated that over four thousand new websites are created every day. Peer-to-peer networking has made the process of making content available even more straightforward, even for the technically illiterate. Clearly the barriers to entry for publishing (in its broadest sense) and distribution have fallen dramatically. The financial and skill barriers to making content available globally have simply fallen away.

Unfortunately for rights holders, these mechanisms not only make it easy to become a legitimate publisher or user of content, but they also make it easy for people to distribute content where they have no express right to do so, whether casually or systematically, and without regard to whether the redistribution is prohibited by law. Therefore, as an increasing volume of content becomes available to users for no fee, in direct competition with legitimate paid for sources, business models which depend on scarcity begin to fail.

Although it is possible to argue that so-called "network effect economics" value ubiquity over scarcity (and there can be little doubt about this from an abstract perspective), it can prove very difficult to monetize that value–to find ways in which the value can be reified

in the value chain. If the content is widely available for nothing, it may indeed increase the potential value associated with the moment of creation and thus with the creator of the content–but how can that value be realized?

The application of technology to this problem, if it is to be effective, must therefore in some way reestablish a point of scarcity on behalf of the rights holder. However, this raises a fundamental paradox, which has not been lost on those who have attempted to implement DRM–that it is the business of publishers (a term used in the widest possible sense to include all businesses that make content of any kind and in any medium available to the public) lies in providing access rather than in preventing it.

The ultimate aim of deploying "technical measures" to manage delivery of intellectual property must be to balance the requirements of rights owners to control and protect the distribution of content with the interests of consumers to have access to that content. Naturally, consumers would rather gain access to content for nothing–why pay for anything you can have for nothing? There are also self-evidently serious problems with persuading consumers of the objective "value" of intangibles. Nevertheless, unless copyright is to be abandoned as a mechanism for trading in intellectual property entirely, it will be essential to find an answer to this paradox.

1.3.3 Some DRM Scenarios

If DRM is to be successful and overcome the ubiquity/scarcity paradox, what types of usage applications must it be able to support which are likely to prove attractive to consumers? Here are some potential scenarios:

– A consumer downloads music at home from a network service, and is given the necessary permissions to listen to this music on any device she owns for 12 months from the date of download (as often as she would like to do so); she may also pass a copy of the music to up to ten friends without charge–but they can only listen to it once without obtaining a license of their own. However, to reward her as the distributor of the protected files, she will be recompensed, either financially or in kind, by the rights holder who benefits from her distribution to friends.

– A consumer downloads a recently released movie. The permissions she is granted mean that she is allowed to watch it only three times within a one-month period. After that, the file becomes inaccessible unless a new license fee is paid. However, the permissions also provide for her to register for a free ticket to her local movie theatre any time in the month after her permissions expire.

– A student "visits" his University library from his room, which is off campus, and finds the five different journal articles and individual chapters of books which he needs to write his assignment. He downloads these to his own laptop. They are only available on "short loan," so after five days the files on his laptop become inaccessible to him. However, the library also has an arrangement with an eBook vendor, who offers discounts on a range of eBooks relevant to the journal articles. This is achieved through the use of complex metadata matching through the DRM system.

1.3.4 The Future of DRM - Trusted Computing

Today, DRM remains a fledgling industry. While the specific technologies required to provide the functionality for protecting rights and content in a digital form are increasingly sophisticated (as will be demonstrated later in this paper), take up is not wide spread. This is partly a question of rights holder confidence, partly a question of consumer resistance. It is also, significantly, connected to the very large amount of free, but infringing, content available on the Internet.

While this problem is currently being tackled by a combination of legal pursuit of pirates and the development of value added content services such as those outlined above, in future a more radical approach, using some of the technologies already developed, is going to be required. This is the reason for what is known generically as the "Trusted Computing" or "Secure Engineering" development.

Essentially, Trusted Computing is about developing microprocessor-based devices (which could include PCs, PDAs, mobile phones, televisions, hi-fi systems or any other device for rending content which is controlled by a microprocessor) that include both hardware and software for the protection of content. And here content can be any type delivered to the device, including IPR protected material or content not protected by IPR that its providers nonetheless wish to see accessed and used only under pre-determined conditions.

Several initiatives, some standards-based (e.g., the Trusted Computing Platform Alliance), some proprietary (e.g., Microsoft's Next-Generation Secure Computing Base) are currently in development. They promise to create a networked environment that is trusted, based on the secure identification of users, devices and software modules, ensuring that content can only be exploited in line with rules set by the owners of the material. While such initiatives beg a great many questions, including the issue of user privacy, the combination of software and hardware security is generally agreed to offer the best hope of an environment that is both secure and trustworthy. In such an environment, the distinction between methods for dealing with IPR-based content and content that is subject to other forms of legal protection (such as trade secret or data protection legislation) will largely disappear. However, this technology is still some way off (and, according to some, will never succeed) and for the moment, it is necessary to concentrate on specific technologies solely designed for the protection of intellectual property rights.

2. DESCRIPTION OF CURRENT DRM TECHNOLOGIES

2.1 Introduction

This section describes, in generic terms, those technologies which can be combined to provide the functionality required for DRM. While all the technologies described have proprietary instantiations, the survey in this report is provided on the basis that all proprietary technology is in reality a response to a requirement for technology. These requirements can be expressed in terms of functionality. This survey, therefore, is akin to a requirements analysis, but is based on the knowledge that the requirements have already been met by commercially available technology.

2.2 DRM as a Set of Tools and Components

It is often assumed that DRM technology is a unitary piece of software, which can be installed and which will then protect content online. In fact, DRM comprises a wide variety of technologies and services, some of which may reside on a user's device, some of which may reside on a merchant's network server and some of which may reside generally on the network.

Broadly speaking, these technologies can be generically identified as follows:

- Identification technologies;
- Metadata technologies;
- Rights language technologies;
- Encryption technologies;
- Persistent Association technologies;
- Privacy technologies;
- Payment technologies.

There has been much study and development in recent years to understand how such components required to produce a secure environment for IPR-based content can be combined. The activity has gone on in commercial software companies, in standards activities and within the academic community. The general consensus that has emerged is that the future of DRM lies in a hybrid of commercial services, software and standardized components. The aim is to provide a competitive market in the technologies, while ensuring that the consumer has the ability to access content through DRM systems without experiencing problems connected with technical barriers, such as incompatibility between systems. While solutions are still emerging and interoperability (see below) remains an intensely debated subject, it is clear that the way forward is becoming increasingly recognized.

2.3 Management of Digital Rights

The infrastructural element of an integrated system for the management of intellectual property access in the network environment requires the development of interlocking infrastructural standards for the unambiguous identification and description of intellectual property, including the rights and permissions associated with it.

Probably the most extensive published study into the identification and description requirements for intellectual property trading on the network was that undertaken by the <indecs> project.[10] This project developed a very simple generic model of trading, and underlined the absolute necessity of identifying each of the key elements in the model–the "content" itself, "deals" relating to the content and the parties to those agreements (whether individuals or organizations).

---

[10] See *www.indecs.org*. The partners in the project, which was supported by the European Commission under the Info2000 program, represented a wide spectrum of organizations concerned with the management of intellectual property rights.

<indecs> took the position that a single monolithic, global identification and description system encompassing all intellectual property would be an impractical ambition, and that the requirement is rather the development of mechanisms to facilitate interoperability between local and sectoral approaches. The solution to effective interoperability lies in the design of the identification and description systems themselves, which need to adhere to certain logical principles if they are to participate in a global intellectual property management solution.

2.3.1 The Basics of Identification

By "identification" is meant ascription of a label to something so that it can be unambiguously identified by someone else. Unambiguous identification is central to any automated business process; this becomes particularly obvious in processes that involve communication beyond the organizational boundary, when "local" identifiers are unlikely to be recognizable by supply chain partners.

In the absence of a monolithic identification framework, such identifiers will only be reliably unique within the context of a given naming authority–commonly referred to as a "namespace."

Unique identifiers are commonly, but not invariably, numbers. An easily recognizable example from within one content industry sector is:

ISBN 0 85021 294 4.

Here, the letters "ISBN" identify the namespace–this identifier falls within the authority of International Standard Book Number namespace; if this namespace is properly managed (as indeed the ISBN is), the combination of namespace and identifier can be expected to uniquely identify something–in the case of ISBN, the something that is identified is a product, something a publisher wants to sell.

A well-organized trading system for Intellectual Property requires more than just product identifiers (sometimes known as "tradable item" identifiers). Identification systems are needed to support the unambiguous recognition of a number of other aspects of Intellectual Property. This may be best recognized through the description of the growing "family" of standard identifiers being developed for the management of music. The following table describes the identification standards that are already implemented (or are in the process of being implemented). In this respect, the music industry is significantly better developed than other media sectors; it can be postulated that the collective management of mechanical and other rights, and the need to communicate between collecting societies in different territories, has particularly forced the pace.

Identifier name and acronym	Identifier status	What does it identify?
International Standard Musical Work Code (ISWC)	International standard ISO 15707	The ISWC identifies musical works–that is, the underlying "abstraction" of a piece of music. Take, for example, "Beethoven's Fifth"–a concept that exists and needs to be identified independently of any particular performance, recording or printed score (but which relates all of these things together). The ISWC plays a central role in rights management in music.
International Standard Recording Code (ISRC)	International standard ISO 3901	The ISRC identifies a particular recording of a musical work, independent of the form in which the recording is held (on a CD, for example, or as an online file). It identifies a recorded "performance" of a musical work. It does not identify the particular fixation medium.
International Standard Music Code (ISMN)	International standard ISO 10957	The identifier (closely related to, but managed separately from, the ISBN) that is used to identify items of printed music in the supply chain.
European Article Number/Universal Product Code (EAN/UPC)	Globally employed de facto standard	These identifiers are those most often used to identifier "tradable items" (audio CDs, audio cassettes) in the physical distribution. Frequently but not necessarily encoded on the product as a bar code.
Global Release Identifier (GRID)	Trade standard under development	This identifier has been developed by the recording industry to identify "electronic music releases"; it has been described as the digital equivalent of an EAN barcode–an identifier of digital tradable items.
Interested Party Number (IPN)	Trade standard implemented collectively by music copyright management societies	This identifier is the recently implemented successor to the "CAE" number (Compositeur, Auteur, Editeur number). Both numbering schemes were developed by–and are used exclusively by–the music copyright management societies to support the collective administration of their members' rights.
International Performers Database Number (IPDN)	Trade standard being implemented by performers' rights societies	This identifier, developed separately from the Interested Party system by a consortium of performers' rights societies, is used for collective administration of performers' rights.

Music Industry Identifiers

Music has been chosen as an example because it well illustrates the complexity of the identification task within a relatively mature identification architecture. Other media are now recognizing similar requirements. The book industry, for example, has been working recently on the development of a standard for the identification of textual works (the International Standard Textual Work Code - ISTC - which should become an international standard during the course of 2003).

What may be most striking about the music identification system is the acknowledged requirement for party identification. The unambiguous identification of rights holders is essential for the accurate and effective distribution of funds collected on their behalf. However, these identifiers have so far been implemented in only isolated parts of the music industry; it is not common for record labels, for example, to identify their artists consistently within their own internal systems. Most other sectors of the content industry do not have effective mechanisms for unambiguous party identification.[11]

The requirement to identify rights holders is mirrored by a similar need to identify users of rights. This becomes a particularly sensitive issue where it touches on the identification of individual consumers. There are, of course, potential proxies for individual identification and the threat to privacy that this implies. This is covered below in the section on privacy (Section 5.2.1).

2.3.2 Network Identifiers

Most of the identifiers discussed here pre-date the development of the Internet and may appear to have little relevance in today's world of network communication. The Universal Resource Locator ("URL") has the substantial advantage of being "actionable" in the network environment: "click" on a URL and a predictable action occurs–your browser is pointed to a specific resource on the World Wide Web.

A predictable action perhaps, but not a predictable result. The result of "resolving" a URL to its address is often unsatisfactory–either there is nothing there, or what is there has changed. The URL is, after all, what it claims to be– the identifier of a location not the identifier of what is to be found at that location. In this respect, it is like a library shelf mark–it takes you to a specific place, where you may find what you are looking for or you may not.

The network community, as represented by its two standards organizations (the World Wide Web Consortium ("W3C"), and the Internet Engineering Task Force ("IETF")), has been grappling with these issues for a decade. The conceptual framework for persistent identification on the network–the Universal Resource Name ("URN") has been in place for several years. However, making URNs actionable (and therefore useful) has proved more difficult.

The publishing industry, led primarily by scientific journal publishers whose publishing output was rapidly moving online, recognized the need for persistent actionable identifiers of

---

[11] In this context, the use of "name authorities" by libraries is worth noting. The InterParty Project (see *www.interparty.org*) is currently exploring mechanisms to facilitate the interoperation of "person identifiers" between different sectors.

content on the network and in 1998 established the International DOI Foundation, to develop and deploy the Digital Object Identifier ("DOI"), an actionable network identifier which uses the Handle "resolution" technology developed by Corporation for National Research Initiatives (CNRI). This was claimed by CNRI to be the first URN implementation.

One potential advantage of the DOI over other solutions lies in the capability for "multiple resolution" of the Handle system–in other words, the "action" undertaken by a DOI can be different dependent on the context in which it is used. However, the real implications of this capability are only now being understood and demonstrated. In the meantime, more generic implementations of URN are being proposed, and "top level" URN domain names are being granted to many of the existing identification systems, the proposition being that an identifier such as "URN:ISBN:0850212944" should become network actionable.

However, such "native" network functionality still does not exist.

2.3.3 Identifiers and Governance

The real challenge with identification systems lies in their governance. It has been pointed out by Tim Berners-Lee, the "father of the World Wide Web," that the problem with using the URL as a persistent identifier is a social rather than technical one. Even well-established identifiers, like the ISBN, have faced challenges through their application by certain users to identify "out-of-scope" items (most famously, the application of ISBN to soft toys which happen to be distributed through the book trade supply chain).

While clarity of guidance on usage is clearly essential, there is ultimately little that can be done to guarantee that users actually apply identifiers in the way that they are intended (or at all!). One approach that is increasingly being taken is to ensure that identifiers can only be applied to things which can be described within minimum metadata structures associated with the identifier.

Ultimately the governance of identifiers is a matter of consent–users have to find that it is to their advantage to "play by the rules." This is not too big a problem with the use of identifiers where the cost of application is relatively trivial. However, the challenge is much greater where the cost of joining the identification system may be relatively high (as is the case, for example, with the Digital Object Identifier). In these cases, organizations can be wary of governance systems which are apparently difficult for them to influence directly.

2.3.4 Identification–a Summary of the Issues

The implementation of an unambiguous identification infrastructure for the management of digital rights will be complex and difficult. The content industries are not (yet?) uniformly convinced of the requirement. However, in the sector where the rights management infrastructure is most developed–music–the extent of the challenge is now recognized.

However, identifiers by themselves have little value. Identifiers simply allow the easy linkage between systems that ensures that both are talking about "the same thing." It is the ability to use an identifier to link information about "the same thing" in different computer systems that gives the identifier its value.

2.3.5 Metadata

"Metadata" is a term which is used in many different ways. This is a clear example of the problem of semantic ambiguity which will be discussed in more detail in this section. It is therefore important to define the particular use of the term adopted for this report: "metadata" means information that describes "content" (which is the "data"). This slightly eccentric definition is the commonly understood meaning in the content industries.

The idea of "description" is, of course, a very broad one. The <indecs> project defined metadata in terms of the expression of relationship, which may be a helpful way of considering the breadth of potential ways in which something (or even someone) can be described.

Our primary focus in this paper will be on the metadata explicitly associated with identifiers, since this is the metadata that has the most direct application in the "management of digital rights." Metadata standards are in many ways less mature than identifier standards, because the significance of metadata interoperability is only now beginning to be understood.

It is worth noting in this context that an enormous amount of metadata has traditionally been compiled and recompiled at many different points in the information supply chain. Effectively "the same" information has been recorded by many different people. The wastefulness of these data collection and maintenance practices–in terms both of cost and quality–has led to development of standards for sharing data (and thus effort).

2.3.6 Identifiers and Minimum Metadata

The importance of the relationship between identification systems and metadata has been becoming increasingly apparent to those involved in establishing identifier standards. ISO TC46/SC 9, the ISO committee responsible for standards in Information and Documentation–Identification and Description (which has responsibility for all the ISO identifier standards mentioned in this document) has decided that no future identifier standard will be issued which does not include a minimum metadata specification.

For example, the current revision of the ISBN standard includes just such a minimum metadata set, designed to be registered with the ISBN.

The primary purpose of these "minimum metadata sets" is defined as disambiguation–there should be enough data to enable the distinction between two superficially similar but different things to be understood (in other words, to distinguish entities that share some but not all the same attributes).

As far as the book publishing sector is concerned, care is being taken to ensure that ISO identifier metadata standards are designed to be compliant with the ONIX trade standard. This will ensure seamless interoperation between different metadata sets in the same sector.

2.3.7 Interoperability of Metadata

Even if one sector, like book publishing, succeeds in defining trade standards that are widely implemented within that sector, it is highly unlikely that such standards will prove acceptable across historic sectoral, territorial and language boundaries.

With an increasingly global market, and the inevitability of media convergence as all types of content are delivered through a common network channel, interoperability across these boundaries will become essential.

As already discussed (see Section 2.3), the <indecs> Project defined the requirements for interoperable metadata. A principal requirement is that metadata terminology should be *well formed* which above all means that it must be *properly and unambiguously defined*. Much of the focus on solving the interoperability challenge has traditionally been on syntax: the real challenge may lie in *semantics*.

2.3.8 Semantics

This requirement for well-defined semantics substantially increases the role of properly structured data dictionaries–dictionaries that define the terms used in a metadata set in accordance with a properly structured data model (essentially, a "view" of the relationships between the different entities in the metadata set). More information on this is set out below.

2.3.9 Rights Expression Languages and Dictionaries

2.3.9.1 Functionality Required

Once content has been identified and described, rights owners will want to create the rules under which content can be accessed by users. Such rules will enable rights owners to create business models, either familiar or new, some examples of which were described in Section 1.3. Rules of this nature must fulfill a number of requirements. They must be:

– Fully expressive–that is they must be capable of enabling rights holders and anyone mandated by a rights owner to express their rights and interests in, and contractual agreements related to, content, according to a variety of usage and business models.

– Unambiguous–that is they must be absolutely precise, so they cannot be interpreted in any other way than the rights owner intended.

– Machine readable–that is, the licenses must be readable by computers and other microprocessor-based devices.

– Secure–they must be created in such a way that any tampering can be detected.

This is only a basic list of requirements for a rights expression language, but sets out the minimum requirements. The use of a rights expression language will be key to the future of digital rights management, because it provides the means for supporting current business models and creating new ones.

2.3.9.2 Description of Rights Expression Language Technology

Perhaps the easiest way of understanding what a rights expression does is to explain it in terms of a language that can express instructions for a computer. In this case, the instructions concern what a user can do with a piece of content. The rights holder turns her human permission (*You can copy this to your hard disk and play it ten times*) into logical language a computer program can interpret. The computer program in question is the encryption system that protects the content the user wishes to access.

Rights expression language technology was first developed in the early 1990s at the Xerox Parc Research Center, in Palo Alto, California. Since that time, the technology available has become increasingly sophisticated. Essentially, it is based on the notion that a permission is granted to a user to carry out a certain act, relating to content protected by intellectual property rights. For instance, if a rights holder wished to grant a user the right to copy a certain piece of content, for the purposes of playing it from the hard disk of a computer, it would be possible to grant that right on certain conditions. The rights holder might wish to prevent the content being passed to any third party (i.e., that it should not be copied again) or being changed in any way. This is a simple permission which a rights expression could formulate into a machine readable rights expression.

A rights expression language itself is written in some kind of computer language, probably XML. This is a so-called high level computer language that can be read (with some difficulty) by human beings as well. XML, sometimes called the language of the Web, is widely used and its value as the basis of a rights expression language is that it is pervasive, hence an aid to interoperability (Section 2.5.3.2).

2.3.9.3 Description of Rights Data Dictionary Technology

A rights expression language requires extremely precise terms (semantics) in order to create precise, unambiguous expressions. However, it has long been recognized that natural language and computer language are two different things. The language of the everyday is far from precise in computer terms and society is built on the notion that the interpretation of the nuance of language is essential. For instance, all law is framed on the basis that it cannot be so precise as to exclude interpretation.

Computers, on the other hand, cannot deal with imprecision. Given an ambiguous expression, computers will either fail to work or will function in an unpredictable manner. For this reason, it is necessary to create a set of terms (words) specifically for use in a rights expression language. These terms form the basis of a rights data dictionary.

A good example of how natural language can be problematic when applied in a rights expression language is the term “Copy.” It is used extensively in copyright legislation (indeed it is the basis of the term copyright), but for the purposes of a computer it is out of place. While to copy theoretically means to make an exact replica of something which is in all respects the same, human beings know that this needs interpretation. We “know” in fact, what “to copy” means. However, to a computer this does not make sense. How can one thing be exactly the same as another thing–they would be the same thing (the same material in the same time and place) and therefore theoretically there would be no copy. So, when using the verb *copy* for a rights expression language that must be interpreted by computers, it is essential to ensure that the imprecision in *copy* is effectively driven out. Furthermore, were

there to be reliance on the semantics of *copy* in a court of law, it would not be possible to precisely define them, which would render the use of a rights expression containing the word *copy* dangerous (Section 2.5.3.3).

2.3.9.4 Integrating Technology With Technical Protection Measures

As noted earlier, a rights expression (couched in terms from a rights data dictionary) is an instruction to a microprocessor-based device to behave in a certain way. The instruction is fed into a program, one of the key parts of a digital rights management system that is used to protect content. As will be seen later the instruction tells the program the terms and conditions under which the content, currently inaccessible to the user, can be consumed. A rights expression, to be of value, must be able to work seamlessly with the protection program so that the instructions it carries can be precisely understood and acted upon.

This requirement suggests that a rights expression language should be able to work with many different DRM programs. Without this ability, the rights expression language will be tied to a single DRM system and may be of limited use. The integration of a rights expression with many different proprietary DRM systems will therefore be one of the routes to achieving interoperability for users of DRM systems. For if the same content, governed by a single rights expression, can be consumed through several different DRM systems, it will both cut down the packaging work of rights holders (who would otherwise have to produce many different rights expressions in many different languages for many different DRM systems) and the inconvenience to consumers, since a single rights expression is likely to work with the technology of their chosen DRM supplier.

2.4 Digital Management of Rights

So far, it should be clear that managing rights to digital content requires persistent identification, clarity of description and usage rules that are precise and can be relied on to provide unambiguous instructions to a computer program used to protect content.

The next section describes the technologies for protecting content from unauthorized use–these are the digital locks and keys.

2.4.1 Encryption Technology Required Functionality

The protection of content from unauthorized access requires some kind of encryption. Encryption, or the process of obscuring information, has been developed over thousands of years. It has been used extensively in diplomatic and military applications, particularly in wartime to conceal information from the enemy. Its use in commerce has been more recent. In particular, it has seen widespread use in banking and other financially vulnerable areas, where security of information transactions and exchange is tantamount.

The process of encryption used on microprocessor devices for digital rights management involves algorithms (mathematical systems) for scrambling the digital information to prevent it being rendered in intelligible form. This can effectively protect rights holders' intellectual property from being accessed without authorization.

In DRM there are several essential requirements for encryption if a system is to be robust, with a level of security sufficient to ensure that content remains secure against unauthorized access or tampering.

– Sufficient Security–encryption systems must be secure enough for the type of content they are intended to protect. For instance, a trade book publication is likely to need less security than a government document dealing with nuclear weapons secrets. There is a tradeoff involved between the level of encryption available and the convenience to the user.

– User Convenience–encryption systems must not be onerous for the user at point of use. For instance, an encryption system that requires a user to wait for an unreasonable period of time while the security process is effected, will not be acceptable.

– Vulnerability–even the best encryption systems will be breached eventually. However, an encryption system should be engineered as far as possible so that a security breach does not vitiate the fundamental security of the entire system, but only that particular device or identity.

– Renewability–following a radical security breach, it must be possible to restore the security across the system with a rapid software upgrade.[12]

– Revocability–it must be possible to prevent a user from accessing a secure system. For instance, if it is known that a user's identity has been stolen, it must be possible to prevent an unauthorized person from using that identity to access the system by the withdrawal of privileges from the stolen identity.

While the main use of encryption technology is for what is often referred to as "content wrapping," it can be used for several other applications. For instance, encryption is integral to digital signature technology, by which the origin and integrity of content and identities (by which moral rights can be protected) can be assured.

2.4.2 Encryption Technologies Description

Digital encryption is used for locking up content so that it cannot be accessed. And, as in the physical world, where there are locks there are keys. One of the most important aspects of the DRM encryption technology, therefore, is management of the keys which provide access to encrypted content. Obviously, it is the security and convenience of these key management processes that can make a difference between "good" and "bad" DRM systems.

Digital encryption employed in digital rights management exploits two kinds of key management processes. One is known as single key encryption, the other is known as Private Key/Public Key encryption. The first kind is fairly simple. Content is secured by Party A (Ted) and sent to Party B (Alice). To unlock the content Alice must have the key Ted used for securing the content in the first place.

---

[12] See Section 3.3.2 for a discussion, in the context of the Digital Rights Management Workshop of the European Commission, of rights holders' views on the importance of renewability.

The easiest way to explain this is by analogy. Suppose Person A (Ted) wants to send a locked box to Person B (Alice). In order for Alice to open the box which had been locked by Ted, Alice has to have Ted's key (or a copy of it). This means Ted has to have given a copy of the key or the key itself to Alice. It would either be necessary for them to meet for the exchange or perhaps Ted could send the key to Alice by post.

This process of exchanging a key seems quite satisfactory, until certain weaknesses are noticed. First of all, Ted obviously cannot send the key in the same parcel as the box (which would be completely insecure), so he will have to pass the key to Alice in a separate transaction. Secondly, what if Ted wants to leave the box for Alice in some public place, but does not know her address in order to send the key? In this case, Alice would be able to find the locked box but would not have access to the key.

At first this seems impossible, but suppose Ted had a box with a special type of lock, one that he could lock with his own key, but could not unlock, because only Alice had a key to unlock it. This may sound strange, but it is precisely the technology that lies behind the encryption used in modern digital rights management encryption. The process is called Public Key/Private Key encryption.

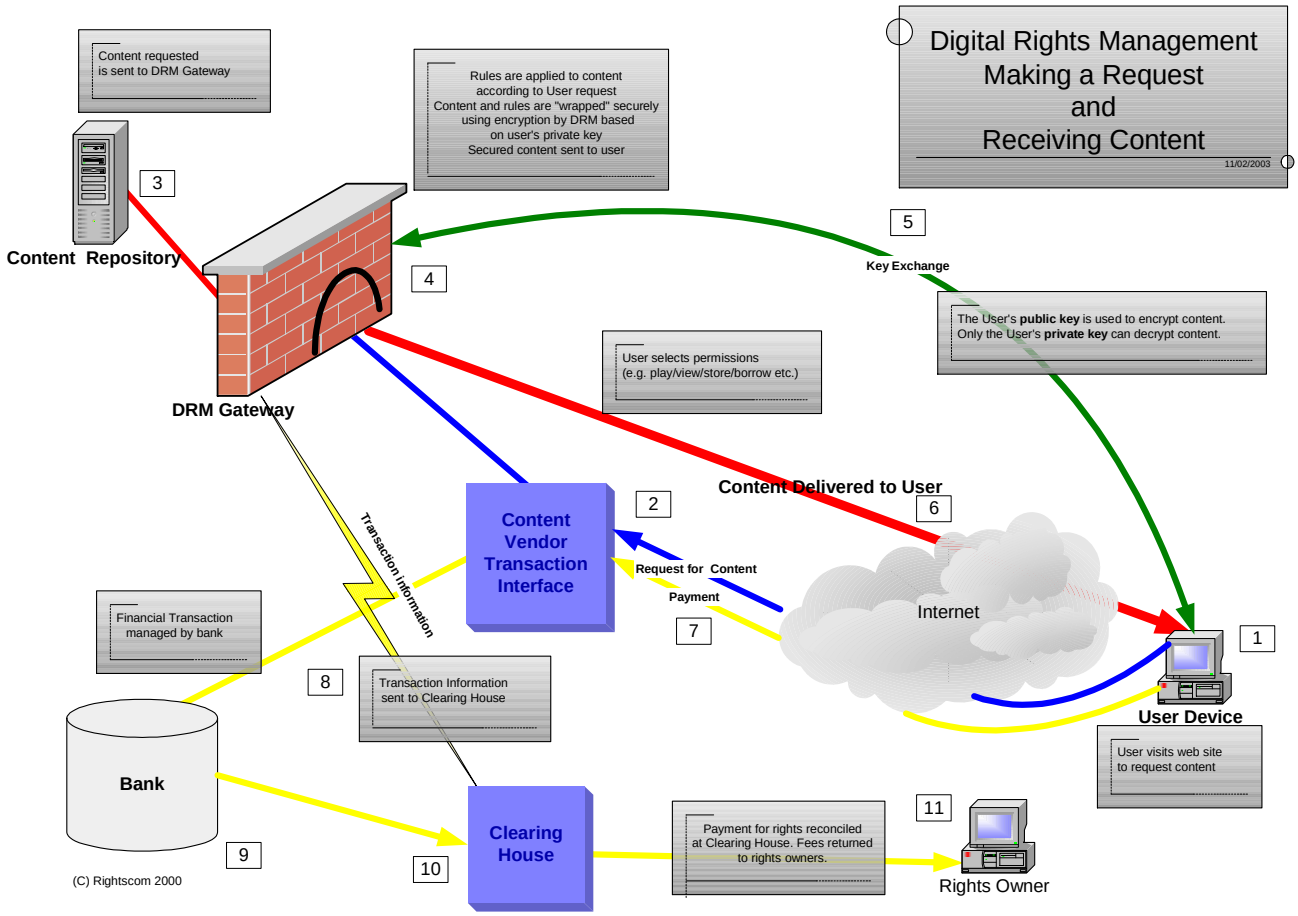
This system of encryption exploits a branch of mathematics called Modular Arithmetic, in which one-way functions enable a computation to be done in one direction which is almost impossible to turn back. Essentially, the process enables the generation of two mathematical (digital) keys, one which locks up, the other of which unlocks. The process of Public Key/Private Key encryption works because it is possible to give anyone the locking up key while keeping the unlocking key private. This way, only the person with access to the unlocking key (which must naturally be kept secure/private) will be able to access the content once it has been encrypted. This process enables a merchant to lock content up and send it on the public Internet to a particular individual who alone will be able to unlock the content.

The unique advantage of using public/private key technology for DRM is that it is possible to ensure that content is locked to a particular user or device. Theoretically this makes it impossible for a user A (Ted) to give content to user B (Alice) without Alice being able to pass the content on to Mike, because doing so would give access to Alice's key. Going further than that, some DRM implementations provide for Alice's key to be inaccessible, so that she cannot pass it on, but can only use it locally on her device to unlock content she has received.

Nothing, however, comes without a price. And the price of public/private key encryption is what is known as technical overhead. In this case, it means that creating and processing content secured with public/private key encryption requires a great deal of computing power, which in turn slows down the process of rendering the content. To get over this, public/private key encryption is used solely for locking up an ordinary key, provided by the DRM system. Because this ordinary key, which both locks and unlocks content, is secured by the private key of the recipient, it cannot be accessed by unauthorized users. These ordinary keys which are secured by public/private key encryption are only useful for a single piece of content and can sometimes only be used once, hence the name "session key."

2.4.3 A Secure DRM Transaction

To understand how a single, secure transaction can be made between content owner and content purchase, the following diagram shows a number of steps. Numbers on the diagram refer to the steps involved.



A secure DRM Transaction (© Rightscom 2003)

A user (Alice) [1] contacts a download service [2] to browse the inventory on offer. Once a selection has been made, the download service [2] accesses a content repository [3] where the content is known to be available. The content is then secured by the DRM gateway [4] using a session key secured by Alice's public key [5]. It doesn't matter that the DRM gateway can get access to Alice's public key because it is solely the locking-up key. The content is then sent to Alice [1], secured by her public key. Alice [1] then unlocks (accesses) the content using the private key which is unique to her. In return, of course, for the downloaded content, Alice [1] has made a payment to the download service [7] which is then passed through the download service banking facility. At the same time the DRM service may make a return to a clearing house [10] where the download is reconciled with the fee from the download server and finally passed on to the rights owner (Ted).

This is, of course, a highly generic view of the activity, but it does describe with some accuracy the various steps that need to take place. The peer-to-peer business model described earlier in this paper could be easily operated using functionality of this nature. In this case, instead of the content being sent to Mike by Ted, Alice sends it. But because the content is secured and cannot be unlocked without Alice's own key (which she either does not wish to

send or to which she does not have access outside her own device), Mike has to ask Ted for a new session key. Ted duly locks up a new session key with Mike's public key and sends it to Mike, so that Mike can unlock the content sent by Alice. This model, whereby one consumer can pass content to another consumer, is likely to be a very significant form of secure content distribution in future.

2.4.2 Description of Persistent Association Technologies

This section gives an overview of several technologies that can be used to meet the high-level requirements for persistently associating information with content. The technologies are: fingerprinting, watermarking and digital signatures.

2.4.5 Persistent Association Technologies Required Functionality

In order to manage and protect intellectual property, it is essential to have adequate identification and description pertaining to content available (i.e., metadata). Such "metadata" needs, however, to be *persistently associated* with the content itself so that various applications–including anti-piracy services–can have access to the metadata.[13] In the analog world such association between content and its metadata can be achieved by printing an identifier onto the data *carrier* containing the content (e.g., by printing a bar code onto a CD cover or an ISBN onto one page in a book). This approach fails in the digital world, however, because there are no physical carriers to carry the identifiers. Hence a technology is needed that allows obtaining the metadata from *looking at the content itself*. The main requirements for such technologies are:[14]

– The technology needs to be able to establish the link between the content and the metadata with high accuracy;

– The quality of the content should not be degraded so that "artifacts" become perceptible;[15]

– Survivability against alteration of the content, ranging from "normal" operations (e.g., resizing or cropping of a picture) to "malicious" attempts to break the link between content and its metadata;

– Survivability into the analog domain (i.e., when the content is (a) decoded, (b) played back on, for example an analog loudspeaker and (c) re-digitized, the identification is still possible);

– Detecting, responding to and processing metadata all require computing power, and the processing burdens on devices and software should be minimized, to the extent possible; and

---

[13] An example of the persistent association of metadata with content is the "broadcast flag," which is discussed in Section 3.2.1.3(b).

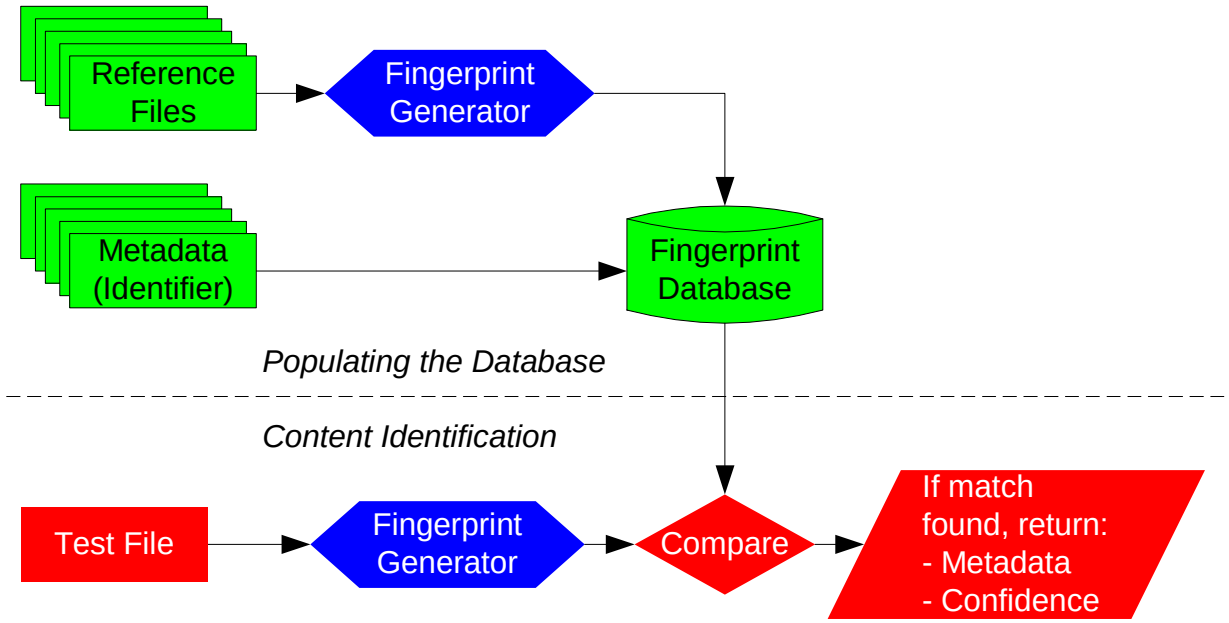
[14] It should be noted that not all requirements apply to all application scenarios.

[15] With the exception of "visible watermarks" used, for example, by television stations to include their logo in their television broadcasts.

– Preserving the backward compatibility of new content with legacy devices, as well as the ability of legacy content to be played back on new devices, is essential.

2.4.6 Fingerprinting

Fingerprinting technologies can be used to identify content by the process depicted in the diagram below. Fingerprinting, or "content-based identification technologies" function by extracting the characteristics of a file and storing them in a database. When the technology is presented with an unknown file, the characteristics of that file are calculated and matched against those stored in the database, in an attempt to find a match. If a match is found, the system will return the appropriate metadata from the fingerprint database.



Fingerprinting System

In order to use fingerprinting technology, three steps need to be undertaken:

– First a database with "reference fingerprints" and appropriate metadata will need to be populated. This step, depicted in the diagram above, will need to be done before attempting to identify unknown content;

– Second, to find information about any file (called a "test file"), the system generates a "test fingerprint" from the test file. This test fingerprint is then compared with all "reference fingerprints" stored in the fingerprint database;[16]

– Finally, when a matching fingerprint has been found, the metadata associated with that metadata will be taken from the Fingerprint Database. This metadata will be the output of the process.

---

[16] It should be noted that this comparison could be a significant task when the fingerprint database is large. However, intelligent database strategies can reduce the resources needed to acceptable levels.

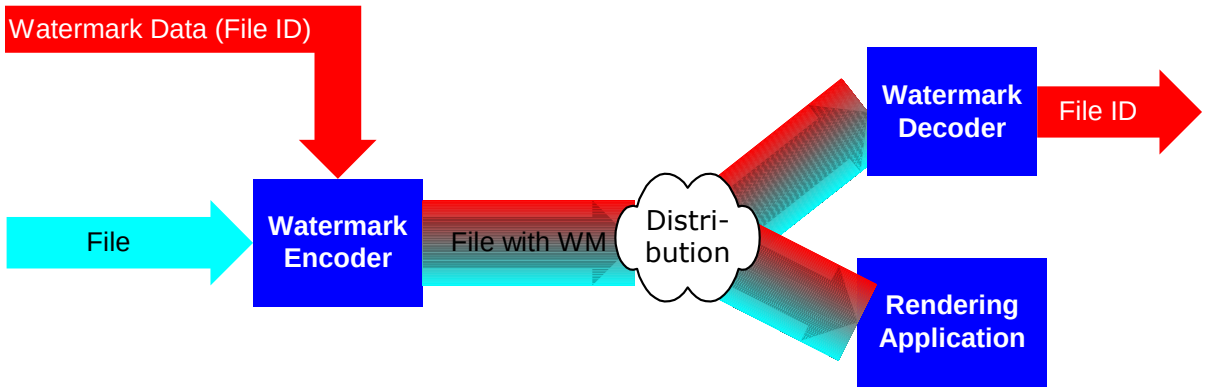
Software programs and services using fingerprinting technologies are available for different media types such as audio and video. The best of these systems will–in certain media fields–correctly identify more than 95 out of 100 files even under bad conditions where the file has been maliciously or unavoidably altered to overcome the fingerprinting system. Some technologies are even able to make high levels of positive matches in circumstances where the test file is created with a lot of background noise, such as in a club.

Fingerprints, while highly effective with certain content types, are less equipped to aid the unique identification of other content types, depending on the "detail" they provide. Hence fingerprints are suitable for audio, video and audio-visual content as well as photographs but less for computer graphics[17] or text.

The traditional field for content fingerprinting technologies is the monitoring of radio stations to (a) compile radio and, since the start of MTV, video charts, and (b) to distribute royalties to rights owners by collecting societies. Fingerprinting systems are increasingly used to monitor peer-to-peer content distribution systems for copyright infringements. Another example of using fingerprinting is the following scenario. A user is sitting in a pub or restaurant and, upon hearing a song he likes, activates his fingerprinting device (e.g., his/her mobile phone) which recognizes the song and transmits some information to a service provider. On arriving home, the user finds the same song as a DRM-governed audio file in his/her email inbox–sent by an automated system using the fingerprint sent from the mobile phone to identify the song the user liked.

2.4.7 Watermarking

Watermarking is also often cited when discussing copyright protection technologies. A watermark is "(imperceptibly) embedded information." This information (often a file or IP identifier) can, though imperceptible[18] to normal consumers, be extracted by special software. This "watermarking detector" can, when applied to content that is suspected to be pirated, check if the content bears the watermark and thereby prove or disprove the suspicion. Typically, all files that are to be distributed are watermarked before they are allowed into the content chain. A functional flow diagram of this is shown in the diagram below.

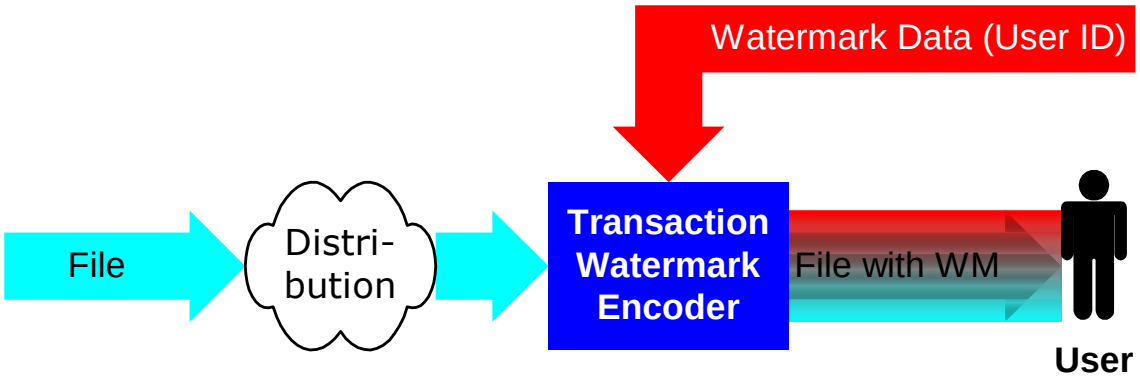


Watermarking System

[17] Naturally, photographs with very little detail (e.g., a picture of a clear blue sky) may be less compatible with fingerprinting technologies than a computer graphic with many details.

[18] As mentioned above, not all watermarks are necessarily imperceptible, see note 15.

A second method of using the same underlying technology is to embed a "transaction watermark" as depicted in the diagram below. Transaction watermarks allow the establishing of a link between an arbitrary user in the content value chain with the content he or she "touched." In scenarios where *both* content and user identifiers are required, both types of watermarks can be combined.



Transaction Watermarking System

The maximum "payload"[19] size of the watermark (be it an *a priori* or a transaction watermark) can vary and depends on the content type, mainly because of the amount of data that can be reliably and resiliently transported within the watermark. Generally speaking, the bigger the file, the more data can be hidden within the file.

Watermarks have, however, some disadvantages. Similar to fingerprinting, watermarks cannot be used with all content types. Small graphic elements such as logos or text are not able to carry watermarks because of a general limitation on the amount of data that can be embedded into the content. The maximum size of the watermark payload depends on three main factors:

- Content type (audio vs. video vs. still pictures vs. graphics vs. text);
- Content size:
    - Video: frame rate, picture size, compression rate, length;
    - Audio: sampling rate, compression rate, duration;
    - Still pictures: picture size, compression rate.
- Robustness:
    - What "attacks" should the watermark survive?;
    - Should it be normal signal processing such as cropping, re-sampling and speed changes?; or should it also be more sophisticated activities such as rotating an image by a few degrees?

[19] The payload of the watermark is the data that is "hidden" (e.g., the identifier used to uniquely identify the file or the intellectual property contained therein).

In turn, one can say that depending on the size of the payload to be embedded into a certain type of content, the robustness of the watermark may vary. As these limitations are fairly severe with today's watermarking algorithms, it is widely agreed that watermarks should only carry a small amount of information, typically a content identifier. A second limitation of watermarking technologies is that embedding a watermark means changing the original content. While in many cases this alteration does not affect the quality of the material from a human's perspective, it may make it difficult to embed watermarks repeatedly in the same content without them becoming perceptible. Hence, watermarks cannot, for example, be embedded during the iterative process of developing an advertisement.

Thirdly, all watermark systems known today are susceptible to being removed without substantially affecting the quality of the content itself–which may lead to the situation that, when a watermarking system has been broken, the originally governed content may become uncontrollable.

A final drawback is that watermark detection cannot work with legacy content if no watermark was inserted in the first place.

Watermarking has been used mainly in the audio and video space to aid the control of copyrighted material. Some audio CDs, for example, contain watermarks. Watermarks, in the form of TV logos, are also added by television stations to the signal they broadcast. These watermarks are clearly visible and act as a deterrent against the program's illicit use by other stations. However these watermarks are not intended to be robust against removal.

As watermarking and fingerprinting technologies are often confused, the table below provides a list of crucial differences between them.

Fingerprinting	Watermarking
Works for all media types (although of limited application for some types).	Only works for some media types.
No alteration to the files needed. Hence the users will only ever use an "original" or unaltered file.	Files need to be watermarked before the watermark can be detected–which may, in some circumstances, impede the usability of the files.
Susceptible to malicious attacks, although the success rate for certain systems for certain content types is well above 95%.	Susceptible to malicious attacks.
Can identify "legacy" content.	Cannot identify "legacy" content.
No data in the fingerprint. Fingerprints only provide a link to a database with unlimited amounts of metadata.	Amount of data that can be contained in a watermark is very limited. When the watermark contains an ID, a link to a database–with unlimited amounts of metadata–can be achieved.
Needs an infrastructure with a populated fingerprint database.	Infrastructure is only necessary for forensic examinations.

Fingerprinting	Watermarking
Needs an infrastructure with a populated fingerprint database.	Infrastructure is only necessary for forensic examinations.
	Effectiveness of watermarking systems may decrease with new, more efficient content compression technologies– notwithstanding improvements in watermarking technologies.

Watermarking vs. Fingerprinting

2.4.8 Digital Signatures

It is important that information associated with content (e.g., IDs and rights expressions) can be trusted. Such functionality can be achieved when the party adding the metadata (a) digitally signs the metadata and (b) is known to be authorized to add the metadata. A digital signature, akin to the hand-written signature,[20] provides information about the origin of a piece of information and knowledge about whether the information has been altered. In the context of insuring that the piece of metadata associated with a file has not been altered the following steps need to be undertaken:

– The signatory will calculate a hash for the content and metadata;

– The signatory will cipher the hash value with a key only the signatory has access to;

– The ciphered hash value ("signature") will be added to the file (which now contains three elements: the original content, the metadata and the signature); and

– The person wanting to verify the signature can use the same tool with which the signatory signed the algorithm with a corresponding key which is known to have come from the signatory.

The four-step process described above allows a user to confirm that content has not been altered, but the verifying person still does not know if the signatory had the right to add the information or to package the content. In order to confirm this, the signatory needs to add a certificate to his signature. This certificate, issued by a certification agency, uniquely identifies the signatory and makes him identifiable (and liable) when errors have been found in the data he provided.

2.4.9 Privacy Management

One aspect of the challenge of building an effective DRM infrastructure lies in the maintenance of privacy, confidentiality and the protection of personal data. There are very real and understandable concerns about the extent to which any DRM infrastructure that proves effective in protecting intellectual property will at the same time imply entirely

[20] Increasingly, countries are affording digital signatures the same legal status as physical (or manual) signatures.

unacceptable intrusion into people's private and commercial lives.[21] This issue is discussed further in Section 5.2.1.

Models of DRM depend on a "trusted identity" infrastructure–involving trusted identification of content, of the permissions related to the content, and of parties to the permissions related to the content. This becomes particularly sensitive when the parties concerned are individual consumers. Much of the discussion around privacy management seems to focus on the commercial value of personal information for marketing, coupled with alarm about "identity theft" and misuse of credit card information. However important these issues may be, they may tend to trivialize the underlying question of privacy rights.

Appropriate implementation of "Privacy Enhancing Technologies" ("PETs") in the DRM infrastructure will likely prove essential to long-term consumer acceptance of the implementation of DRM. This will include the use of anonymizing technologies, which allow identities to be authenticated by "trusted third parties" (in other words, by an organization trusted by both consumer and distributor) without the actual identity of the consumer being disclosed. While such additional levels of indirection may add apparently unnecessary complexity, a DRM infrastructure that fails to take into account legitimate concerns about privacy and confidentiality will be likely to fail.

2.4.10 Payment Systems

There are several types of payment models available with DRM systems.

A typical way to pay for content is entering a credit card number on a secure Web page encrypted by the SSL protocol. Using a credit card is the most common way to purchase content (and goods) online. Recent estimates from the credit card company Visa, have shown that European customers spent €2.57 billion online using Visa cards during Q4 2002, which is 136% higher than in the same period in 2001. Visa also estimates that 31.1 million online transactions were recorded during Q4 2002, compared with 14.5 million in Q4 2001. However, many users are still reluctant to use their credit cards directly on an online merchant's Website because of privacy and security concerns, while online merchants are sometimes confronted with liability issues.

Even though most online payments are made via credit cards, alternative modes of payment have been or are currently being developed. For instance, the music portal Popfile.de in Germany has developed a system in partnership with Deutsche Telekom, which allows users to stream and download DRM-enabled music tracks and charge for content via the user's fixed phone bill. Various micropayment systems are also developing and will potentially become a common method of purchasing DRM-enabled content, not only online but also for mobile content.

---

[21] For a spectacularly dystopian view of DRM, see Richard Stallman's article, *The Right to Read*, originally published in *Communications of the ACM*, February 1997, 40 No 2; available, with an author's note updated in 2002, at *http://www.gnu.org/philosophy/right-to-read.html*. Although the tone of this article can be criticized for being a little hyperbolic, it ought to be read thoughtfully by anyone engaged in the development or deployment of DRM.

Several companies have also developed systems, which allow users to enter their credit card once in a central server. Once registered, a consumer receives access to an electronic wallet, which can subsequently be used to purchase content on online portals, which have partnered with the service. The system claims to guarantee anonymity and privacy, while reducing liability issues on the side of online merchants. Other companies have developed micropayment systems, which are generally processed via mobile phones, for low-price transactions such as one piece of music from an online catalog, an eBook or an article on the premium (paid) section of a newspaper's Website.

2.5 Underlying Standards for DRM

A crucial issue for the future of Digital Rights Management is the development of standards. Many applications intended for managing and enforcing content protection are based on standards. Standards are a crucial point for DRM applications and are found on several "stages" of electronic content distribution. Implementing standards in DRM applications is equally important for enabling devices, applications and services from different vendors to exchange content as they are for service providers, who own and control the DRM infrastructure, rights owners who are interested in maximum dissemination of their content and consumers who listen, watch and read content on devices and applications typically referred to as "players." The primary goal of using standards in DRM applications is to lead toward interoperability among devices, applications and services, which is crucial for the success of any business utilizing DRM.

2.5.1 Formal and Informal Standards

Standards can be either formal or informal. Formal standards are those under the management of internationally agreed standardization bodies, such as the International Organization for Standardization ("ISO") or the International Telecommunication Union ("ITU"). Although these organizations are internationally recognized, their processes tend to be slow and some people believe they are not suited to the pace of change in the computer age. Alongside the formal standards bodies are other organizations such as the Internet Engineering Task Force ("IETF") and the World Wide Web Consortium ("W3C"). While not formal standards bodies as such, both the IETF and the W3C are fundamental sources of standards for the Internet and their recommendations are widely adopted.

Informal standards range from those supported internationally by an entire industry sector, such as the Digital Video Broadcasting Project ("DVB") or the Organization for the Advancement of Structured Information Standards ("OASIS"). Both these organizations have memberships drawn from industry and are working toward solutions that will enable manufacturers to create products and services of use to both rights holders and consumers. They are recognized internationally, and the specifications they develop are respected as important contributions to the technical and regulatory landscape for digital rights management.

2.5.2 Standards for Management of Digital Rights

As has been seen in the table in Section 2.3.1, many identification systems are standardized and managed by the ISO. Such formal standardization provides a guarantee of stability to an identification scheme and should underwrite its longevity, both crucial factors

in promoting widespread implementation. However, there are also identification systems that are not managed by ISO, such as the DOI standard (Section 2.3.2).

The earliest significant "metadata" standard was developed by the library community to enable the sharing of library catalog cards. This standard, MARC, is still widely in use. However, library metadata has been designed to support only one class of user activity–"discovery"–focused on providing library patrons with points of access to library holdings (as are its successors in library practice). How will a (human) user want to look for things: through the name of the item (what editions of this book are in the library?), or through its author (what books by this author are in the library?) or through its subject matter (what books on this subject are in the library?).

The tradition of library "discovery" metadata has been carried forward into online practice through "Dublin Core,"[22] a standard developed primarily by librarians that was initially conceived as a "lowest common denominator" standard for cross-media and cross-sector discovery on the Internet. Attempts have been made to further elaborate Dublin Core through the addition of "qualifiers" to the original 15 elements; unfortunately, these simply serve to underline the extent to which Dublin Core is conceptually inextensible (it has no underlying "view" expressed through a coherent data model).

The need for "product data" to support distribution channels has also long been recognized. In particular, the book trade, with its enormous number of product lines and new product launches, has for many years recognized the need to distribute "books in print" information–initially as printed volumes, more recently in various electronic forms that recipients (book wholesalers and retailers) can load into local computer systems.

Typically this product information has been aggregated by a limited number of "bibliographic agencies" in each territory; as book retail has increasingly moved online, the bibliographic agencies have enhanced their offerings to include the increasingly sophisticated product information (cover images, for example) that may be needed to encourage consumers to purchase in the absence of any ability to "browse." The recording industry, although not faced with quite the same issues in terms of sheer numbers of products, has also seen the development of a number of data aggregators to provide consolidated product information to retailers.

The demand for increased communicability of "rich product information" in the book trade is apparent in the development of the ONIX (online information exchange) standard. This XML-based standard, which is now being widely implemented, allows the distribution of comprehensive product information from the point of creation at the publisher and throughout the supply chain (either direct or through intermediaries, who may offer quality control and data enhancement, and, of course, comprehensiveness, which can be a particularly important attribute). It is expected that similar standards for product data are likely to emerge in the music and audio-visual industries.

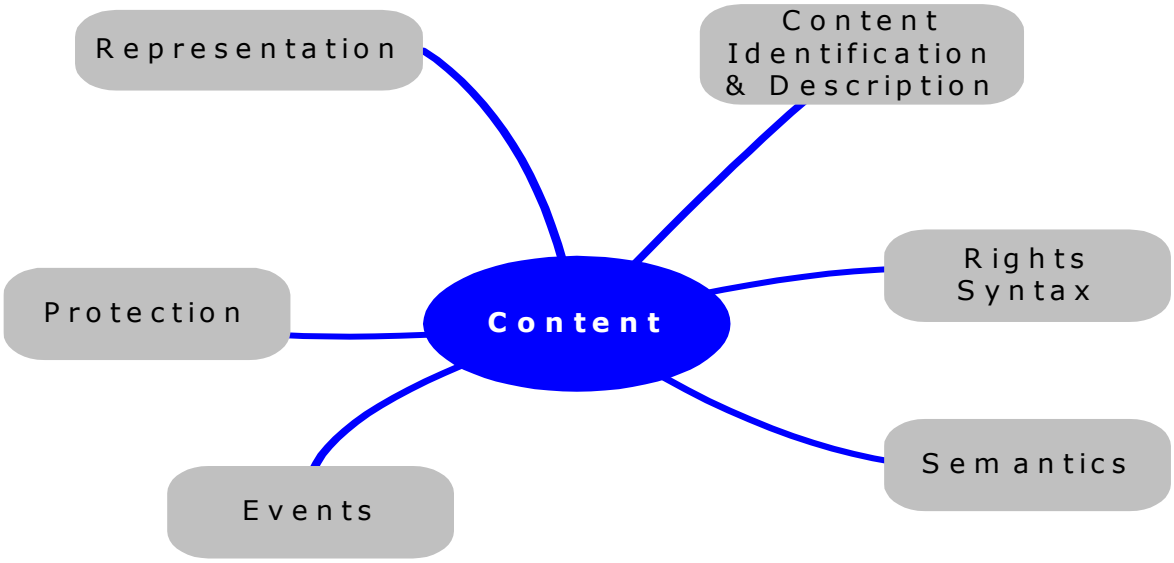
---

[22] See *www.dublincore.org*.

2.5.3 Standards for Digital Management of Rights

Several elements are required to establish a coherent and functional standard infrastructure for DRM applications. The figure below shows the various areas that qualify content elements (such as music files, video clips or eBooks), within a DRM application.

The following subsections give a brief overview of these qualifiers:



Content Elements and DRM-Related Qualifiers

2.5.3.1 Content Representation

Content representation is used to package content. Typical standards are MP3 or MPEG-4. In the DRM context, it is important to be able to also represent metadata and the structure of complex content items. Examples of typical content representation standards that can be used in such a context are XML and MPEG-21 DID:

– The eXtensible Markup Language ("XML") is a common "Web" language used for many purposes. XML is able to represent structured online content such as text, but also metadata associated with any content. It is less appropriate for representing other types of content such as audio and video files.

– MPEG-21 Digital Item Declaration ("DID") is part of the MPEG-21 framework.[23] This content representation standard provides the ability to declare the structure and metadata of complex content elements. For example, a digital music release, comprising several sound recordings, the cover art, inlay with lyrics, etc.

[23] See *www.telecomitalialab.com*.

2.5.3.2 Rights Syntax

Technically a part of content description as well, a rights syntax is a set of terms to specify rules in relation to such content. Standardized rights syntaxes are often called rights expression languages ("REL"), as described in Section 2.3.9. One example is the MPEG-21 Rights Expression Language ("MPEG-21 REL").

The MPEG-21 REL specification describes the syntax and semantics of the rights expression. The language uses a simple and extensible core data model for its key concepts and elements. The data model includes four basic entities and the relationship among these entities. The relationships are defined by the REL assertion "grant." A typical MPEG REL grant includes:

– The principal to whom the grant is issued;

– The right that the grant specifies;

– The resource to which the right in the grant applies; and

– The condition that must be met before the right can be exercised.

The core data model will be enhanced by a number of so-called "Extensions" which will add functionality. For instance, such extension can be used to enhance the range of conditions that can be applied to grants, thus providing extra functionality. The MPEG-21 REL is expected to become an International Standard by the autumn of 2003.

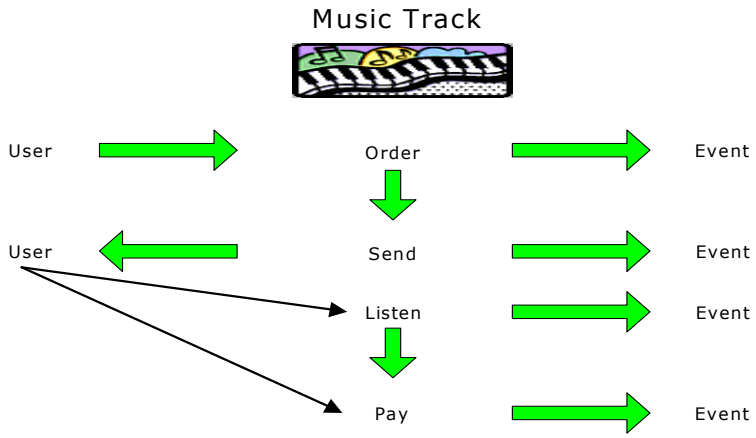
2.5.3.3 Semantics

Rights syntaxes can only be used when their terms are well-defined through underlying semantics. Semantics provides the exact meaning of verbs and terms used in any language or, in fact, rights syntaxes. The goal of semantics standards in this area is to allow content to be exchanged between domains using different rights language standards and schemas. Thus, semantics standards could soon become an important element for interoperability between DRM applications. The most notable semantics standard, which is currently under development, is the MPEG-21 Rights Data Dictionary ("RDD"). (See Section 2.3.9.3 for a discussion of rights data dictionaries.)

The MPEG-21 RDD aims to support the implementation of a rights language for secure exchange of intellectual property on networks by the provision of an interoperable data dictionary for rights. The initiative, based on the original <indecs> analysis (see Section 2.3), has been underway since mid-2001.

2.5.3.4 Event Reporting

Reporting events play a major role in content-related eCommerce applications. Every step of a typical eCommerce transaction generates an event. For example, the purchase of a music track online, which includes ordering, sending, listening to and paying for content, will generate the events shown in the figure below:



Event Reporting

Event reporting standards, such as MPEG-21 Event Reporting, can therefore be an important part of a DRM application. MPEG-21 Event Reporting, which is currently under development, is expected to comprise a library of Event Report "templates": the MPEG-21 Event Reporting Language ("ERL"), based on the MPEG-21 REL, on which a user can request and/or describe an event, and the MPEG-21 Event Reporting Dictionary, based on the MPEG-21 RDD, which is the semantics supporting MPEG-21 ERL.

2.5.3.5 Content Protection

The last area, content protection, which enforces restrictions on digital content and prevents unauthorized content use, is also a crucial element of a DRM system.

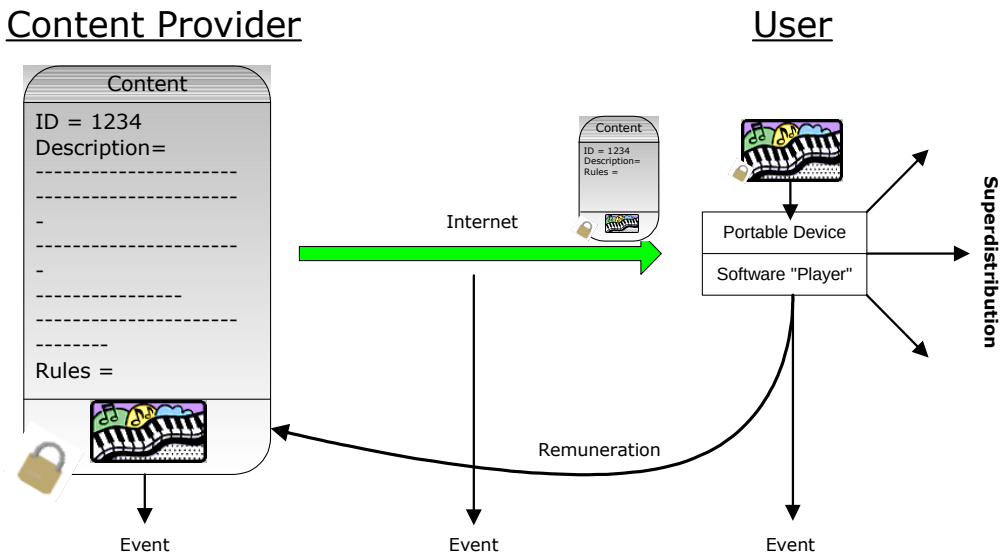
Content protection standards deal directly with the physical protection of the content. Content protection standards include low-level standards such as cryptographic algorithms, conditional access standards and watermarking standards, intermediate level specifications such as the smart media protection standards, and high-level specifications such as MPEG-4 IPMP.

The Content Scramble System ("CSS") is an example of a content protection technology; it is used to protect audiovisual material on DVD video disks. The DVD CCA licenses CSS to studios and to manufacturers of DVD playback devices (including stand-alone players and drives, and integrated devices, such as personal computers), as well as various components of the CSS system. CSS is itself a complete content protection technology. The protection afforded by the technology is supplemented by the mandatory terms and conditions of the CSS license; these are intended to ensure maximum protection for DVD content, by such means as authorizing only certain outputs and imposing "robustness" standards on product manufacturers. Although CSS has been hacked by DeCSS, the technology continues to be used to protect content on DVD video disks.

Another approach to enforcement standards has been pursued by MPEG. MPEG does not specify the entire security system but only provides a framework for enforcing content protection. Proprietary solutions can therefore be "hooked" into the standard.

2.5.3.6 The Big Picture

As described above, content representation, content identification and description, rights syntax, semantics, event reporting and content protection are crucial elements required to build a DRM system. One must keep in mind that each element relies upon another element, as demonstrated in the workflow chart below:



Content Protection Work Flow

The content provider "wraps" content into a container, which contains the file (in this case a music track). The container includes a unique identifier (e.g., ISRC), a set of descriptions, a set of rules (with implicit semantics) and the music track itself (e.g., an MP3 file).

Once wrapped, the content is now able to "travel" via the Internet to the user. The user can replay the content on a software "player" or a customized device. It is important to note that the initial ID, description, rules and protection are still associated with data. This allows the content provider to be remunerated by the user for playing the content and to accurately report (event reporting), for example, how often the content is played. The user can also send (if allowed by the rules) the content further to another user (superdistribution).

3. THE PRESENT LEGAL FRAMEWORK

3.1 International Treaty Obligations

3.1.1 WIPO Internet Treaties

3.1.1.1 The Anti-Circumvention Provisions

The WCT and the WPPT have established the new international legal norms for protection of technological measures, such as DRM technologies, used to safeguard content from unauthorized access and use. The WIPO Treaties were the product of a substantial amount of negotiation both before and during the Diplomatic Conference itself. To understand the obligations imposed by the treaty language that was ultimately adopted, it might be useful to compare the Basic Proposal,[24] which was before the delegates to the Diplomatic Conference, with the final text.

Article 13 of the Basic Proposal would have prohibited "protection-defeating"–or circumvention–devices and services, knowing that they would be used in connection with the unauthorized "exercise of rights" provided "under this Treaty," i.e., "copyright rights."[25] The Article would also have required that Contracting Parties provide "appropriate and effective remedies" against those unlawful acts. Finally, technological protection measures were not defined by the Basic Proposal, but the draft text would have prohibited circumvention of "any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty."

This Basic Proposal would have applied only to copyright control (not access control) measures, and only to devices and services, not to the act of circumvention. During the course of the Diplomatic Conference, the text was modified. Article 11 of the WCT, entitled "Obligations Concerning Technological Measures," provides:

"Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by

---

[24] See *Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference*, prepared by the Chairman of the Committees of Experts on a Possible Protocol to the Berne Convention and on a Possible Instrument for the Protection of the Rights of Performers and Producers of Phonograms (WIPO doc. CRNR/DC/4 of August 30, 1996), available at *http://www.wipo. int/eng/dip/conf/ 4dc_all.htm* ["Basic Proposal"].

[25] Article 10: Obligations concerning Technological Measures
(1) Contracting Parties shall make unlawful the importation, manufacture or distribution of protection-defeating devices, or the offer or performance of any service having the same effect, by any person knowing or having reasonable grounds to know that the device or service will be used for, or in the course of, the exercise of rights provided under this Treaty that is not authorised by the rightholder or the law.
(2) Contracting Parties shall provide for appropriate and effective remedies against the unlawful acts referred to in paragraph (1).
(3) As used in this Article, "protection-defeating device" means any device, product or component incorporated into a device or product, the primary purpose or primary effect of which is to circumvent any process, treatment, mechanism or system that prevents or inhibits any of the acts covered by the rights under this Treaty.

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."[26]

The WPPT, in Article 18, adopts largely the same wording.

The two Articles give substantial leeway to the Contracting Parties in determining how to implement these obligations. So long as the legal protection is "adequate" and the legal remedies "effective," the obligations will be met. They do not have to be air-tight and prevent every single type of act of circumvention. In particular, the texts do not bar Contracting Parties from crafting appropriate exceptions and limitations to the legal protections and remedies, so long as those carve-outs do not undermine the protections envisioned by the Contracting Parties for "effective technological measures."

What, then, does Article 11 require? First, does it require prohibiting both the act of circumvention and the trafficking in circumventing devices and services? Although the language is ambiguous, it does lend itself to the interpretation that it focuses more on the act of circumvention rather than on the devices, as had the Basic Proposal. Nevertheless, prohibiting technologies alone may be permissible because that would be one (or an additional) way in which such actual acts of circumvention could effectively be prevented.

Second, Article 11 only prohibits circumvention of "effective" technological measures. A measure need not be completely "effective," however, to enjoy the protections that would be mandated by Article 11; if it were completely effective, then obviously no legal prohibition against its circumvention would be needed, since the technology would seem to be, by definition, immune from circumvention.

Third, Article 11 addresses measures used in connection with authors' exercise of their copyright rights under the Berne Convention and the WCT. To the extent that a technological measure is used by an author to exercise rights that are beyond those granted by the Berne Convention (e.g., where uses fall within limitations or exceptions to copyright, such as fair use), arguably Article 11 would not require a Contracting Party to prohibit circumvention in connection with such a use.

Fourth, are technological measures that effect only "access control," but not copyright control, subject to protection under Article 11, given that there is no express "right of access" in the Berne Convention? It also has been argued that because authors can and do authorize access to their works, and given that an access control measure can effectively "restrict" any unauthorized access, then the last clause of Article 11 does cover such technological measures (in addition to measures that implement copyright control).

In any event, as suggested above, Article 11 does not prohibit Contracting Parties from affording protections for technological measures that exceed the requirements of the WIPO Treaties. Furthermore, the WIPO Treaties permit Contracting Parties to use existing legal remedies against the circumvention of technological measures, including DRMs. In this regard, Article 11 of the WCT and Article 18 of the WPPT do not require specific new anti-circumvention legislation and, indeed, some states have since determined that their existing legal regimes are adequate and effective to meet their obligations under the WIPO Treaties.

---

[26] WIPO Copyright Treaty, Art. 11 (adopted December 20, 1996).

3.1.1.2 Rights Management Information

The WIPO Treaties also establish benchmarks for protection of rights management information. Rights management information is defined as information that identifies the work, the author of or the owner of any rights in the work, or information about the terms and conditions of use of the work, as well as any numbers or codes that represent such information.

Article 12 of the WCT and Article 19 of the WPPT require that the Contracting Parties provide "adequate and effective legal remedies" against two types of acts. Persons who knowingly perform acts that they know will induce, enable, facilitate or conceal an infringement (or have reason to know that their acts will do so) may not:

– Remove or alter any electronic rights management information without authority; or

– Distribute, import for distribution, broadcast or communicate to the public without authority works or copies of works knowing that the electronic rights management information has been removed or altered without authority.

3.1.1.3 The Digital Environment

The WCT also established certain rights under copyright, including authors' right of distribution and right of communication to the public, "including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."[27] Rights holders have thought that having these rights would be critical to best make use of the opportunities in the digital environment. These rights were especially important for the distribution of content over the Internet and through other digital media, including television, broadcasting and cable. To address concerns of certain nations and user communities, however, Article 10 states expressly that the Contracting Parties may provide for "limitations of or exceptions to the rights granted to authors," so long as such exceptions are confined to "special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author."[28] Importantly, the Agreed Statement accompanying Article 10 makes clear that Member States may "extend into the digital environment limitations and exceptions" and "devise new exceptions and limitations" appropriate for the digital environment.[29] The extent to which DRMs and national legislation to implement the anti-circumvention provisions of the WIPO Treaties have, as a practical and technical matter, accommodated the policies reflected in Article 10 and the accompanying Agreed Statement is discussed below in this Section 3 and in Section 5.1.2.

---

27 WCT, Art. 6 (right of distribution) and Art. 8 (right of communication to the public).

28 *Id*. at Art. 10.

29 *Id.* at Agreed Statement concerning Article 10.

3.1.2 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)

3.1.2.1 Scope of TRIPS Agreement

The World Trade Organization (WTO) TRIPS Agreement is another critically important international treaty for rights holders who are distributing their content through the means of eCommerce, including via DRM schemes. The TRIPS Agreement was concluded in 1995 as an integral part of the broader set of trade negotiations undertaken during the Uruguay Round of the General Agreement on Tariffs and Trade.[30]

The TRIPS Agreement came into effect on January 1, 1995. It provides protection and enforcement for various types of intellectual property rights, including copyrights, patents, trademarks and trade secrets, among others. Specifically, Part II of the TRIPS Agreement establishes minimum standards for substantive areas of intellectual property to which members must adhere. Part III sets minimum standards regarding members' domestic enforcement of intellectual property rights. Part V addresses dispute prevention and settlement and Part VI sets out certain transitional arrangements.[31] The TRIPS Agreement also generally requires national treatment (by a Member State with respect to its treatment of nationals of other states) and most-favored-nation treatment (forbidding discrimination between the nationals of other Member States).

With respect to Part II, the TRIPS Agreement incorporates by reference and, to some extent, expands upon the substantive protections that are required by the Berne Convention for copyrights, the Paris Convention for the Protection of Industrial Property and others. These are minimum standards, so members are entirely free to provide greater protections for intellectual property. As to Part III, the TRIPS Agreement requires that member states implement and comply with procedures to enforce intellectual property rights, including civil and administrative procedures and remedies, the right of rights holders to obtain provisional measures against alleged infringers and special requirements related to border measures and criminal procedures.

Although the TRIPS Agreement establishes an important common and basic international legal framework for protecting copyrights and other intellectual property, and for enforcing those rights domestically, the agreement was largely negotiated by December 1991, and then came into effect before the WIPO Treaties. In this regard, some commentators have observed that the TRIPS Agreement did not adequately take into account the intellectual property issues implicated by the digital distribution of content, including via the Internet, and that the protections for DRMs afforded by the WIPO Treaties are not covered by the Agreement.[32] Much of the debate over electronic distribution has, however, shifted from the fundamental issues of the basic standards of copyright protection, which the TRIPS

---

30 *Agreement on Trade-Related Aspects of Intellectual Property Rights*, available at *http://www.wto.org*.

31 Among the transitional provisions are the timetables for coming into full compliance with the TRIPS Agreement. Developed countries were required to comply with the entirety of the TRIPS Agreement by January 1, 1996. Developing countries had five years, until January 1, 2000. The least developed countries were given ten years, until January 1, 2005.

32 See S. Baker, P. Lichtenbaum, M. Shenk and M. Yeo, *E-Products and the WTO*, 35 *The International Lawyer* 5, 20 (2001).

Agreement provides, to the challenges of the digital environment and the more novel issues of protecting technical safeguards from circumvention, which are among the subjects of the WIPO Treaties. Thus, it has been noted that the WIPO Treaties were prompted, in part, by the need to fill "lacuna" in the TRIPS Agreement and the Berne and Rome Conventions.[33]

3.1.2.2 World Trade Organization (WTO) Work Programme on Electronic Commerce

Within the WTO, however, there has been some consideration of, for example, whether and how to fold prohibitions on circumvention of DRMs and other technological measures into the TRIPS Agreement. These discussions have occurred in the context of the WTO's broader Work Programme on Electronic Commerce ("Work Programme"), which began with a declaration at the Ministerial Conference in May 1998, that the General Council would establish a comprehensive work program to examine "all trade-related issues relating to global electronic commerce."[34] The Work Programme was established on September 25, 1998 for the relevant WTO bodies, including the WTO Council for Trade-Related Aspects of Intellectual Property Rights ("TRIPS Council"). The issues that the TRIPS Council was intended to examine included protection and enforcement of copyright and related rights, and new technologies and access to technology.[35]

As phrased by the Secretariat of the TRIPS Council in a Background Note of February 10, 1999, the question is whether, in the digital network environment, the TRIPS Agreement norms provide "effective and adequate protection of intellectual property rights."[36] The Background Note specifically identifies and discusses issues addressed by the WIPO Treaties, such as the definition of "publication" and the scope of the rights of reproduction and communication to the public in an online environment. Significantly, the Background Note comments on the importance of technological measures for copy protection, encryption and watermarking, and on the usefulness of electronic rights management information, which are dependent on the legal protections reflected in the WIPO Treaties.[37] The Background Note extensively discusses the activities of WIPO, including the two WIPO Treaties and the implications of electronic commerce for intellectual property.[38]

The Background Note spurred further consideration of these issues by the TRIPS Council, including contributions from WTO members and a presentation by a WIPO representative on the activities underway within WIPO. WTO members submitted contributions to the Council, suggesting further work. One of the suggestions was to consider whether the TRIPS Agreement itself should be adapted or clarified to reflect new technological developments, such as the use of DRMs. Some contributions, however, also

---

33 See Submission from Australia, *Electronic Commerce Work Programme,* WTO Document IP/C/W/233, at paragraph 28 (December 7, 2000). See *also Work Programme on Electronic Commerce: Background Note by the Secretariat*, WTO Document IP/C/W/128, paragraph 75 (February 10, 1999) (technological measures were not raised in TRIPS negotiations and TRIPS Agreement contains no specific provisions concerning such measures) ["Background Note"].

34 *Declaration on Global Electronic Commerce*, WTO Document WT/MIN(98)/DEC/2 (May 25, 1998).

35 *Work Programme on Electronic Commerce*, WT/L/274, at paragraph 4.1 (September 30, 1998).

36 Background Note, at paragraph 14.

37 Background Note, at paragraphs 75-76.

38 *Id*. at paragraphs 80-92.

reflected a preference for not having the WTO duplicate work already underway at WIPO. In its Progress Reports of July 1999 and December 2000, the TRIPS Council set out the consensus of the members: that the Council continues to acknowledge the complexity of the issues and notes that further study in certain core areas is required and that the Council is of the view that the WTO should continue to consider these developments, including the ongoing work of WIPO.[39] Thereafter, within the WTO, the Doha *Ministerial Declaration* of November 2001 noted the work underway regarding electronic commerce and asked the General Council to report on appropriate institutional arrangements for continuing that work at the Fifth Session of the Ministerial Conference,[40] scheduled for September 2003.

3.2 United States of America

3.2.1 Legal Framework

In October 1998, the United States of America implemented the anti-circumvention provisions of the WIPO Treaties in Title I of the Digital Millennium Copyright Act ("DMCA").[41] Other federal and state laws also may be available to protect DRM technologies against unlawful circumvention, or are otherwise available to rights holders whose works are accessed without their authorization.

In the United States of America, legal protection for DRM technologies arises out of a delicate interplay between private sector agreements–which are used to license content protection technologies–and governmental action, including federal and state laws and federal regulations. The prevailing view in the United States of America since the mid-1990s has been to prefer private sector solutions arising, where possible, out of inter-industry negotiations. These solutions enable rights holders to rely on contractual protections and remedies to address products that fail to conform to the agreed-upon standard for content protection. This interplay, and these contractual arrangements, are discussed in detail in a paper previously prepared for WIPO by Dean S. Marks and Bruce H. Turnbull: "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses."[42]

To summarize the conclusions of that paper, a welter of private sector content protection technology license agreements include specific requirements intended to protect content, such as motion pictures and music, upon entry into the home environment and in personal networks. As described in the paper, these agreements contain:

– Encoding rules–addressing when content can be "encoded" by rights holders to restrict copying or re-distribution;

---

39 *Work Programme on Electronic Commerce: Progress Report to the General Council*, WTO Document IP/C/18 (July 30, 1999); *Work Programme on Electronic Commerce: Progress Report by the Chairman to the General Council*, WTO Document IP/C/20 (December 4, 2000).

40 *Ministerial Declaration*, WTO Document WT/MIN(01)/DEC/1, at paragraph 34 (November 20, 2001).

41 WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, Title I of the Digital Millennium Copyright Act (codified at 17 U.S.C. Chapter 12).

42 WIPO Doc. No. WCT-WPPT/IMP/3 (December 3, 1999) ["Marks/Turnbull"], available at *http://www.wipo.int/eng/meetings/1999/wct_wppt/pdf/imp99_3.pdf*. The paper was reprinted in 22 E.I.P.R. 198 (2000).

– Compliance rules–governing the outputs to which protected content can be redirected; and

– Robustness rules–mandating how products should be built to withstand circumvention of their copy protection elements.

Although a detailed discussion of these agreements is beyond the scope of the present paper, they include the following: Digital Transmission Content Protection ("DTCP"), which is licensed by the Digital Transmission Licensing Administrator LLC ("DTLA"); High-bandwidth Digital Content Protection ("HDCP"), which is licensed by the Digital Content Protection LLC; Content Protection For Prerecorded Media ("CPPM") and Content Protection for Recordable Media ("CPRM"), which are both licensed by the 4C Entity LLC; and the Content Scramble System ("CSS"), which is licensed by the DVD Copy Control Association, Inc. ("DVD CCA").[43]

Where gaps in content protection cannot be filled by private sector arrangements such as these, industry groups in the United States of America have considered and then pursued governmental action. Of course, where compliance across the board is required, governmental mandates would seem to be required. In addition, in many situations contract-based approaches would be neither available nor effective, where, for example, DRMs could be circumvented by individuals or by products manufactured by entities that are outside the realm of contract. To address such cases, only the civil and criminal remedies afforded by law would be adequate.[44]

3.2.1.1 DMCA

3.2.1.1(a) Background

The legislative consideration and the enactment of the bill that became the DMCA was marked by the most intensive debate–in both the halls of Congress and public discourse–over intellectual property legislation since the enactment of the comprehensive U.S.A. Copyright Act of 1976. On one side of the debate–promoting robust, broad-based implementation of the requirements of the WIPO Treaties–were copyright-owning interests, principally the motion picture, recording and publishing industries. On the other side, urging caution, balance and broader exceptions to the prohibitions on circumvention, were technology companies, such as computer and consumer electronics companies, and user interests, including libraries, educational institutions and consumers. The DMCA has been subject to substantial criticism from these groups, both then and into the present.

Various committees of Congress, each with its particular perspective, were involved in the legislative deliberations. Among the most significant of the many issues Congress considered were:

---

43 *Id*.

44 *Id*. This point is elaborated in Section 5.2.3, which discusses the role of government in DRM standard setting.

– Whether the DMCA should prohibit circumvention tools (including services), [45] or only the acts of circumvention;

– Whether circumvention of a technological measure in aid of a non-infringing act, such as fair use, should be permitted;

– Whether legitimate activities, such as reverse engineering and the testing of encryption systems, should be prohibited;

– Whether tools that are lawful, under the prevailing legal standard for contributory copyright infringement, should be prohibited because they are designed to circumvent technological measures;

– Whether the DMCA should or does prohibit only "black boxes" that are designed to circumvent, and not ordinary computer, consumer electronics or telecommunications products;

– Whether the DMCA should define the "technological measures" for which circumvention is prohibited; and

– To what extent the DMCA represents the transition to a "pay per use" society, limiting access to works made available only in encrypted form.

3.2.1.1(b) The Anti-Circumvention Provisions

At a high level, the anti-circumvention provisions of the DMCA, which implement Article 11 of the WCT and Article 18 of the WPPT, reflect a matrix of prohibitions:

	Act of Circumvention	**Circumvention Tools**
Access Control Technological Measure	Prohibited (§ 1201 (a)(1))	Prohibited (§ 1201(a)(2))
Copyright Control Technological Measure	Not prohibited (by DMCA)	Prohibited (§ 1201(b))

As noted, the WIPO Treaties arguably only require adequate and effective protection against circumventing *acts* and only with respect to measures used to protect authors' exercise of their *copyright rights* under the Berne Convention, the WCT and the WPPT. The DMCA, however, exceeds the minima of the WIPO Treaties to separately prohibit both circumventing acts and circumventing products, and with respect to both "access control" and "copyright control" technological measures used to protect a copyrighted work.

Section 1201(a): This section prohibits acts and products that circumvent access control technological measures. The definition of "circumvention" is expansive, including to

[45] Ultimately, the concept of circumvention tools was encompassed in the DMCA's phrase "technology, product, service, device, component, or part thereof." 17 U.S.C. §§ 1201(a)(2), 1201(b)(1).

descramble, decrypt, or "otherwise to avoid, bypass, remote, deactivate, or impair a technological measure, without the authority of the copyright owner."[46]

The DMCA does not define "technological measure." It does, however, define whether a technological measure "effectively controls access to a work": it controls access "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[47] The legislative history of the DMCA suggests that Congress was contemplating that such measures as encryption and authentication would be the sorts of technological measures that would control access to a work, but that the definition was purposefully left open to accommodate possible future developments.

Among the various technological measures that have been determined by the courts and the Librarian of Congress ("Librarian") to control access to a work are an authentication sequence to ensure that content was streamed only to an authorized player; CSS, which is used to protect DVD video disks from unauthorized access; the region coding system used on DVD video disks to make them playable only in particular geographic regions; and region codes used in video games.

Section 1201(a)(1): This section prohibits a person from circumventing a technological measure that "effectively controls access to a work." The prohibition flatly outlaws the act of circumvention, even if the act is undertaken for purposes that are entirely lawful and authorized by the Copyright Act. During the course of the DMCA debate, among the most heated of the controversies was whether there should be an express "fair use" (or other similar) exception to this prohibition. Congress ultimately concluded that no such exception should be provided and that circumvention, even in aid of a fair use, is unlawful.

Nevertheless, a compromise of sorts was struck, due to concerns about the effect of the prohibition. First, the statute delayed the date on which this section became effective for two years, until October 28, 2000. The purpose of the delay was to enable the Librarian, upon recommendation of the Register of Copyrights, to conduct a study that would examine whether persons who are users of a copyrighted work will be "adversely affected" by the prohibition in being able to make non-infringing uses of particular classes of works. Second, the DMCA requires that the Librarian conduct the same study every three years thereafter. This regulatory process, the conclusions of the Librarian in 2000 and the current study (to be concluded later in 2003) are described below in Section 3.2.1..3(a).

Further, by prohibiting circumvention of technological measures that control access to a work, it has been said that the DMCA has indirectly created for rights holders a new "right of access" to their works; to be sure, however, the availability of such a new right is made expressly contingent on the use of a technological measure. Such an access right was not previously provided in either the Berne Convention or the WCT.

Librarians and other users have argued that this new right–in the absence of a right to circumvent to facilitate a fair use–inexorably will lead to the establishment of a new "pay-per-use" society. The future, they have warned, would differ markedly from the traditional world of tangible copies, where a user who purchases a book or record can enjoy it

---

[46] 17 U.S.C. § 1201(a)(3)(A).

[47] § 1201(a)(3)(B).

over and over again without having to pay for each use. Under this view, the balance of interests in U.S.A. copyright law, between rights holders and users, has been or will be threatened.

Rights holders have responded to these concerns by pointing out that a variety of new business models that could cater to a wider range of consumer preferences can be facilitated through access control. Indeed, they point out, users might well want to pay only for a single use, rather than buying the right to use a work multiple times by purchasing a copy at what could be a higher price. They further emphasize that if there is a market for a particular type of use, they will sensibly provide the product in a way that satisfies that demand.

Section 1201(a)(2): This section prohibits the manufacturing, selling, offering to the public or providing of (i.e., "trafficking" in) any technology, product, service, device, component, or part thereof (i.e., any "tool") that circumvents a technological protection measure. Note that even if any such technology as a whole does not violate the statutory proscription, any single component–or even a part of a component–can be prohibited. To be prohibited, however, such a tool must meet any one of three tests:

– Be "primarily designed or produced for the purpose of circumventing the technological measure that effectively controls access to a work";[48]

– Have "only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work";[49] or

– Be "marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work."[50]

These three independent tests were controversial at the time of the DMCA's enactment and remain so. In particular, the test of being "primarily designed or produced for the purpose of circumventing" departs significantly from the test established by the U.S.A. Supreme Court in 1984, in a case involving the lawfulness of Sony's Betamax videocassette recorder. The Supreme Court decided that Sony was not contributorily liable for the Betamax users' home taping practices because the recorder, like other staple items of commerce, was capable of commercially significant non-infringing uses.[51] The DMCA, however, flatly prohibits tools (to the extent they circumvent technological measures) based on their primary design or production, without regard to whether they can or will be used for non-infringing uses.

To respond to the substantial shift in the law with respect to manufacturers' potential liability for their products, Congress adopted Section 1201(c)(3), discussed below, in Section 3.2.1.1(c).

Another area of uncertainty surrounds what is meant by "primarily designed or produced." In this respect, the legislative history of the DMCA is not clear. Nevertheless, it would seem that the use of "primarily" means only the most significant of the "purposes"; there probably can be only a single "primary" purpose. A tool that circumvents, but has

---

48 § 1201(a)(2)(A).
49 § 1201(a)(2)(B).
50 § 1201(a)(2)(C).
51 *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

multiple purposes, all of which are equal in stature, might not therefore have been "primarily designed or produced" for the purpose of circumvention.

Section 1201(b): This section only prohibits the trafficking in tools that circumvent technologies that protect the right of a copyright owner in a work or portion thereof. To be outlawed, the tool must meet any one of three tests, which are substantially similar to those set out above.[52] The section also defines circumvention in the same way as Section 1201(a). Again, a technological measure is not defined, but such a measure "effectively protects a right of a copyright owner" if the measure "in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a [copyright] right of a copyright owner." In other words, if a technological measure is used to prevent unauthorized reproduction, distribution, public performance or public display–an unauthorized copyright "use"–then a circumvention tool is prohibited (assuming that one of the three tests, such as "primarily designed or produced," is met).

Notably, the DMCA does not prohibit the act of circumventing a technological measure that protects a copyright owner's exclusive right to authorize use of a work. Congress determined that the DMCA need not itself prohibit the act of circumventing, in order to make a copy of a work, for example, because, in most instances, the ultimate act–of unauthorized copying–would infringe copyright. Consequently, a rights holder could resort to copyright law and the defendant could assert any applicable defenses or limitations available under that law.

3.2.1.1(c) Limitation and Exceptions

The DMCA is replete with limitations and exceptions reflecting both the exceptional intensity of the discussions in Congress and the interests of particular groups. Some of the most significant of these are discussed below.

Relationship to Copyright Infringement, Including Fair Use: The DMCA states that Section 1201 does not affect "rights, remedies, limitations, or defenses to copyright infringement, including fair use."[53] The provision superficially might be read as protecting fair use activities. Nevertheless, as courts interpreting the provision have found, it is clear that any rights and defenses under copyright law are separate from and not affected by the new rights, remedies and exceptions of the anti-circumvention provisions: it is no defense to a DMCA claim brought under Section 1201(a)(1) to argue that circumvention was done for the purpose of carrying out an entirely lawful, fair use activity.[54]

Relationship to Vicarious or Contributory Copyright Infringement: The DMCA provides that nothing in Section 1201 will "enlarge or diminish vicarious or contributory" copyright liability for any technology.[55] That language is largely meaningless, however, because, as noted above, if a product violates Section 1201(a)(2) or Section 1201(b) that violation may be prosecuted–under the standards of Section 1201–without regard to whether the product assists in or contributes to the infringement of copyright.

---

52 17 U.S.C. § 1201(b)(1)(A)-(C).

53 § 1201(c)(1).

54 See Section 3.2.2 (discussing *Universal City Studios, Inc. v. Corley*).

55 17 U.S.C. § 1201(c)(2).

No Mandate Provision for Ordinary Products: In response to concerns from manufacturers of computer, consumer electronics and telecommunications products that their products might be held to violate Section 1201, the DMCA provides that the provision does not require that their legitimate products be designed, or that parts and components need to be designed or selected, to "provide for a response to any particular technological measure."[56] This clause has generally been referred to as the "no mandate" provision, because it means that such products will not be required to affirmatively respond to a technological measure in order to avoid an allegation that they circumvent; in other words, only affirmative acts of circumvention (rather than the mere non-response to a technology) will violate Section 1201.

Manufacturers may avail themselves of this provision, however, only "so long as" the product, part or component "does not otherwise fall within the prohibitions" of the section. Although the meaning of this proviso is not altogether clear, some of the legislative history is to the effect that a product must be looked at in its entirety to determine why it failed to respond, whether for some legitimate design reason or for some illicit purpose of circumvention. The language itself suggests that a manufacturer cannot rely on this provision where some functionality of the product does affirmatively engage in bypassing, avoiding or otherwise circumventing a technological measure.

In addition to these limitations, Section 1201 contains other specific exceptions. The WIPO Treaties do not prohibit Contracting Parties from creating exceptions to the general proscription on circumvention. The requirement that the legal remedies must be "adequate" and "effective" does imply, however, that an implementing country may decide to weigh the benefits and burdens, to rights holders and users, of prohibiting circumvention. This is just what happened in Congress, which adopted seven exceptions that are, however, widely conceded to be both very narrow and highly particularized. In most situations, the exceptions would, on their own terms, be inapplicable. All of these exceptions are applicable to the act of circumvention of access controls, but only five of them would apply to the provisions that prohibit the trafficking in circumvention technologies.

The seven exceptions are as follows:

– Nonprofit Libraries, Archives and Educational Institutions:[57] These institutions, if they are open to the public or to persons not affiliated with the library, may circumvent solely for the purpose of gaining access to a work to make a good faith determination whether they wish to purchase it. A qualifying institution may only gain access for the time needed to determine whether to obtain a lawful copy. Any circumvention for commercial advantage or financial gain is prohibited.

---

[56] § 1201 (c)(3). Another important section of the DMCA expressly does provide for an affirmative response in a particular case: essentially all analog videocassette recorders must be designed to conform to certain analog copy protection technologies licensed by Macrovision Corp. § 1201(k). As part of the compromise between manufacturers of those devices and rights holders, the provision specifically includes encoding rules, which provide that these anti-copying technologies may not be applied to free, over-the-air broadcast television; however, they can be used to restrict copying (1) of a copy made from subscription program; (2) of a pay-per-view or a video-on-demand program, or from packaged media; or (3) from copies made from such programs or media. § 1201(k)(2).

[57] § 1201(d).

– Law Enforcement, Intelligence and Other Government Agencies:[58] National security and law enforcement activities, including information security activities, where lawfully authorized, will not be subject to the prohibitions on the acts of circumvention, and the trafficking in technologies, set out in Sections 1201(a) and 1201(b). Nor are they subject to the provisions of Section 1202, which is described in Section 3.2.1.1(d) below.[59]

– Reverse Engineering of Computer Programs:[60] Reverse engineering of a computer program–and only a computer program–by someone who has lawfully obtained a copy of the program is permitted (notwithstanding access controls), but subject to a series of conditions. First, the "sole purpose" of the circumvention must be to identify and analyze program elements "necessary to achieve interoperability" with an "independently created computer program." Second, those program elements must not otherwise have been previously "readily available" to the person circumventing. Third, the activities must not themselves constitute infringement. (In the ordinary course, under prevailing U.S.A. case law, making a reproduction in connection with otherwise lawful reverse engineering is considered a non-infringing fair use.[61]) Furthermore, a person may "develop and employ" tools to circumvent, for the permitted purpose. In addition, the person may make the information he acquires through the reverse engineering activity available to others, but solely to enable interoperability.

– Encryption Research:[62] "Good faith" encryption research of an access control technological measure is permitted subject to four conditions: (1) the person engaging in the research has lawfully obtained the copy; (2) the act is necessary to conduct the research; (3) the person made a "good faith effort" to obtain authorization; and (4) the act does not constitute infringement or a violation of another law. Encryption research is defined as the "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies . . . to advance the state of knowledge . . . or to assist in the development of encryption products." In determining whether the exemption is available, a court is instructed to consider whether and how the information resulting from the encryption research was disseminated, whether the person is legitimately engaged in encryption research and whether the findings and documentation of the research are provided to the copyright owner of the work protected by the technological measure.

At the time of enactment, it was thought that the limitations and conditions of this exception would severely curtail its applicability and that, therefore, legitimate encryption research might be adversely affected by the DMCA. To this end, the DMCA required that a report be prepared within one year on the effect of the DMCA on encryption research; the adequacy and effectiveness of technological measures; and the protection of copyright owners against unauthorized access to encrypted works.[63] The report, published in July 1999 by the Register of Copyrights and the Assistant Secretary for Communications and Information, concluded that no one had identified a "discernible impact" on these matters, that

---

58 § 1201(e).
59 § 1202(d).
60 § 1201(f).
61 See *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9th Cir. 1992).
62 17 U.S.C. § 1201(g).
63 § 1202(g)(5).

any harms were prospective and that such a result was not surprising since the actual Section 1201(a)(1) prohibition on acts of circumvention had yet to become effective.[64]

– Protection of Minors:[65] This exception provides that a court, in applying the anti-trafficking provisions of Section 1201(a) to a component or part, may consider whether the exception to the prohibition on circumvention is necessary for a technology that "has the sole purpose to prevent access of minors to material on the Internet."

– Protection of Personally Identifying Information:[66] This exception, targeted at cookies, permits the act of circumvention where the technological measure (or the work it protects) collects or disseminates personally identifying information gathered in the course of online activities; where such collection or dissemination is done without "conspicuous notice"; where such act has the "sole effect" of identifying and disabling this collection or dissemination capability; and the act is carried out solely to prevent those activities and does not otherwise violate the law.

– Security Testing:[67] This exception permits a person to engage in good faith testing of the security of a computer, computer system or computer network, with the authorization of the owner. It permits both the act of circumvention and allows the person to develop, distribute and use technological means for the sole purpose of security testing, but for no other purpose. Acts are permitted only if they do not constitute infringement or violate any other law. If a defendant invokes this exception, a court is instructed to consider whether the information was used "solely to promote the security of the owner" of the computer, or was shared with him; and whether the information as "used or maintained" so as not to facilitate infringement or the violation of any other law.

3.2.1.1(d) Copyright Management Information

The DMCA, in Section 1202, separately provides for protection of "copyright management information" ("CMI"). CMI is central to an effective DRM system, as it is information that describes the work and how it may be used.

The DMCA defines CMI quite broadly, and includes any information conveyed with a work that describes the work, including the title, author, information set out in a copyright notice, the name of performers (in certain circumstances, not including public performances of a work by a radio and television broadcast station, and not an audiovisual work), the names of writers, directors and performers (in an audiovisual work, except where broadcast), terms and conditions for use, identifying numbers or symbols and other information prescribed by the Register of Copyrights.[68]

---

64 See Register of Copyrights and Assistant Secretary for Communications and Information, *Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act*, Part III (1999), available at *http://www.copyright.gov/ reports/studies/dmca_report.html*.

65 17 U.S.C. § 1201(h).

66 § 1201(i).

67 § 1201(j).

68 § 1202(c).

Section 1202 has two operative provisions. The first prohibits the provision of false CMI or the distribution or importation of false CMI, where the person does so knowingly and where the intent is to "induce, enable, facilitate, or conceal infringement."[69]

The second prohibits an unauthorized person from intentionally removing or altering CMI; distributing or importing CMI knowing that it has been removed or altered without authorization; or distributing, importing or publicly performing a copy of a work or a work knowing that the CMI has been removed or altered without the authorization of the copyright. The above acts are prohibited where the person knows or has reasonable grounds to know that that activity will induce, enable, facilitate or conceal an infringement.[70]

3.2.1.1(e) Remedies

The DMCA provides for civil and criminal penalties.[71] Civil remedies include injunctions and impoundment, as well as actual damages and statutory damages. The statutory damages may, at the discretion of the court, range from US$200 to US$2,500 for each act of circumvention or circumventing product (for Section 1201 violations) and from US$2,500 to US$25,000 (for Section 1202). Awards can be adjusted upward for repeated violations and downward for innocent violations. Nonprofit libraries, archives and educational institutions may not be liable for damages where they were unaware that their activities violated the law, and no criminal penalties may be levied on them.

3.2.1.2 Other Laws/State Laws

A wide variety of other federal and state laws provide some protection against circumvention of technological measures that could be used in DRM systems. They are briefly identified here:

– Copyright Act: Where a product facilitates copyright infringement, including by circumventing a DRM to enable unauthorized copying, a copyright infringement action may lie against the manufacturer or other provider of the device. In addition, therefore, to being sued under Section 1201(b) of the DMCA, they may also be found liable for contributory copyright infringement if the device enables a user to directly infringe a copyright or if there is other encouragement to infringe. The manufacturer of a "staple item of commerce"–defined by the Supreme Court as a product capable of "commercially significant noninfringing uses"–will not be found liable for contributory copyright infringement, however.[72]

– TEACH Act: At the end of 2002, Congress enacted the Technology, Education and Copyright Harmonization Act, which amended the Copyright Act to provide for digitally-delivered distance education. The TEACH Act expanded the scope of the traditional in-class and broadcasting exemptions to the copyright holder's exclusive right to authorize a public

---

69 § 1202(a).
70 § 1202(b).
71 § 1204.
72 *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 442-43 (1984).

performance.[73] These exemptions had been tied to technology and, with the emergence of the Internet, had become outmoded over time.

The TEACH Act permits transmissions in connection with online education, subject to specific conditions. One of these is that technological protection measures, such as password protection to enable access to Websites, must be used. And where digital transmission is used to disseminate the materials, the institution must use DRM technologies that "reasonably prevent" the students both from retaining the works for longer than the period of the class session and from further disseminating the works.[74]

The TEACH Act also required the Under Secretary of Commerce for Intellectual Property, after consultation with the Register of Copyrights, to submit a report to Congress on technological protection measures to protect digitized copyrighted works and to prevent infringement. The report, which is a useful, high-level overview of the subject, was submitted in December 2002.[75] The Report identified various "core technologies" used to protect content, including encryption, digital watermarking, authentication and DRM systems. Within the field of DRM, the Report discusses the concepts of "trusted computing" and "rights models and rights expression languages," and discusses different types of DRM architecture and systems. Finally, the Report lists and summarily describes a wide range of companies; private, voluntary industry-led initiatives; standard setting and related organizations; and trade associations involved in developing, promoting and standardizing DRM and other technological protection measures.

– Safe Harbors for Online Service Providers: The Online Copyright Infringement Liability Limitation Act was enacted in 1998 as part of the DMCA. It provides for "safe harbors" from copyright liability for various kinds of activities, including transmission, system caching, storage of third-party material and the provision of information location tools.[76] These safe harbors are only made available if the service provider complies with some general conditions. One of these is that the service provider "accommodates and does not interfere with standard technical measures."[77] A service provider that strips out or does not otherwise design its system to accommodate such measures would not be specifically penalized but would lose its eligibility for the safe harbor.

For this reason, it is not surprising that the definition of "standard technical measures" includes concepts of industry-wide agreement and ready implementation. The definition specifically states that such measures–as used by copyright holders to identify and protect copyrighted works–must have been developed "pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; are available on reasonable and non-discriminatory terms; and do not impose substantial costs on service providers or substantial burdens on their systems or networks."[78] By contrast, Section 1201 of the DMCA contains no definition of "technological measure." Differing from the principles embodied in the definition of "standard technical measure,"

---

73 17 U.S.C. § 110(2).

74 § 110(2)(d)(ii).

75 See *Technological Protection Systems for Digitized Copyrighted Works: A Report to Congress* (December 2002), available at *http://www.uspto.gov/web/offices/dcom/ olia/teachreport.pdf*.

76 17 U.S.C. § 512.

77 § 512(i)(1)(B).

78 § 512(i)(2).

Section 1201 would protect proprietary DRMs that are developed or adopted unilaterally, that are priced high or as to which compliance might be technically burdensome–except to the extent the "no mandate" provision permits products to not respond to such measures.

– Audio Home Recording Act: The Audio Home Recording Act, enacted in 1992, mandates the inclusion of the "serial copy management system" ("SCMS"), or a functionally equivalent system, in all "digital audio recording devices" manufactured, imported or distributed in the United States of America.[79] The purpose of the Act was to limit uncontrolled serial copying of music; an unlimited number of first generation digital copies of a recording can be made, but the making of further digital copies from those copies is technologically proscribed. The Act also prohibits trafficking in devices or the provision of services "the primary purpose or effect of which" is to circumvent any program or circuit that implements SCMS (or a system with the same functional characteristics as SCMS);[80] the act of circumvention is not itself prohibited.

The Act also protects information encoded in a digital musical recording of a sound recording. It is forbidden to encode inaccurate information regarding the category code (which relates to the type of device implementing the system), copyright status (copyright asserted or not) or generation status (original or copy) of source material for a recording.[81] The Act also imposes levies on digital audio recording devices and digital audio recording media.[82] Finally, the Act provides for civil remedies, including injunctive relief and an award of actual or statutory damages.[83]

– Computer Fraud and Abuse Act: In 1986, Congress enacted the Computer Fraud and Abuse Act, which might be relevant where the circumvention of a DRM system occurs by accessing a computer, whether a server or a personal computer, without authorization. The Act provides both civil and criminal remedies against "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer if the conduct involved an interstate or foreign communication."[84] It also prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage."[85] In general, the act of unauthorized access must have caused US$5,000 in damage to be actionable.

– Communications Act: The Communications Act prohibits the sale and distribution of "black boxes" that decrypt encrypted signals in three separate provisions. First, it protects conditional access technologies used to encrypt satellite cable programming or direct-to-home satellite services by prohibiting the manufacture, assembly, modification and trafficking in any device that a person knows (or has reason to know) will "primarily be of assistance in the unauthorized decryption" of such programming.[86] Civil damages (actual and statutory) may be recovered and criminal penalties include a fine of up to US$500,000 and a prison term of up to five years.

---

79 17 U.S.C. § 1002.
80 § 1002(c).
81 § 1002(d).
82 § 1003.
83 § 1009.
84 18 U.S.C. § 1030(a)(2)(C).
85 § 1030(a)(5)(A)(iii).
86 47 U.S.C. § 605(e)(4).

Second, the Communications Act has long prohibited unauthorized interception of any radio communication, and the unauthorized reception (or assistance in the receipt) of a radio communication for a person's own benefit or for another person not entitled to have access to such communication.[87] Civil damages are recoverable. In addition, a willful violation can result in a fine of up to US$2,000 and a prison term of six months. If the act was done for purpose of direct or indirect commercial advantage or private financial gain, the penalties include a fine up to US$50,000 and a prison term of two years for the first conviction.

Third, unauthorized interception or reception of any communications services offered over a cable system is prohibited.[88] The prohibited acts include the manufacture or distribution of devices intended for such unauthorized reception. Civil damages are recoverable. Violations are punishable by a fine of up to US$1,000 and a prison term of up to six months, with higher penalties if the acts were for commercial advantage or private financial gain (up to US$50,000 and two years for the first conviction).

– State Communications Security Laws: Many states have long had laws on their books that prohibit theft of cable and telecommunications services, video piracy and computer crimes. Since 2002, a substantial effort has been underway to modernize these laws for the digital environment. A coalition of the motion picture industry and communication service providers, such as cable operators and programmers, has been urging that the states facilitate eCommerce by addressing the protection of content streamed or downloaded over the Internet and through broadband services.

This group is promoting "Model Communications Security Legislation," which would provide more comprehensive legal protection for all broadband and Internet-based services against unauthorized access, receipt, transmission and decryption. In addition, technological measures used to protect programming content would be legally protected from circumvention by outlawing devices that facilitate unlawful access. The Model Communications Security Legislation is seen by its critics as a state-level counterpart to the DMCA. As of this writing, the model legislation or variants thereof has been adopted in several states and is under consideration in several more.

In summary form, the model law, as it has evolved in discussions with technology companies and other interests, would prohibit, among other acts:

– the knowing, and with the intent to defraud a communication service provider, possession, use, manufacture, development, promotion and trafficking of any "communication device" for the commission of the theft of a "communication service" or to receive, intercept, decrypt or acquire a communication service without consent as set forth in a contract;

– the modification, alteration or reprogramming of a communication device for such purposes;

– the possession, use, manufacture, development, promotion and trafficking of any "unlawful access device"; or

– the possession, use or trafficking of any (1) plans or instructions for making or assembling any "communication device" or "unlawful access device" for any of these prohibited purposes or (2) material, including hardware, data, computer software or other

---

87 § 605(a).

88 § 553.

information, knowing that the purchaser or a third person will use such material in manufacturing, assembling or developing an unlawful access device or a communication device for a prohibited purpose.

Violations of these provisions would give rise to both civil and criminal penalties.

The Model Communications Security Legislation has comprehensive definitions, which are summarized below:

– "Communication device" would include both any equipment that is capable of intercepting, transmitting, acquiring, decrypting or receiving any communication service, and any component thereof, including any number, circuit, switch, card, software or chip that is "capable of facilitating" any interception, transmission, decryption, acquisition or reception of any communication service.

– "Communication service" is defined comprehensively, and essentially includes any conceivable service that, for a fee, provides content over any medium of communication, including the Internet.

– Finally, an "unlawful access device" is defined broadly to include any device, technology or software that is "primarily designed, developed, assembled, manufactured" or trafficked in "for the purpose of defeating or circumventing any effective technology, device or software, or any component or part thereof," used to protect any communication, data or service from unauthorized acquisition, interception, access, decryption or disclosure.

The Model Communications Security Legislation is seen as broader than the DMCA itself and, for that reason, has been controversial in some quarters. It prohibits both the act of circumvention and tools that circumvent. The model legislation does not include the exceptions and limitations (such as those for reverse engineering and encryption research) in the DMCA. More recent iterations, however, have included a "no mandate clause," which is intended to carve out legitimate products from the scope of the prohibitions.

3.2.1.3 Regulatory Activities

3.2.1..3(a) Copyright Office Rulemaking

As described above, Congress was concerned that Section 1201(a)(1) of the DMCA would affect traditional fair uses of copyright material because the law prohibits circumventing access control technologies even for such uses. In the course of legislative consideration, however, Congress determined not to amend the bill to authorize circumvention of access controls in connection with a non-infringing activity. Instead, it established a process by which the Librarian of Congress would have to define "particular class[es] of works" as to which the act of circumventing technological measures by particular persons would be permitted.[89] The Librarian is required to determine every three years (after the initial two-year period) whether, as to such class, persons are, or are likely to be, "adversely affected" by virtue of Section 1201(a)(1) in their ability to make non-infringing use of that class of works.

[89] 17 U.S.C. § 1201(a)(1)(C).

The Librarian is instructed to examine a variety of factors in reaching a decision, including the availability for use of works (particularly nonprofit archival, preservation and educational uses); the impact of Section 1201(a)(1) on traditional fair uses; and the effect of circumvention on the market for the works.

On October 28, 2000, in the first such decision, the Librarian ruled that only two narrow classes of works would benefit from an exemption from the prohibition for the next three years: compilations of Websites blocked by filtering software applications and literary works that fail to permit access because of malfunction, damage or obsoleteness.[90] Currently, the Copyright Office of the Library of Congress, which must make a recommendation to the Librarian, is in the midst of the second such rulemaking proceeding, which must be concluded by October 28, 2003.[91]

The burden on those who are attempting to obtain an exemption has proven to be quite substantial. First, they must show that they have actually been, or will actually be, "adversely affected" in their use of works by the anti-circumvention provision. Naturally, it has been difficult to meet this burden because access control technologies are not yet in widespread use.

Second, they must show that they are impaired with respect to a "class of works." It has proven somewhat difficult for the Copyright Office to define a "class of works." Although commenting parties sought an exemption for "fair use works," the Copyright Office denied that request because there a "class of works" may not be determined by reference to how the works might be used. The Office concluded that the statutory language and the legislative history precluded the grant of broad exemptions for fair use.

Some fair use advocates and others who have opposed both the DMCA generally and the narrowness of its exceptions may have hoped that these proceedings would have resulted in a more refined calibration of the DMCA than was possible during the congressional debate. In the current proceeding, for example, they have asked the Copyright Office to determine that circumvention be permitted for such specific purposes as avoiding DVD region coding or unskippable DVD advertising, accessing public domain films on DVD and such general purposes as engaging in research relating to access control technologies and obtaining access to any works protected by access control mechanisms that require use of a DRM system specified by the rights holder. Based on the standards set out in the Librarian's October 2000 decision, the language of the DMCA and the associated burden of proof make it unlikely that many or broad "classes of works" will be exempted from the prohibition of Section 1201(a)(1). In this regard, the Register of Copyrights has suggested that any arguments that the possible categories of works eligible for an exemption should be broadened, or that the evidentiary burden of qualifying for an exemption should be lightened, ought to be made to Congress.[92]

Finally, it should be pointed out that even where an exemption is made available for a particular class of works, only the act of circumvention would be permitted. Tools for

---

[90] Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556 (October 27, 2000); 37 C.F.R. § 201.

[91] Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 67 Fed. Reg. 63578 (October 15, 2002).

[92] 65 Fed. Reg. at 64562.

circumvention continue to be proscribed.[93] Yet, without tools that would enable the ordinary users to circumvent, having the right to circumvent an access control measure may be of little use indeed. Section 1201(a)(2) would, notwithstanding any exemption for the act itself, continue to prohibit trafficking in circumvention tools; arguably, such a tool might fail to satisfy the tests of that section if it were primarily designed or produced for the purpose of circumvention in those circumstances where the Librarian had so authorized (and had limited other uses).

3.2.1.3(b) Federal Communications Commission: Broadcasting Flag Rulemaking

Rights holders have contended for several years that among the most critical missing pieces of the protection available for content in the digital era is safeguarding digital free, over-the-air broadcast television content–which is transmitted without any native encryption. Conditional access schemes are able to protect content until it reaches the home. As noted in Section 3.2.1, new technologies–DTCP, HDCP and CPRM–are available to protect audiovisual and audio content from unauthorized distribution on networks within the home, or from the home to the Internet, and to record content securely. To be protected by those technologies, however, content must be delivered in a protected form, such as by a conditional access system, or by some other mechanism that signals that the content is to be protected in the home.

Rights holders have been very concerned that digital broadcast television content, not being protected as it enters the home, may then be copied, routed to the Internet or otherwise be subject to unauthorized distribution. As a result, they may well be less willing to make high-quality programming available to over-the-air digital broadcast television.

Responding to these concerns, various private sector interests began evaluating possible approaches in the forum of the Copy Protection Technical Working Group ("CPTWG"), which, in November 2001, established the Broadcast Protection Discussion Group. (Since 1996, the CPTWG has been meeting monthly in Los Angeles, California to evaluate technical approaches to copy protection issues.) In June 2002, the co-chairs of that group released a report reflecting what was largely a multi-industry consensus on a reasonable approach to addressing this problem. The report recommends that the Redistribution Control Descriptor in the ATSC Standard A/65A–the so-called "broadcast flag"–be used to signal that digital broadcast television content is to be protected.

Among the central issues recognized by all parties was the question of enforcement: any private sector consensus on the desirability of using a broadcast flag essentially would be without significance unless there were a mechanism for ensuring that devices would detect and respond to the presence of a broadcast flag. In particular, to ensure that all products receiving digital broadcast content would behave properly, it was widely (but not uniformly) agreed that some form of governmental mandate would be required.

A further set of issues concerns the rules that would apply to devices that receive broadcast content, either before they look for a broadcast flag or once they detect its presence. These include 1) the extent to which the broadcast content should be protected and 2) to

---

[93] 17 U.S.C. § 1201(a)(1)(E).

which analog and protected digital outputs a product that is governed by these rules is permitted to send content that has been marked with the broadcast flag. Another issue is circumvention: to what level of "robustness" should devices be designed and manufactured when they implement these requirements, to avoid ready bypass or defeating of the broadcast flag.

To answer these and other questions, the Federal Communications Commission ("FCC") began a rulemaking proceeding in August 2002.[94] The FCC is evaluating whether it should mandate that devices recognize and give effect to the ATSC flag or some other signal; whether and how devices downstream from the receiver should be required to protect digital broadcast content; and what criteria should be used to determine which output protection technologies are authorized to receive content marked with the broadcast flag.

The FCC received many comments on these proposals from industry participants and the public at large. The principal supporters of issuance of a regulatory mandate by the FCC are rights holders, such as the motion picture industry, television broadcasters and some of the major technology companies. Many dissenting views were expressed, however, by some technology companies (principally with respect to whether the FCC should be regulating devices), as well as by many consumers and public interest groups. Among the principal points of contention is whether a regulatory requirement that digital broadcast content marked with the broadcast flag must be recorded securely would either curtail legitimate in-home personal recording and playback practices or impair the ability to send content over a home digital network. Further issues for discussion have included whether marking with the broadcast flag should be prohibited for certain types of content–for which distribution may be permissible, or desirable, such as emergency programming.

Finally, with respect to protecting digital broadcast content, it is broadly agreed among rights holders and some major technology companies that a common approach must be adopted internationally. Although the FCC's adoption of the broadcast flag might well result in significantly limiting the flow of marked digital broadcast content to the Internet in the United States of America, over-the-air television programs broadcast in the United States of America can be received in neighboring countries, from which they could then be redistributed. Similarly, when such programs are broadcast digitally without encryption outside the United States of America, they also may be captured by receiving devices and then routed to the Internet. Accordingly, it is thought that if the FCC chooses to adopt a broadcast flag requirement, then similar governmental mandates may–and may need to–be sought in other jurisdictions.

3.2.1.3(c) Federal Communications Commission: Cable-Consumer Electronics Compatibility Rules

Another area of rights management in which the FCC has become involved arose from efforts to ensure that there is compatibility between cable services and consumer electronics devices, such as High Definition Television ("HDTV") sets. In December 2002, after lengthy and intensive negotiations, major consumer electronics manufacturers and the leading cable operators entered into a comprehensive agreement to ensure "plug and play" compatibility

---

94 In the Matter of Digital Broadcast Copy Protection, Notice of Proposed Rulemaking, MB Docket No. 02-230, 67 Fed. Reg. 53903 (August 20, 2002).

between one-way cable services and the next generation of digital television sets, without the need for set-top converter boxes; to enable consumers to receive and record HDTV signals; and to allow new devices to be connected to HDTV sets.

Having concluded their private-sector negotiations, the parties to the agreement then took their agreement to the FCC. They have jointly recommended that the FCC mandate the arrangement and have the requirements on which they have agreed apply to all types of providers of pay television programming, cable and satellite alike, as well as to equipment manufacturers. Government mandates are critical, in the eyes of the promoters of the agreement, in order to ensure a "level playing field" among all industry players. And they have argued strongly that both Congress and the FCC have expressed the view that the FCC ought to implement compatibility requirements in a universal manner that encompasses both satellite and cable systems.

Importantly, throughout the process, the FCC expressed the strongest encouragement for these private-sector negotiations. Indeed, it invited the joint submission because it believed that ongoing and unresolved disputes about content protection for television programming were significant impediments to effecting the transition to digital television in the United States of America.

With respect to DRM-related issues, the parties are asking the FCC to adopt rules addressing copy protection of pay television programming, to include federally mandated encoding rules. These rules, if adopted by the FCC, would govern the extent to which consumers would be able to record certain types of programming received via satellite and cable (but not including services delivered through use of a cable modem or the Internet). From the standpoint of consumer electronics manufacturers and consumer interests, these rules are an integral and necessary part of the agreement.

In general, the specific encoding rules on which the parties have agreed and that the FCC is considering are modeled on those set out in the DTCP technology license and in Section 1201(k) of the DMCA.[95] The rules would permit the rights holders of television programs to mark their content so that (1) only one generation of copies may be made of a program delivered by a monthly subscription service; (2) programs sold through pay-per-view, video-on-demand and subscription video-on-demand services may be restricted to no copies, but may be stored for 90 minutes (or more, if agreed) on a personal video recorder; and (3) free, over-the-air broadcast content may be copied freely. The proposed rules would also address the issue of whether and how to permit encoding of content delivered through new and undefined business models (i.e., other than by the types of services described in the preceding sentence) and for updating these encoding rules; the proposal provides that operators may apply different encoding rules for new business models, but that any such rules are subject to the possible filing of a complaint with–and resolution by–the FCC.

Shortly after the agreement was submitted to it, the FCC launched a proceeding to obtain public comment, including with regard to the proposed rules.[96] Naturally, the encoding

---

[95] See note 56, describing Section 1201(k).

[96] In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, CS Docket No. 97-80, Compatibility Between Cable Systems and Consumer Electronics Equipment, PP Docket No. 00-67, Further Notice of Proposed Rulemaking, 68 Fed. Reg. 2278 (January 16, 2003).

rules (and other elements of the agreement) are supported by the parties to the agreement and similarly situated entities. Satellite operators object to being covered by the rules.

Furthermore, at least some consumer-oriented groups have expressed strong reservations, particularly with respect to whether there should be any mandated encoding rules; they are fearful that the rules will effectively eliminate some fair use recording of certain types of programming for which home recording is now permitted. Many rights holders, while expressing limited support for the agreements, also were quite critical, particularly with respect to the inclusion of encoding rules that, they believe, would constrain their ability to determine which business models to use to distribute content over conditional access systems. Conversely, other participants expressed reservations that, under the agreement, the encoding rules could be too easily changed or be made inapplicable by operators.

3.2.1.4 Legislative Proposals

After the enactment of the DMCA, many other legislative proposals have been introduced in Congress to address a range of issues–from amending the DMCA itself, to establishing a higher profile for government in establishing DRM schemes, to allowing rights holders to engage in "self-help" solutions against unauthorized distribution of content. None of the bills introduced in the 107th Congress (which ended in 2002) was enacted into law. None of the bills introduced in the current (108th) Congress has yet been enacted. Nevertheless, these proposals are instructive in highlighting some of the open and contentious issues that remain after the United States of America implemented the WIPO Treaties. These proposals are summarized below:

– Amending the DMCA: Authorizing Fair Use Circumventions: In October 2002, two bills were introduced to amend the DMCA to permit circumvention in certain circumstances. First, H.R. 5544, the Digital Media Consumers' Rights Act, would have created an exemption for activities "solely in furtherance of scientific research into technological protection measures."[97] The bill also would have permitted circumvention of a technological measure "if such circumvention does not result in an infringement"–that is, to permit circumvention in aid of a fair use.[98] Finally, the bill would have authorized the manufacture, distribution or non-infringing use of a "product capable of enabling significant non-infringing use of a copyrighted work"–essentially to restore the contributory liability standard articulated by the Supreme Court.[99] Rep. Richard Boucher, the bill's principal promoter, stated that his bill addressed the threat to fair use posed by the technological measures protected by the DMCA. In January 2003, Rep. Boucher re-introduced the Digital Media Consumers' Rights Act as H.R. 107.[100]

Second, H.R. 5522, the Digital Choice and Freedom Act, also was introduced with a view toward addressing the DMCA's endangerment of legitimate consumers' rights and expectations.[101] The bill would have modified the copyright law and the DMCA in several

---

97 H.R. 5544, 107th Cong., 2d Sess. § 5(a) (2002).
98 *Id*. § 5(b).
99 *Id*.
100 H.R. 107, 108th Cong., 2d Sess. (2003).
101 H.R. 5522, 107th Cong., 2d Sess. (2002).

ways. It would have added a new limitation on copyright owners' exclusive rights: persons who lawfully acquired a copy of a digital work, or lawfully received a transmission of the work, would have been entitled to "reproduce, store, adapt or access the work" for archival purposes or to perform or display the work for non-commercial purposes,[102] presumably without regard to the application of any technological measures. In addition, the bill would have amended the DMCA to expressly state that a person could circumvent any technological measure if the measure would prevent a non-infringing use and the copyright owner does not make available the means needed to perform such use.[103] Finally, the bill would have specifically excepted from the device-oriented anti-circumvention provisions of the DMCA those products that are designed, produced or marketed for the purpose of circumvention of a measure if that measure prevents non-infringing uses and the rights owner does not make available the means needed to make such uses.[104]

A broad range of copyright owners and affiliated interests have opposed both H.R. 5544 and H.R. 5522 in the 107th Congress and H.R. 107 in the current Congress. They have argued that these bills would raise prices and stifle innovation in DRM and digital distribution technologies. Furthermore, although they concede that the proposals would permit circumvention of DRM technologies in aid of fair use, they emphasize that the products that would thereby be permitted could also be used to circumvent DRM systems for altogether illegitimate purposes. Additionally, they contend that because the DMCA is balanced and has, therefore, been a model for other countries, the adoption of H.R. 107 would establish a bad precedent internationally: that the United States of America believes some level of circumvention is acceptable.

– Government Standard Setting for DRM Technologies: Perhaps the most visible and controversial DRM-related bill considered by Congress in the post-DMCA implementation era was S. 2048, the Consumer Broadband and Digital Television Promotion Act, which was introduced in March 2002.[105] The bill placed in sharp relief differences in perception with respect to the appropriate roles of the private sector and government in setting standards, including with respect to DRMs. Sen. Ernest Hollings, at the urging of some motion picture companies, introduced and was the principal sponsor of S. 2048. The purpose of the legislation was to create substantial incentives for the private sector to reach an agreement on "security system standards" for digital devices and on encoding rules. If they failed to do so, the government would step in and mandate standards. The agreed-upon standards would have had to meet certain standards elaborated in the bill, and the encoding rules would have had to permit personal copying from broadcast and pay television cable and satellite television.[106]

Essentially, the bill gave the private sector 12 months to conclude such an agreement. If, at the end of that period, the FCC determined that the private sector had successfully done so, then the FCC, by regulation, would be required to mandate those technology standards and encoding rules by embedding them in regulation.[107] If the FCC determined, however, that the private sector had failed to do so, then the bill would have required that the FCC itself adopt

---

102 *Id*. § 3 (proposing to add a new § 123 to the Copyright Act).
103 *Id*. § 5.
104 *Id*.
105 S. 2048, 107th Cong., 2d Sess. (2002).
106 *Id*. § 3(d).
107 *Id*. § 3(b).

government-developed DRM standards and encoding rules–meeting the statutory criteria–within thirteen months after making that determination.[108] The bill would have permitted the private sector to modify agreed-upon or government-mandated standards in circumstances where the technology had been compromised or in light of technological improvements.[109]

In addition, S. 2048 contained a set of provisions to ensure that manufacturers and rights holders would comply with the standards. The first would have prohibited the sale of future "digital media devices"–defined as digital recording, conversion, or retrieval or access devices–if they failed to comply with the standards.[110] The second would have prohibited the knowing removal or alteration of a technology that complied with the standards or the knowing transmission of copyrighted material where the security measure had been removed or altered.[111] The third would have prohibited the application of a security technology in violation of the encoding rules.[112]

On its face, S. 2048 did not reveal which specific problems or gaps in DRM technologies–or failures of the private sector–it was intended to address. The bill would have had Congress find that existing agreements did not provide a secure digital environment and that existing DRM schemes provide only proprietary, partial solutions. The potential congressional findings also would have been critical of the private sector, stating that "competing business interests have frustrated agreement on the deployment of existing technology in digital media devices to protect digital content on the Internet or on digital broadcast television."[113] It was known, and congressional hearings demonstrated, that there were three issues of concern to Sen. Hollings and the supporters of S. 2048: (1) the failure to protect over-the-air digital broadcast television from retransmission to the Internet; (2) the difficulty of preventing the retransmission of analog content that had been converted from a protected digital source (the so-called "analog hole" problem); and (3) the threats posed by uncontrolled and unauthorized peer-to-peer file sharing of digital content.

S. 2048 met stiff and virtually unanimous opposition from information technology companies, consumer electronics companies, consumer groups and users of content. There were several arguments against the proposal. First, that the private sector was making progress in addressing these issues–the work on the broadcast flag that culminated in a report that eventually launched the FCC rulemaking described above being a notable example. Second, that it would be highly counterproductive and misguided for government to become enmeshed in developing and mandating standards. Third, that government should not set artificial deadlines for private sector efforts to find technological solutions, especially for the extremely thorny problem of file sharing. The bill's principal proponents were the motion picture studios and affiliated broadcasting interests.

– Self-Help Solutions to Address File Sharing: An altogether different approach toward the issues of content protection would have encouraged the development and use of "self-help" solutions to block unauthorized peer-to-peer file trading. Rights owners and Congress had been frustrated by the inability of technical measures to address such systems.

---

108 *Id*. § 3(c).
109 *Id*. § 3(h).
110 *Id*. § 5.
111 *Id*. § 6.
112 *Id*.
113 *Id*. § 2.

The copyright infringement suits brought against Napster and other file trading systems, though successful from the rights holders' viewpoint, were time consuming and could only attack the problem one system at a time. And where the systems are fully distributed, with none of the centralized directories or servers of Napster and similar services, using litigation to stop massive amounts of file sharing could prove to be an immensely difficult enterprise.

Increasingly, rights holders began to consider whether and how they could deploy technologies to interfere with unauthorized file trading–technologies such as interdiction, decoys, redirection, file-blocking or spoofs. In using these tools, however, copyright owners had some concerns that these activities might themselves become a magnet for litigation brought by file traders, other adversely affected users and consumer organizations.

To address these concerns, H.R. 5211, the Peer-to-Peer Piracy Prevention Act, was introduced in July 2002, with Rep. Howard Berman its principal sponsor.[114] Upon introducing the bill, he commented that although the development and deployment of DRM solutions should be encouraged, these approaches would not completely address the problem of file sharing since the copyrighted works that are distributed through peer-to-peer systems are already "in the clear" on the Internet.

H.R. 5211 would have granted a copyright owner an unqualified safe harbor in engaging in self-help activities directed at file sharing, provided that there were no collateral consequences. A copyright owner would have had a complete shield from any criminal and civil liability under any federal or state law for "disabling, interfering with, blocking, diverting or otherwise impairing" any unauthorized use of the copyrighted owner's own copyrighted work on a "publicly accessible peer-to-peer file trading network."[115] The safe harbor would have been available, however, only on the condition that the copyright owner's act would have no effect on any other computer file or data on the file trader's computer. The safe harbor would not be available if economic loss was caused to a person other than the file trader or if there was more than US$50 worth of impairment to the property of the affected file trader (not including the copyright owner's own works).[116]

A further condition on the availability of the safe harbor was that the copyright owner must have days earlier notified the Department of Justice of the specific technologies that the copyright owner thereafter intended to use to impair the unauthorized file-trading activities.[117] Copyright owners also would have to give notice to the affected file trader, if requested, of the reason for impairing the file trading; notice would not need to be given prior to launching the impairment tool. Egregious impairment activities of the copyright owner that result in real economic loss to the file trader would entitle the injured person to file a claim for compensation. The Department of Justice could have enjoined copyright owners who engaged in a pattern of abusive impairment activity without having had a reasonable basis for believing that infringing behavior had occurred.[118]

H.R. 5211 was opposed by some interests because, in their view, the bill was not limited to authorizing a copyright owner to impair only the unauthorized use of its own work. They

---

114 H.R. 5211, 107th Cong., 2d Sess. (2002).
115 *Id*. § 1(a) (proposing to add a new § 514 to the Copyright Act).
116 *Id*.
117 *Id*.
118 *Id*.

argued that H.R. 5211 would confer immunity for any activities–even those that resulted in destruction of other files–that a copyright owner undertook in aid of stopping infringing peer-to-peer activity. They also argued that any copyright owner could attack a file trader's computer using any impairment technology, provided merely that the owner had previously notified the Department of Justice. The bill's proponents pointed to the narrowness of the safe harbor and emphasized that a copyright owner would be barred from altering or removing any files on a file trader's computer, though blocking the transmission of the copyright owner's own work would have been permitted by the bill.

– Prohibiting Trafficking in Illicit Authentication Features: Congress has also considered strengthening the anti-counterfeiting law to prohibit trafficking in an "illicit authentication feature affixed to or embedded" in a copy of a computer program, motion picture, other audiovisual work or a phonorecord. S. 2395, the Anticounterfeiting Amendments of 2002, was introduced in April 2002 for just this purpose.[119]

S. 2395 defined an "authentication feature" to include watermarks, symbols, codes, certifications, holograms and other means used to identify that a copy or phonorecord is not counterfeit. An "illicit authentication feature" was defined as an authentication feature that is genuine in origin, but either has been tampered with or altered "for the purpose of inducing a third party to reproduce or accept distribution" of the copy or has been distributed without authorization of the copyright owner and not in connection with a lawfully made copy to which the authentication feature was intended to be embedded. In other words, it would have been unlawful to alter an element of a DRM system, such as a watermark or computer code, that verifies that a copy of a work is authentic, and then to distribute that element to facilitate the distribution of pirated copies. Civil and criminal remedies would have been available.

Because S. 2395 essentially was an anti-counterfeiting bill it did not initially attract much opposition. Some interests opposed it when they interpreted the proposal to apply potentially to technologies or acts that would impair digital watermarks. In March 2003, the bill was reintroduced, as S. 731, the Secure Authentication Feature and Enhanced Identification Defense Act of 2003, but it was much narrowed, to apply only to protect government-issued authentication features.[120]

– Mandated Disclosure of Technological Measures: One legislative proposal that does involve government in DRM technologies, but would, if enacted, be less intrusive than several of the bills discussed above, would simply require that consumers be adequately informed about the use of technological features that would restrict their ability to use content. S. 692, the Digital Consumer Right to Know Act, was introduced in March 2003 to create market-based incentives to develop DRM systems that address problems of unauthorized reproduction and distribution, but "preserve the maximum possible flexibility for consumers to use and manipulate" content lawfully.[121]

S. 692 would require that the Federal Trade Commission issue rules to require producers or distributors of copyrighted digital content to disclose conspicuously any technological features that would limit the ability of consumers to play, copy, transmit or

---

119 S. 2395, Anticounterfeiting Amendments of 2002, 107th Cong., 2d Sess. (2002).
120 S. 731, 108th Cong., 1st Sess. (2003).
121 S. 692, 108th Cong., 1st Sess. (2003).

transfer such content between commonly used consumer devices.[122] The bill's proponent describes such advance notice as a matter of basic fairness, so that consumers' customary uses are not unexpectedly stifled. Specifically, S. 692 would mandate the disclosure of any technological limitations on the following practices: time-shift recording of broadcast or pay (but not pay-per-view) programming; space-shifting or platform-shifting of audio or video content (e.g., between home and office or to portable devices); making back-up copies of legally acquired content; using excerpts for fair use-type purposes; and transferring or selling legally acquired content to another consumer (where the transferor/seller retains no further rights in the content).[123]

3.2.2 Case Law

Several judicial decisions in the United States of America have now interpreted the anti-circumvention provisions of Section 1201.

Universal City Studios, Inc. v. Corley:[124] The most significant DMCA-related case involves a suit brought by eight major motion picture studios against the defendants, who operated a Web-based publication. The defendants had posted, and encouraged others to copy and distribute, a decryption algorithm known as DeCSS. DeCSS allows users to crack or circumvent the technological measure–CSS–which restricts unauthorized access to DVD video disks. The defendants also linked to other Websites where DeCSS was posted. The principal defense in the case was that the anti-trafficking provisions of Section 1201(a)(2) were unconstitutional because they violated the defendants' First Amendment right to free speech by means of the exchange of DeCSS source code.

The district court found that CSS "effectively controls access" to motion pictures on DVD video disks, inasmuch as keys are required to access the motion pictures, and the keys cannot be obtained without a CSS license from the DVD CCA. The court also rejected defendants' argument that because CSS was "weak" encryption it should not be considered an "effective" technological measure, noting that the statute would be rendered meaningless if it only protected completely effective measures.

The district court rejected all of the defenses. It categorically concluded that defendants failed to satisfy the conditions for coming within the three Section 1201 exemptions that they claimed applied to their activities (reverse engineering, encryption research and security testing). It also found that fair use does not apply in an action brought under Section 1201.

The defendants were ordered not to post DeCSS on their Website. The injunction also prohibited the defendants from linking to other sites that carried DeCSS. The court noted that enjoining such linking would help to prevent the spread of DeCSS, especially where the links are to Websites outside the United States of America.

---

122 *Id*. § 3(a).

123 *Id*. § 3(c). H.R. 107, cited above, also has a provision that takes a disclosure-oriented approach; it would direct the Federal Trade Commission to ensure adequate labeling of CDs that are copy-protected.

124 273 F.3d 429 (2d Cir. 2001), *aff'g Universal City Studios, Inc. v. Reimerdes,* 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

In November 2001, the U.S.A. Court of Appeals for the Second Circuit affirmed the decision of the district court in all respects. The court found that the injunction was constitutional because it was "content-neutral"–it targeted only the functional, non-speech components of the decryption code (and, in the case of linking, only the functional, not expressive, aspects of the hyperlink)–and it had only an incidental effect on the defendants' speech.

The court of appeals specifically examined the question of whether circumvention of CSS was permitted where done to aid in a fair use of motion pictures on DVD video disks. Interpreting Section 1201(c)(1), the court concluded that the DMCA targets the circumvention of digital protections through its anti-trafficking provisions, but does not concern itself with the use of the content after circumvention has occurred. It rejected the notion that Congress intended to permit "fair use" circumvention. Finally, the court disagreed with defendants' position that the DMCA was unconstitutional insofar as it eliminated the ability to make fair use of copyrighted works protected by access control; the court found that the fair use doctrine did not guarantee that anyone would have access to copyrighted material.

RealNetworks, Inc. v. Streambox, Inc.:[125] An earlier decision involved a suit brought by RealNetworks under Section 1201(a) and Section 1201(b). RealNetworks had developed a content delivery system that permits rights holders to encode their works in a digital form, and then communicate them, using the RealServer, via a secure method to consumers. Consumers must use a RealPlayer to access the works. Together, the RealServer and RealPlayer allow for streaming, but not copying, of works using both an authentication sequence and a copy switch (which allows the rights holder to determine whether copying is authorized or not). Streambox had developed a product that substitutes for the RealPlayer and tricks the RealServer into thinking that proper authentication had occurred; the product does not respond to the copy switch, so that consumers can record streamed content.

The court concluded that the authentication was a technological measure that effectively controls access, within the meaning of Section 1201(a). The copy switch, when used with the authentication, was a Section 1201(b) technological measure because it enabled a rights holder to control consumer copying. Accordingly, the court granted the injunction against the distribution of the product, finding that it was primarily designed to circumvent both access control and copy control technological measures and had no other commercially significant purposes. The parties reached a settlement in September 2000.

Sony Computer Entertainment America, Inc. v. GameMasters, Inc.:[126] An early decision, rendered shortly after enactment of the DMCA, found that a product sold by the defendant violated Section 1201(a)(2)(A). Sony's PlayStations are designed so that they authenticate video games; each video game has a region code that must match the geographic location in the game console before the game can be played. The defendant's product plugged into a Sony PlayStation console and enabled a consumer to play imported or non-territorial video games. The court enjoined the product because it found that its primary function was to circumvent the region coding authentication function.

---

125 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).

126 87 F. Supp. 2d 976 (N.D. Cal. 1999).

United States of America v. Elcom, Ltd.:[127] Dmitry Sklyarov, a Russian programmer, was indicted for violating the DMCA's anti-trafficking provisions. As an employee of the Russian company Elcom, he created software that decrypted the Adobe eBook security software, which both allowed users to read eBooks in multiple formats and allowed them to copy eBooks. Elcom moved to dismiss the indictment, challenging the DMCA on various constitutional grounds, including that Section 1201(b) was unconstitutionally vague, that the section restricted the content of its speech and that it curtailed third parties' rights to engage in fair use of copyrighted material. In May 2002, the district rejected each of these claims and denied Elcom's motion. Echoing the decision in *Corley*, the court concluded that even if the DMCA directly regulated constitutionally protected expression, it did not affect the public's right to use either public domain or copyrighted works because it affects only the ability to access and use particular copies of those works.

Various other cases are pending with respect to the interpretation and application of the DMCA. In one case, a software manufacturer is seeking a declaratory judgment that software that enables the copying of DVD video disks does not violate the anti-circumvention provisions of the DMCA.[128] One of the most interesting developments in the United States of America is that the DMCA is now being interpreted broadly to prohibit circumvention of non-DRM technologies that manufacturers use in various industrial applications, with the effect that competitors and their products are prevented from having access to a computer code that a manufacturer may use for purposes of authenticating that only its products are being used by a consumer.[129]

3.3 European Union

3.3.1 Legal Framework

On May 22, 2001, the European Union adopted the Directive on the harmonization of certain aspects of copyright and related rights in the information society ("Copyright Directive").[130] The Copyright Directive implemented the various provisions of the WIPO Treaties, including the copyright-related provisions on the rights of reproduction, communication to the public and distribution, as well as the provisions that prohibit circumvention of technological measures and rights management information. Prior to the adoption of the Copyright Directive, at the European Community level, circumvention of technological measures was addressed in three other directives, dealing with the legal protection of computer programs, conditional access and electronic commerce, which are discussed below.

---

127 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

128 *321 Studios v. Metro-Goldwyn-Mayer Studios, Inc.*, No. C-02-1955 (N.D. Cal., filed April 23, 2002).

129 See, *e.g., Lexmark International, Inc. v. Static Control, Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003) (order granting preliminary injunction) (access to printer engine program involves authentication sequence between printer and toner cartridge).

130 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L167/10, 22/06/2001.

These directives are intended to harmonize the legislation of the Member States. The principles of the directives either have been or must be transposed by the Member States into their respective national laws. In this respect, the Copyright Directive, for example, is somewhat less detailed, particularly with respect to exemptions, than the DMCA–the precise contours of these exemptions, based on the Directive, will be set out in the domestic legislation of each Member State. The deadline for transposition of the Copyright Directive was December 22, 2002.

3.3.1.1 Copyright Directive

3.3.1.1(a) Background

The Copyright Directive was initially proposed in 1997 and, from then until the date of its adoption, was the subject of intensive Community-wide debate involving the main interested sectors–rights holders, information technology and consumer electronics equipment manufacturers and consumer organizations. The early draft of what became the Copyright Directive prohibited "any activities" of circumvention, principally outlawing trafficking in circumvention tools, not the acts of circumvention themselves. Over time, multiple versions of the Directive were prepared and discussed. Among the most significant issues discussed during this period was the fundamental distinction between prohibiting, on the one hand, the act of circumvention and, on the other, the trafficking in circumvention tools, as well as the scope of any exemptions. In addition, the scope of the Directive expanded from prohibiting tools that circumvented copyright control measures to those that also circumvented access controls.

3.3.1.1(b) The Anti-Circumvention Provisions

Article 6 of the Copyright Directive implements both Article 11 of the WCT and Article 18 of the WPPT. Like the DMCA, Article 6 applies to both circumventing acts and circumventing tools, and broadly applies to technological measures that control access as well as copyright.

Article 6(1) prohibits circumventing acts: Member States are directed to provide "adequate legal protection against the circumvention of effective technological measures." Only acts carried out with the "knowledge" or reason to know that the objective of circumvention is pursued are prohibited.

Article 6(2) covers circumvention tools (including services): Member States are directed to provide "adequate legal protection" against trafficking–as well as possession for commercial purposes–of tools that meet one of three tests. They are:

– promoted, advertised or marketed for the purpose of circumvention of; or

– have only a limited commercially significant purpose or use other than to circumvent; or

– are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measure. These tests are quite similar to those in the DMCA and, as such, contain similar uncertainties (e.g., the meaning of

"primarily"). It should also be noted, however, that one of the recitals to the Copyright Directive suggests that national law may also go further than Article 6(2) and prohibit the "private possession" of products for circumvention.[131]

The Copyright Directive builds on the DMCA's approach to defining "effective technological measures." Unlike the DMCA, however, it is this definition–and not separate provisions (along the lines of Section 1201(a) and 1201(b))–that establishes the broad scope of the anti-circumvention provisions as applying to both access and copyright control measures.

Article 6(3) defines technological measures to include any technology that "in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorized by law or the *sui generis* right provided for in Chapter III of Directive 96/9/EC [applicable to databases]." Accordingly, where a technological measure is used to ensure that the authorization of the rights holder is obtained before having access to or using a work, circumvention of the measure–by act or product–is prohibited. In this regard, the concept of "technological measures" is broader than that of the DMCA.

Article 6(3) also defines when a technological measure is "effective." A technological measure is "effective" where use of a work or subject matter is controlled by the rights holder through "an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective." In defining the measures to be protected against circumvention as only those that "achieve[] the protection objective," the Article could be interpreted as stating that only those measures that are, in fact, "effective" shall be deemed to be "effective" for purposes of the Copyright Directive and implementing law. In addition, it is not clear whether an "effective" access control or protection process may only make use of "encryption, scrambling or other transformation" of the work," and whether any type of "mechanism" may be used for "copy control." Furthermore, the Article here uses the term "copy control" instead of "copyright control"; in doing so, the question has been raised as to whether technological measures that control non-copying uses of copyrighted material, such as public performances or distribution, actually fall within the scope of Article 6.

The Copyright Directive is broader than the DMCA because it also prohibits acts of circumventing copyright control measures and other acts not authorized by the rights holder. Assume, for example, that a technological measure is used to condition access to and use of copyrighted content, and that access is made available to the user on the basis of an agreement that controls a person's subsequent use. If that person violates those usage conditions, that would be an "act not authorized by the rightholder." Such an act would be prohibited by the anti-circumvention provisions of the Copyright Directive. (In the United States of America, by contrast, breaching an agreement in this way might be an act of infringement under copyright, but not an act of circumvention outlawed by the DMCA.) The matrix of prohibitions in the Copyright Directive appears as follows:

---

131 Recital 49, Copyright Directive.

	Act of Circumvention	Circumvention Tools
Access Control Technological Measure	Prohibited (Art. 6(1))	Prohibited (Art. 6(2))
Copyright Control Technological Measure	Prohibited (Art. 6(1))	Prohibited (Art. 6(2))

3.3.1.1(c) Limitations and Exceptions

The Copyright Directive, like the DMCA, also provides for limitations and exceptions, but in a manner quite different from that of the U.S.A. law. Article 6(4) does not provide for outright exceptions to the anti-circumvention provisions along the lines of those set out in Section 1201 of the DMCA. Instead, it strongly prefers private sector arrangements. Article 6(4) relies substantially on the rights holders' willingness to act voluntarily in affording access to and use of works protected by technological measures in certain circumstances. Only if and when rights holders fail to do so, the Copyright Directive states, shall the Member States "take appropriate measures to ensure that rightsholders" do make available to beneficiaries the benefits of the very specific exceptions or limitations set out in Article 5. When and how a Member State is to determine that it should act, because there are no voluntary agreements with rights holders that actually do accommodate the exceptions and limitations, is not addressed by the Copyright Directive.

The Copyright Directive's approach, therefore, contemplates multiple steps to making an exception or limitation available. First, Member States are instructed to act only "in the absence of voluntary measures taken by right holders, including by agreement" with other parties. These "other parties" could include manufacturers of consumer electronics and information technology products, consumers and vendors of technological measures. With respect to intended beneficiaries of the exceptions who are end users, it may not always be clear who the other parties to a dialogue or agreement might be. The Copyright Directive requires leaving a "reasonable period of time" for rights holders to enter into these agreements before Member States intervene.[132]

Second, the measures that Member States must take do not require exceptions be written into national law. Instead, they may mandate that rights holders (and, presumably, the technological measures that they use) utilize safety valves to accommodate specifically identified acts by end users. It should also be noted that there is no certainty that Member States will implement these exceptions in a harmonized manner. Furthermore, the form and manner of Member States' intervention, should there be an absence of voluntary measures, also is unspecified, and, consequently, may differ among the various Member States.

Third, the exceptions made available by rights holders to beneficiaries need only be granted "to the extent necessary" and no further. Fourth, persons who have "legal access" to the work are to be afforded the benefit of an exception. Fifth, and as described below, a special regime applies with respect to the exception or limitation applicable to circumvention for private use.

---

[132] Recital 51.

This entire regime of exceptions, however, has a further critical caveat that, in some respect, may have significant consequences for the whole. Article 6(4)(4) provides that none of the mandates with respect to voluntary agreements and Member State requirements apply to works "made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them." This proviso is intended to accommodate various business models and is aimed principally at works that are made available to users on an interactive, on-demand basis.[133] These would include pay-per-view/listen/download or video-on-demand services–arguably distinct from subscription or online "broadcasting." In such circumstances, the Copyright Directive provides that the rights holders, in light of the direct contract made with the end user with respect to the use of the particular work, need not provide for any exceptions or limitations to access or copy control measures.

Article 5 sets out exceptions and limitations on copyright rights that Member States may–but are not required to–provide with respect to the use of copyrighted materials. (Indeed, various Member States do not provide for broad-based exemptions for private copying, for example.) Therefore, Article 5 and Article 6 work together as follows: circumvention of technological measures is permitted where the act of doing so (or the trafficking in circumventing products themselves) is undertaken in order to benefit from these exceptions or limitations in national law. Thus, unlike the DMCA, where the exceptions in Section 1201 are essentially defenses to an action for circumvention, the Copyright Directive's approach is to suggest that a Member State may (or may not) permit certain underlying acts, acts that the technological measures are supposed to accommodate (whether on a voluntary basis, or otherwise). The acts that might be permitted are set out below.

Permitted Reproductions: Article 5 states that Member States may provide for exceptions in their national laws to the rights of reproduction (5(2)) and reproduction and communication (5(2) and (3)). These include:

– Reproductions on paper (photocopying), provided that rights holders receive fair compensation;[134]

– Reproductions by public libraries, educational establishments and museums, or archives, for non-commercial purposes;[135]

– Ephemeral recordings made by broadcasting organizations and associated archiving;[136]

– Reproductions by non-commercial institutions (such as hospitals and prisons), provided that rights holders receive fair compensation;[137]

– Uses for teaching or scientific research, for non-commercial purposes, where credit is given, if possible;[138]

---

133 Recital 53.
134 Article 5(2)(a), Copyright Directive.
135 Article 5(2)(c).
136 Article 5(2)(d).
137 Article 5(2)(e).
138 Article 5(3)(a).

– Non-commercial uses for persons with disabilities, where related to the disability and to the extent required;[139] and

– Uses for public security or reporting of governmental proceedings.[140]

As noted, these acts appear to be favored for purposes of Article 6 insofar as it is expected that technological measures will accommodate them. Article 5 sets out exceptions and limitations for various other acts, such as for news reporting, criticism or review, use in connection with political discourse or religious celebrations. These, too, appear to be legitimate uses and are appropriately the subject of exceptions in national copyright laws. Article 6, however, does not require that these additional exceptions be given preferred treatment by rights holders or Member States.

Private Copying: Article 5(2)(b) permits Member States to make an exception for reproductions made by a "natural person for private use." Again, a recital to the Copyright Directive states that Member States should promote voluntary measures to accommodate this exception, and that they may take measures if no such accommodation has been made in a "reasonable time."[141] Here, too, there is no certainty with respect to whether Member States will intervene in the absence of such measures and whether they will do so on a harmonized basis.

Any such permitted reproductions must be neither directly nor indirectly commercial. Furthermore, the rights holders must receive "fair compensation" that "takes account of the application or non-application of technological measures." As to this last point, the relationship between the use of DRMs and other technological measures and private-copying levy schemes, which are intended to give rights holders fair compensation, has been the subject of substantial Community-wide debate, and is discussed in Section 5.1.3.

This provision was among the most-debated prior to the adoption of the Copyright Directive. Article 6(4)(2) provides specifically that Member States may take measures vis-à-vis rights holders to ensure that this type of personal non-commercial copying is permitted unless the rights holders accommodate such copying in the technological measures they use. In this regard, the Copyright Directive also provides that technological measures may be permitted to limit the number of reproductions that might be made by invoking this exception. (Presumably, this refers to the number of private copies that an individual person may make.)

In this provision, the Copyright Directive is much more direct and more permissive than the DMCA in the linkage of private copying and circumvention. Whereas circumvention in aid of fair uses (including private copying) remains prohibited in the United States of America, the Copyright Directive contemplates that private use copying may justify a requirement that rights holders accommodate such uses in the technological measures that they deploy.

Further exceptions and limitations are set out in the recitals to the Copyright Directive. Recital language is not, however, imbued with the mandatory force of the articles themselves.

---

139 Article 5(3)(b).
140 Article 5(3)(e).
141 Recital 52, Copyright Directive.

Reverse Engineering: A recital to the Copyright Directive states that Member States should not inhibit or prevent the development or use of a means of circumventing a technological measure if necessary to enable reverse engineering or the functioning of computer programs, as authorized by the Computer Program Directive.[142] Such reverse engineering must comply with that Directive, that is, it must be undertaken for the purpose of interoperability.

Cryptographic Research: Another recital states that legal protection should not "hinder research into cryptography."[143]

No Mandate Provision: With respect to the concept of "no mandate," the Copyright Directive is not as protective of ordinary products as is the DMCA, which states that such products need not respond to particular technological measures. There is no specific exemption in the Copyright Directive to this effect, though there is a recital that includes language similar to Section 1201(c)(3) of the DMCA: Member States' legal protection "implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6."[144] The recital states that legal measures should not restrict devices or activities that have a "commercially significant purpose or use other than to circumvent" technological measures. This recital goes beyond the text of the DMCA itself, though the legislative history of the DMCA underscores the same point.

3.3.1.1(d) Rights-Management Information

Article 7 of the Copyright Directive separately requires that Member States provide for adequate legal protection against a person who "knowingly" removes or alters electronic "rights-management information" or distributes works from which such information has been removed or altered without authority. Such removal or alteration is prohibited if and to the extent that the person knows or has reason to know that by doing so he or she is inducing, enabling, facilitating or concealing an infringement of copyright, related rights or the *sui generis* database right.

"Rights-management information" is defined similarly to copyright management information under Section 1202 of the DMCA. It includes information that identifies or relates to the work, conditions of use and numbers or codes representing such information.

The recital to the Copyright Directive applicable to rights-management information notes the nexus between the processing of personal data obtained from DRM or other technical systems and the requirements of European privacy law.[145] This relationship is discussed in Section 5.2.1.

---

142 Recital 50, Copyright Directive, citing Article 5(3) and Article 6 of Directive 91/250/EEC of the Council on the legal protection of computer programs, Official Journal L 122/42, 17/05/1991 ["Computer Program Directive"].

143 Recital 48, Copyright Directive.

144 *Id.*

145 Recital 57, Copyright Directive.

3.3.1.1(e) Remedies

Although the Copyright Directive requires that Member States implement its provisions in national law, the Directive does not establish remedies for violations of the anti-circumvention provisions. That aspect is left for the Member States. Article 8 of the Copyright Directive specifically requires, however, that Member States provide for "appropriate sanctions and remedies" for infringements. It mandates that these remedies must include giving rights holders the right to bring actions for damages, to obtain an injunction and to seize infringing materials, as well as circumvention products. This Article is based in significant part on the enforcement provisions in the TRIPS Agreement discussed in Section 3.2.1.1.

3.3.1.1(f) Monitoring and Implementation

Self-contained within the Copyright Directive are several mechanisms to assess the effect of the use of technological measures on the internal market and end users. First, every three years, the European Commission must submit a report on the application of the Copyright Directive. The report must examine whether Article 6 "confers a sufficient level of protection and whether acts which are permitted by law are being adversely affected by the use of effective technological measures."[146] This study is somewhat akin to the biennial Copyright Office proceeding required by Section 1201(a)(1) of the DMCA, which requires an examination of whether users are being adversely affected by technological measures.

Second, where necessary, the Commission could submit proposals for amendments to the Copyright Directive.[147] Third, the Copyright Directive establishes a contact committee to examine the impact of the Copyright Directive on the functioning of the internal market and "to act as a forum for the assessment of the digital market in works and other items, including private copying and the use of technological measures."[148] Overall, the process of review and amendment set out in the Copyright Directive appears to be more expansive than the DMCA-mandated proceeding, which is limited in scope and sets the bar for exceptions at a high threshold.

---

146 Article 12(1), Copyright Directive.

147 *Id*.

148 Article 12(3) and (4).

3.3.1.1(g) Implementation

On July 14, 2003, the European Commission issued a press release stating that only Greece and Denmark had met the December 22, 2002 deadline for implementation of the Copyright Directive, and that Italy and Austria had done so subsequently (enacting laws in April and June 2003, respectively); the Commission stated that it will pursue infringement procedures against Member States that have not transposed the Copyright Directive.[149] Germany also has enacted legislation to implement the Directive. Other Member States are in the course of implementation. A draft proposal has been prepared in France, for example, and consultative activities are underway in various other Member States.

Italy: Italy transposed the Copyright Directive in a *Decreto Legislativo* ("Decree Law") of April 9, 2003.[150] The Decree Law amends the Italian Law for the Protection of Copyright and Neighboring Rights. Article 23 of the *Decreto* reflects Article 6(3) of the Copyright Directive in its definition of "technological measures" and in describing when they would be regarded as being "effective." The abusive use of circumvention processes (that is, the act of circumvention), including the purchase or rental of circumvention tools, is subject to administrative sanction.[151] Trafficking in circumvention tools and services is subject to criminal penalties.[152]

Germany: In mid-July 2003, Germany adopted legislation to implement the Copyright Directive. The law defines "technical measures" and "effective" technical measures consistently with the Copyright Directive. A new Section 95a of the Copyright Law of 1965 prohibits the act of knowingly circumventing effective technical measures and the trafficking in circumvention tools.[153]

Certain acts of unlawful trafficking in circumvention tools, as well as the ownership or possession of a tool for commercial purposes or the provision of a service, are administrative (not criminal) offenses; each German state will determine which authority will be responsible for taking administrative action against violators. Unlawful trafficking in circumvention tools for commercial purposes is subject to criminal penalties. Intentional circumvention is subject to criminal penalties, but only when the act is not exclusively for the person's private use (or that of related persons); a stiffer sanction is prescribed where the act was done for commercial gain.[154] Although the law does not specifically so provide, it is presumed that rights holders also will have rights to pursue private actions against violators in courts.

---

149 See European Commission, *Internal Market: Commission moves against 13 Member States for failure to implement EU legislation* (July 14, 2003), available at *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1005|0|RAPID&lg=en&display*.

150 See Decree Law, April 9, 2003, n. 68, *Gazzetta Ufficiale*, n. 87 (April 14, 2003), available at *http://www.giustizia.it/cassazione/leggi/dlgs68_03.html*.

151 *Id*. at Art. 28 (amending art. 174-ter of the Law for the Protection of Copyright and Neighboring Rights (Law No. 633 of April 22, 1941, as amended by Decree Law, May 26, 1997, n. 154)).

152 *Id*. at Art. 26 (amending art. 171-ter of the Law for the Protection of Copyright and Neighboring Rights).

153 See *Drucksache* 271/03 (May 2, 2003), Art. 1, section 34 (proposing to amend the Copyright Law to include new §§ 95a to 95d).

154 *Id*. at Section 42 (proposing to include a new § 111a).

The German approach to implementing the exceptions and limitations of Article 5 of the Copyright Directive has drawn some attention, and has been of concern to rights holder interests. A new Section 95b of the Copyright Law requires that rights holders afford persons the ability to take advantage of the exceptions for which the Copyright Law provides, if they have legal access to the work or material. Included in these exceptions in the Copyright Law are the right to make a single reproduction of a work for private use on any storage medium; although, Section 95b recognizes this exception, it limits authorized circumvention (for the sole purpose of benefiting from the exception) only to the extent that the reproduction is on paper. The private copying exception is not available, however, where the copies are made from obviously illegal sources.

It is unclear how the rights holder would be able to comply with these requirements if, for example, the technical measure is not associated directly with the work itself but, instead, with the mode of distribution. How to comply is a matter of some concern to rights holders because if they fail to make available the means necessary to benefit from the exception, they would be committing an administrative offense. The law also specifically provides that contractual obligations that preclude users from taking advantage of the exceptions would be void; however, consistent with Article 6(4) of the Copyright Directive, the right to benefit from exceptions would be rendered inapplicable where works are distributed pursuant to contractual agreements that allow users to access the works at a place and time of their choosing.[155] In addition, beneficiaries of the exceptions could require rights holders to supply the means (at the rights holders' discretion) by which they can benefit from the exceptions. To satisfy their obligations, rights holders could, for example, make available an analog or another copy protected copy to a beneficiary; the law does not confer on beneficiaries the right to hack or circumvent.

The law provides that rights holders must label works and materials protected by technical measures; failure to do so also would be an administrative offense. Such an obligation goes beyond the requirements of the Copyright Directive. How labeling will work with respect to works that are downloaded from, for example, servers located outside Germany remains an open question.

The law also provides that its provisions will enter into force at different times. The effectiveness of the provisions relating to the exceptions would be delayed for one year, to allow rights holders and associations representing beneficiaries to negotiate and enter into voluntary arrangements.

France: In France, the Ministry of Culture and Communications has prepared a draft law to transpose the Copyright Directive. The present draft contains a chapter on technical measures, which would amend the Intellectual Property Code to include articles authorizing authors to use technical measures. Circumventing acts and the trafficking in circumvention tools would be prohibited. At the same time, however, the draft would require authors to permit beneficiaries of exceptions set out in the Code (including the right of private copying) to benefit from those exceptions, notwithstanding the use of technical measures, where such beneficiaries have lawful access to the work. (The exception set out in Article 6(4) of the Copyright Directive, with respect to "on demand" services, is reflected in the draft as well.) Sanctions for unauthorized circumvention and trafficking generally would track those set out in the Code for infringements of copyright.

---

[155] *Id*. Section 34 (proposing to include a new §95b).

United Kingdom: In August 2002, the Copyright Directorate of the Patent Office released a *Consultation Paper on Implementation of the Directive in the United Kingdom*, including proposed statutory amendments.[156] Substantial comments were received on the amendments to implement Article 6 of the Copyright Directive. Given the nature of the comments, the Patent Office stated in June 2003 that the circulation of statutory amendments had been delayed, but indicated that work on U.K. implementation of the Copyright Directive is "well advanced."

3.3.1.2 Other Applicable Directives

The Copyright Directive was not the first effort by the European Union to adopt measures to protect DRMs and other technological measures used to protect copyrighted works. Three earlier directives bear mentioning. They are described briefly below.

3.3.1.2(a) Computer Program Directive

The Computer Program Directive, which was adopted in 1991, addresses technological measures used to protect computer programs.[157] Article 7 specifically requires that Member States adopt remedies against anyone who puts "into circulation" or possesses for commercial purpose "any means" of which the "sole purpose" is to "facilitate the unauthorized removal or the circumvention of any technical device which may have been applied to protect a computer program."[158]

3.3.1.2(b) Conditional Access Directive

The Conditional Access Directive was adopted in 1998 to protect access to and remuneration for various kinds of services delivered electronically and through means of conditional access.[159] The Conditional Access Directive is targeted at ensuring that the service provider is remunerated, and not at the content of the service itself. The scope of the Conditional Access Directive is indeed expansive. It applies to online services, as well as to television and radio broadcasting, whether by wire or over the air (including by satellite), as well as "information society services."[160]

Conditional access is defined as "any technical measure and/or arrangement whereby access to the protected service in an intelligible form is made conditional upon prior

---

156 See EC Directive 2001/29/EC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society: Consultation Paper on Implementation of the Directive in the United Kingdom (Copyright Directorate: August 7, 2002), available at *http://www.patent.gov.uk/about/consultations/eccopyright/pdf/ 2001_29_ec.pdf*.

157 Directive 91/250/EEC of the Council on the legal protection of computer programs, Official Journal L 122/42, 17/05/1991 ["Computer Program Directive"].

158 Article 7, Computer Program Directive.

159 Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, Official Journal L 320/54, 28/11/1998 ["Conditional Access Directive"].

160 Article 2(a), Conditional Access Directive.

individual authorization."[161] The Conditional Access Directive prohibits the business of trafficking in "illicit devices." Illicit devices are defined as "equipment or software designed or adapted to give access to a protected service in an intelligible form without the authorization of the service provider."[162]

The Conditional Access Directive instructs Member States to ban the manufacturing, sale and rental of such devices, and their possession for commercial purposes, as well as their installation, maintenance or replacement and commercial promotion.[163] The sanction and remedy provisions in Article 5 are similar to those set out in the Copyright Directive. Neither the act of circumvention nor the possession of an illicit device for personal use is prohibited by the Conditional Access Directive. The deadline for transposition into national law was May 28, 2000.

Based largely on the Conditional Access Directive, the Council of Europe drafted the European Convention on Legal Protection of Services based on, or consisting of, conditional access schemes.[164] The Convention, which was adopted by the Committee of Ministers in October 2000 and has been open for signature since January 24, 2001, would apply to nations in Europe both within and beyond those of the European Union.

3.3.1.2(c) Electronic Commerce Directive

The Electronic Commerce Directive was adopted in July 2000 to establish the basic framework for electronic commerce within the European Community.[165] The deadline for transposition into national law was January 17, 2002. The Electronic Commerce Directive has several important provisions that are applicable to the use of DRMs to deliver and protect content that is being distributed to the consumer electronically.

First, Member States are required to ensure that contracts can be concluded by electronic means, and that such contracts will be legally effective and valid.[166] Accordingly, click-wrap and other electronic contracts can be the basis on which content is made available online to end users. Various provisions require that service providers present information in a clear form to consumers prior to their placing an order and that providers acknowledge receipt of electronic orders.[167]

Second, the Electronic Commerce Directive provides intermediary service providers with "safe harbors" from liability for the content that they transmit, cache and store. These are similar to those in the DMCA, as described in Section 3.2.1.2. The Article applicable to "caching" provides that Member States may not impose liability on a service provider that

---

161 Article 2(b).
162 Article 2(e).
163 Article 4.
164 European Convention on the Legal Protection of Services based on, or consisting of, Conditional Access, ETS 178, available at *http://conventions.coe.int/Treaty EN/cadreprincipal.htm.*
165 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178/1, 17/07/2000 ["Electronic Commerce Directive"].
166 Article 9(1), Electronic Commerce Directive.
167 Articles 10 and 11.

automatically and temporarily stores content for purposes of onward transmission, subject to several conditions. One of these conditions is that the provider may not interfere with the "lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information." This provision is modeled on the predicate condition for safe harbor status set out in Section 512(i)(1)(B) of the DMCA. As in the United States of America, the Electronic Commerce Directive provides in Europe that the service provider's immunity is lost to the extent that the process of caching content interferes with DRM systems and other technological measures that rights holders might use to track usage of information. There is, therefore, a powerful incentive for service providers to ensure that they preserve industry-recognized technical measures lest they be subject to suit for copyright (or other) infringements.

3.3.2 European Commission DG Information Society: Digital Rights Management Workshop

Having succeeded in adoption of the Copyright Directive, the European Commission initiated a process to explore a series of follow-on issues, including how the Commission itself could assist in further elaboration of a regime for DRMs. In February 2002, the DG Information Society launched what became a multi-workshop process to bring together various stakeholders to discuss DRM-related matters, including whether there was a consensus for further action by the Commission.[168]

Among the most significant issues under discussion–particularly from the standpoint of technology companies and consumers–has been whether the implementation of DRMs would cause the rationale for levies imposed on recording devices and media to disappear. Rights holders, however, were more interested in urging that the Commission or other institutions step in to solve content protection problems in the absence of private sector developments and agreements. The process was launched to facilitate discussions and the exchange of views rather than with a fixed goal in mind. It should be noted that the Commission–in contemplating a potential role for itself–launched this series of workshops against the backdrop of consideration by the U.S.A. Congress of the Consumer Broadband and Digital Television Promotion Act, which would have established a role for the U.S.A. Government in setting standards.

A further impetus for the process was grounded on Recital 54 of the Copyright Directive, concerning the possibility that differences in technological measures could lead to an incompatibility of systems within the Community. To the extent that barriers to internal trade might then develop, the DG for Enterprise Policy also was interested in examining whether there was a need to standardize DRMs.

In the wake of the Copyright Directive, the European Commission had requested that CEN/ISSS (the Information Society Standardization System within the European Standards Committee) examine the state of the art in DRM standardization. The DRM Group of CEN/ISSS was established in October 2001. A very substantial draft report, the first draft of

---

168 See *Report*, Digital Rights Management (DRM) Workshop (April 16, 2002), available at *http://europa.eu.int/information_society/topics/multi/digital_rights/doc/workshop2002/workshop_report1.pdf*.

which was dated January 31, 2003, was released for comment.[169] The draft essentially summarizes the views of the various stakeholders in a comprehensive fashion, without itself offering policy recommendations, standards or conclusions.

The DG Information Society Digital Rights Management process encompassed four workshops. Each was led by a particular sector, but representatives of all sectors were invited to attend. The final workshop, at which these views were presented, took place on March 25, 2003.[170]

User/Consumer Interests: The first workshop was led by user/consumer interests, such as the European Consumers' Organization (*Bureau Européen des Unions de Consommateurs*, or "BEUC"), and third-party distributors of content, represented by the European Digital Media Association ("EdiMA"). The topics discussed included the possibility that DRMS would limit consumers' ability to access content, including by private copying. They urged that DRMs themselves respect the legal framework, including the possibility of benefiting from the exceptions set out in the Copyright Directive, and that technologies should be interoperable. In this regard, consumers expressed concerns that, through DRMs, they might be required to contract away rights provided them under copyright exceptions. They also requested that governments not permit rights holders to use DRMs to hinder access to works in the public domain.

Further policy issues raised by the user communities include the need for clear disclosure to consumers that products are copy-protected and that levies are eliminated, so that rights holders are not compensated twice, once through a levy and a second time through a DRM-facilitated payment. They urged, therefore, that levies be phased out after DRM systems are in place.

Another matter of concern to consumers is the possibility that DRM systems could collect personal data and adversely affect privacy interests. They also urged that DRM standards not be made mandatory by government but, instead, be the product of industry-led efforts.

ICT and Consumer Electronics Industry: The technology industries, through the European Information and Communication Technology Association ("EICTA"), led the second workshop. The principal thrust of the session was to ensure that the participants have a common understanding of the state of developments in DRM technologies and to explain that DRMs are intended to "keep honest people honest," rather than to eradicate commercial piracy. In addition, the industries asked that rights holders ensure that DRMs be deployed so that consumers can take advantage of the copyright exceptions, consistent with their legitimate demands and expectations.

A centerpiece of the technology industries' position is that there is no need for private-copying levies on devices and media in a digital environment. First, the industries argued that rights holders can control the private copying of their works through DRMs, thereby introducing the prospect of extracting multiple payments from consumers. Second, they

---

169 See *Digital Rights Management: Draft Report*, CEN/ISSS (Draft 1.2, February 5, 2003), available at *http://www.cenorm.be/isss/DRM/draft_report1_2.pdf.*

170 See *http://europa.eu.int/information_society/topics/multi/digital_rights/events/ index_en.htm* (describing the various events of the DG Information Society DRM process).

noted that the scope for imposing levies in a digital environment might expand enormously, given that a broad range of devices and media–from personal computers and personal digital assistants to digital set-top boxes and removable or integrated memory–can manipulate and store content. They argued that it would be inappropriate to impose levies on multi-purpose devices and media, regardless of their actual use.

The technology industries continued to express a strong preference for private sector, rather than governmental, involvement with regard to DRMs. The ICT and consumer electronics sector resisted any suggestion that there be governmental mandates with respect to specifying technology. They also stressed that interoperability issues be addressed in voluntary, industry-led fora.

Rights Holders: The rights holder community, including the Motion Picture Association ("MPA"), the International Federation of the Phonographic Industry ("IFPI") and the Federation of European Publishers, organized the third workshop. In their view, DRMs should be considered as enabling technologies: they facilitate making more content available (rather than locking it up), make possible new business models and, as a result, expand the range of choices that consumers have in selecting and interacting with copyrighted content. With respect to DRM systems specifically, rights holders commented that the DRM market is still young, with insufficient supporting hardware, and that it is imperative that DRM technologies be made secure and renewable (that is, that they enable recovery of security in case of hacking or other circumvention).

In addition, given that DRM technologies are not yet mature, rights holders believe that it is premature to use technological controls enabled by DRMs as a justification for the elimination of levies. Rights holders also expressed the concern that current DRM technologies have only limited interoperability and they encouraged government and industry to support the work undertaken in international fora toward developing open standards. Rights holders expressed a clear preference for industry-led standards. But, they also emphasized that a government role may be needed to ensure compliance with an agreed-upon standard and that where private sector negotiations fail, involvement of government may be required.

The rights holders also identified specific issues for future work. Among the most pressing is the need to ensure that a secure environment for content is developed for personal computers–a challenging task given that these devices are both multi-functional and freely programmable. The rights holders also earmarked for present and future work what they describe as "gaps" in DRM systems, including the "analog hole," presented by the conversion of digital to analog formats, without maintaining the original protection, and the need to protect over-the-air digital television broadcast content from unauthorized retransmission (the subject of the FCC's broadcast flag rulemaking discussed in Section 3.2.1.3(b)).

Collective Management Societies: The collective management societies ("CMS") represent rights holders in negotiating and administering license agreements, including the collection and distribution of royalties, through authors societies around the world. As described in the CMS's own submission to the Information Society process, they undertake to document and license rights, enforce intellectual property laws, monitor and audit and educate and inform the public about the need to respect copyright. During the workshop, the CMS expressed concern that there was insufficient awareness of their role in the information society generally–they provide the means to access and license use of copyrighted works on a global basis–and, particularly, with respect to the development and use of DRMs to assist

them in carrying out their functions. Specifically, CMS are concerned that to the extent that DRMs can facilitate direct relationships, for both rights clearance and compensation, between various types of rights holders and consumers, the need for CMS in a digital environment may be diminished. In this respect, the CMS are keen to stake out a continuing role for themselves that would enhance, not duplicate, the functions of DRM systems. They noted that the CMS are themselves developing DRM components and stressed the importance of cooperation in the development of DRM technologies.

Furthermore, like the rights holders, the CMS stated that DRMs are still at an early stage of development, and may not apply in many circumstances, including with respect to legacy devices, digital-to-analog reconversion and private copying. In general, the CMS do not believe that the time is yet ripe to abolish private-copying levies.

In addition, the CMS urged that additional work be undertaken with respect to interoperability–necessitating the development and application of international standards–as well as security and enforcement (including adaptation to new business models). They noted that industry-led, voluntary standards appear to be sufficient, and thus did not advocate a more active role for government.

Summary of Themes: Although a formal synthetic report was not produced by the DRM Workshop process, the following themes, generally speaking, appear to have emerged from the discussions:

– More work may need to be done with respect to understanding the scope and capabilities of DRM solutions.

– DRM technologies–including interoperability among different systems–should be developed on the basis of voluntary, industry-led efforts with the proper role of government not yet agreed upon.

– Particular, discrete content protection issues merit further attention by all of the affected private sector groups.

– Although DRMs enable new business models and consumer choice, it is recognized that consumer expectations and copyright exceptions should be taken into account.

– Further work is required on the implementation of DRM systems in relation to the continuation or imposition of levies on digital devices and media.

3.3.3 Case Law

Given the relatively recent adoption of the Copyright Directive and that it has not yet been transposed by most of the Member States into their national laws, it is not surprising that there is not yet significant case law applying the anti-circumvention provisions. Cases have interpreted existing national laws, however, to prohibit certain types of circumvention devices.

Sony Computer Entertainment v. Owen:[171] In the United Kingdom, for example, Sony Computer Entertainment brought suit against various defendants, who imported "modification

[171] [2002] EWHC 45 (CH).

chips" that could be used to circumvent copy protection and region-control technologies on PlayStation 2 discs. The facts raised were substantially identical to those at issue in the earlier *GameMasters* decision in the United States of America.

The English court relied on a copyright-based cause of action set out in Section 296 of the Copyright, Designs and Patents Act 1988. Section 296 applies where copies of a work are issued in an electronic form that is "copy protected" and gives rights to the distributor of the copies–as if he were the copyright owner in an action for infringement–against any person who sells a device that is "specifically designed or adapted to circumvent" copy protection, knowing that the device will be used to make infringing copies.[172] "Copy protected" is defined to include "any means intended to prevent or restrict copying of the work." The court found for Sony because the copying that was to be prevented was the unauthorized loading of the game into the computer and because the codes on the discs fell within the definition of copy protection. The defendants violated Section 296 because their chips were specifically designed to circumvent Sony's copy protection technology.

3.4 Australia

3.4.1 Legal Framework

3.4.1.1 Copyright Amendment (Digital Agenda) Act 2000

3.4.1.1(a) Background

Australia substantially implemented the WIPO Treaties through the Copyright Amendment (Digital Agenda) Act 2000 ("DAA"), which came into effect on March 4, 2001 and amended the Copyright Act 1968.[173] Consideration of implementation in Australia began with a 1997 Discussion Paper, *Copyright Reform and the Digital Agenda*, and continued with an Exposure Draft and Commentary on the Digital Agenda Copyright Amendments in 1999. Ultimately, the Australian approach to implementation of the WIPO Treaties has been characterized as more favorable to users than its counterparts in the United States of America and the European Union. This is said to reflect the fact that Australia imports more copyright-related products than it exports.

3.4.1.1(b) Anti-Circumvention Provisions

The DAA prohibits the business of trafficking in circumventing tools, including manufacturing, selling, renting, offering for sale, promoting, advertising, marketing, distributing and exhibiting a device. Included in the prohibited activities is making the circumvention device available online, but only "to the extent that it will affect prejudicially the owner of the copyright."[174] Where the acts involved are the offering of a "circumvention service," the DAA, like its U.S.A. and European counterparts, forbids the activity.[175] An

---

172 Copyright, Designs and Patents Act 1988 (c. 48), s 296(2).

173 The relevant provisions are included in a new Division 2A of Part V of the Copyright Act 1968 (Cth).

174 Copyright Act 1968 (Cth) s 116A(1)(b)(i)-(vi).

175 s 116A(1)(b)(vii).

element of the prohibition is that the defendant must have known, or ought reasonably to have known, that the device or service could be used to circumvent, or facilitate the circumvention, of a technological protection measure.[176] The DAA does not specifically prohibit the act of circumvention, however.

The definition of "technological protection measures" anticipates the approach followed in the European Union by including both access control and copy control measures. The language largely follows that of the DMCA, however. Specifically, the DAA defines a technological protection measure as a device or product (including components) that is designed "in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject-matter by either or both of the following means":

– Ensuring that "access to a work" is available "solely by use of an access code or process (including decryption, unscrambling or other transformation of the work . . .) with the authority of the owner or licensee of the copyright;

– Through a copy control mechanism.[177]

In limiting the protected technological protection measures to those that are "designed to prevent or inhibit infringement," the DAA follows the WIPO Treaties and the approaches in the United States of America and the European Union: the purpose of using such measures is to enhance rights holders' ability to prevent unauthorized uses of their works.

Much like the Copyright Directive, however, the use of the phrase "copy control mechanism" suggests that the DAA does not outlaw circumvention of technological measures that are used by rights holders to prevent other types of unauthorized uses that fall within their exclusive rights (such as public performance). The legislative history of the DAA offers serial copy control technologies as an example of a "copy control" measure. In the *Sony v. Stevens* case described below, the Federal Court interpreted this language to refer to a mechanism that restricts copying of a work.

The DAA defines circumvention devices and services by reference to two tests: whether the device or service has 1) only a "limited commercially significant purpose or use" of circumvention or 2) no purpose or use other than circumvention.[178] The first of these two tests is similar to one prong of the test used in the DMCA and the Copyright Directive. The second test–the sole purpose test–was considered and rejected in other jurisdictions (but not in the Japanese Unfair Competition Prevention Law) because it would permit trafficking in a device or service that had some, perhaps minor or marginal, legitimate purpose, but was otherwise designed for circumvention. The addition of the first test, however, would seem to address concerns of rights holders and others who believed that it would be too easy to evade a sole purpose test. An important distinction, then, between the DAA and the approaches in the United States of America and the European Union is that, under Australian law, a device or service that has a commercially significant purpose other than circumvention would be lawful.

---

176 s 116(A)(1)(c).

177 s 10(1) (definition of "technological protection measure").

178 s 10(1) (definitions of "circumvention device" and "circumvention service").

The Australian approach, therefore, can be summarized as follows:

	Act of Circumvention	**Circumvention Tools**
Access Control Technological Measure	Not prohibited	Prohibited (s 10(1); s 116A)
Copyright Control Technological Measure	Not prohibited	Prohibited (s 10(1); s 116A)

3.4.1.1(c) Limitations and Exceptions

The DAA established three basic exceptions to the prohibition on trafficking in circumvention devices or services.

Use for a Permitted Purpose: Where a circumvention device or service is supplied to a "qualified person" for a "permitted purpose" it will not be prohibited, if the qualified person provides the supplier with a signed declaration. These "permitted purposes" are established by reference to exceptions to copyright infringement set out in the Copyright Act. A "permitted purpose" is one that falls within at least one of the statutory exceptions to copyright infringement.[179] These include:

– Reproduction of computer programs for purposes of interoperability, to correct errors and for security testing;

– Lawful copying by libraries, archives, educational and other institutions, including institutions assisting persons with an intellectual disability; and

– A lawful use of copyrighted material for the services of the Commonwealth or a State.

Importantly, a "permitted purpose" does not include a use that amounts to "fair dealing," such as private copying or "fair uses." Given the potential breadth of such an exemption and the inability to control circumvention devices that lawfully could be supplied only to persons who engaged in "fair dealing," it would have been difficult to limit the scope and effect of such an exemption solely to persons who are demonstrably "qualified" and who submit declarations to that effect.

A "qualified person" is one who is authorized to use material for purposes of one of the above-mentioned exceptions.[180] Finally, the qualified person must give a signed declaration confirming that the device or service will be used only for the permitted purpose and that the copyrighted material is not readily available other than in a form protected by a technological measure.[181] To prevent pirates and other wrongdoers from using this process to obtain access to devices that would circumvent technological measures, the DAA made it a criminal offense for a person to knowingly or recklessly make a false or misleading declaration.[182]

179 s 116(A)(7).
180 s 116(A)(8).
181 s 116(A)(3)(b).
182 ss 203G(1), (2).

The strength of the Australian approach may depend, therefore, to a significant extent on the integrity of the declaration process. It has been noted, for example, that if a declaration is not false or misleading at the time that it is made, but the device or service is later used for a purpose other than one that is "permitted," then no offense has occurred. In such cases, the suppliers would not be held liable, because they had supplied the circumvention device or service upon receipt of a valid declaration. Nor can users of such devices be held liable because acts of circumvention are not outlawed by the DAA.

Making or Importing for a Permitted Purpose: A similar provision applies to the making or importing of a circumvention device. To fall within the exception, it must be established that the device is made or imported for a "permitted purpose"–as discussed above–and that the copyrighted material is not readily available in a form other than one protected by a technological measure.[183]

In addition, a device can be made or imported if it enables a person to supply a device or a circumvention service, but only if that supply is for a "permitted purpose."[184]

Law Enforcement or National Security: Any act lawfully done for purposes of law enforcement or security falls within a blanket exception.[185]

3.4.1.1(d) Electronic Rights Management Information

The DAA also implements the rights management provisions of the WIPO Treaties. It prohibits the knowing, unauthorized removal or alteration of electronic rights management information to induce, enable, facilitate or conceal an infringement.[186] In addition, it also forbids the knowing distribution, importation or communicating of a copy of a copyrighted work to the public where electronic rights management information has been removed and the person knows or had reason to know that doing so would aid in infringing behavior.[187] For both violations, the statutory provisions presume that the defendants had the requisite knowledge: they have the burden of proving that they did not knowingly alter or remove the information and that they did not know that their trafficking in altered copies would aid infringement.

3.4.1.1(e) Remedies

The remedies available for breach of the civil provisions include an injunction and either damages or an accounting of profits.[188] Punitive damages also are available for flagrant breaches.[189] Rights holders also may bring an action for conversion or detention for

---

183 s 116(A)(4)(a).
184 s 116(A)(4)(b).
185 s 116(A)(2).
186 s 116B.
187 s 116C.
188 s 116(D)(1).
189 s 116(D)(2).

circumvention devices that are used to make infringing copies.[190] Punishments for criminal offenses include fines and imprisonment (up to five years).[191]

3.4.1.2 Other Laws

Various other provisions of Australian law prohibit unauthorized access to computers and encrypted content. Notably, encrypted broadcasting services are protected under Part VAA of the Copyright Act 1968, which also was inserted by the DAA. The DAA was drawn, in part, from the Conditional Access Directive, but is narrower in scope, as it applies only to "encoded broadcasts," which are defined in the statute.

Part VAA prohibits the making, various kinds of trafficking in (including making available online) and commercial use of "broadcast decoding devices."[192] Such a device is defined as a device "(including a computer program) that is designed or adapted to enable a person to gain access to an encoded broadcast without the authorization of the broadcaster by circumventing, or facilitating the circumvention of, the technical means or arrangements that protect access in an intelligible form to the broadcast."[193] "Encoded broadcasts" include 1) television or radio broadcasts made available only to authorized persons and on payment of fees and 2) television broadcasts delivered by broadcasting services, access to which, in intelligible form, is protected by technical measures.[194] Video and audio on-demand, teletext and Internet streaming services do not fall or have been determined not to fall within the definition of broadcasting services and therefore are not protected against unauthorized access by Part VAA.[195]

Broadcasters may sue for the unauthorized commercial use of broadcast decoding devices where they make encoded broadcasts, and persons use such devices to gain access without authorization, knowing (or where they reasonably ought to have known) that access was unauthorized.[196] Broadcasters may obtain both an injunction and either damages or an accounting of profits.[197] The commercial distribution of a broadcast decoding device may also rise to a criminal offense.[198]

Two elements of the Australian legal regime are noteworthy. First, the Copyright Act vests the right to sue civilly in the broadcaster, not the copyright owner. Second, the private possession or unauthorized non-commercial use of broadcast decoding devices is not prohibited.

---

190 s 116.
191 s 132(6)(A).
192 s 135AN(1)(b).
193 s 135AL (definition of "broadcast decoding device").
194 s 135AL (definitions of "encoded broadcast" (a) and (b)).
195 Broadcasting Services Act 1992 (Cth) s 6 (definition of "broadcasting service"); Determination under paragraph (c) of the definition of "broadcasting service" (No. 1 of 2000), Notified in *Gaz GN38* of September 27, 2000 (streaming of television or radio programs using the Internet excluded from definition of "broadcasting service").
196 *Id*. s 135ANA(1).
197 *Id*. s 135ANA(4).
198 *Id*. s 135AS(1).

3.4.2 Case Law

Autodesk, Inc. v. Dyson:[199] Prior to the adoption of the DAA, the Australian High Court applied then-existing principles of Australian copyright law to prohibit a device that was employed to circumvent a technological measure used to protect a computer program. In that case, Autodesk owned a copyrighted computer-assisted design program; users could only obtain authorized access through a hardware device, a "dongle," which was purchased with the program and was then plugged into the computer to enable the program to run. A separate, substantial part of the program challenged the dongle to authenticate itself; this module compared the responses in a "look-up table." Only if the correct response was received, would the entire program run.

The defendant produced a circumvention device by reverse engineering the dongle. The High Court held that the production of the circumvention device infringed the copyright in Autodesk's program because, in the course of reproducing the "look-up table" in the dongle, a substantial part of the program was necessarily copied. Accordingly, the defendant's liability for manufacturing the circumvention device was predicated on his infringement of Autodesk's copyright.

Kabushiki Kaisha Sony Computer Entertainment v. Stevens:[200] In interpreting and applying Section 116A of the DAA, in July 2003, the Federal Court of Australia allowed Sony Computer Entertainment's appeal of the decision of the primary judge, who had for a defendant who had sold and installed modification chips to circumvent coding used for PlayStation 2 games (as well as counterfeit copies of those games). Sony's protection measures included both a boot ROM located on the circuit board of its consoles, which were designed to read and verify the access codes stored on the boot track of the discs, and region codes designed to ensure that only discs coded for Australia would play on consoles sold there. The Australian Competition and Consumer Commission appeared as amicus curiae in the proceedings before the primary judge in favor of the defendant on the ground that regional coding is detrimental to consumer welfare and limits consumer choice.

The primary judge had carefully reviewed Australia's consideration of the WIPO Treaties and the various draft texts of the DAA, as well as the Copyright Directive, by way of coming to understand the term "technological protection measure," as defined by the DAA. It found that Sony's measures were not "technological protection measures" within the scope of Section 116(A): although they deterred or discouraged access to the work, they did not do so by means of an access code or process described in Section 10(1) of the Copyright Act 1968. Justice Lindgren, on appeal, analyzed extensively both the text and the legislative history of the DAA.

In allowing the appeal, the Federal Court adopted a broader construction of the definition of "technological protection measure. It held that the definition included devices that would have the intended result of deterring or discouraging infringement not, as the primary judge had held, measures that physically prevent or inhibit acts that might infringe. In this respect, the court interpreted Section 116A to apply not only to unauthorized reproduction, but also to the selling of articles, the making of which constitute an infringement of copyright. To the extent that Sony's protection measures render copies of

---

199 173 CLR 330 (1992).

200 [2003] FCAFC 157.

computer games useless, the court said, then they prevent infringement in the sense that they render the sale of the copies impracticable or impossible. The primary judge had not found it necessary to rule on whether the modification chips were themselves circumvention devices. Nevertheless, he offered the view that, in light of the limited commercially significant uses of the chips other than to circumvent, had the access codes qualified as "technological protection measures," the chips would have been unlawful circumvention devices.

The decision on appeal is largely consistent with the decision in the *Owen* case discussed in Section 3.3.3, which concluded that a similar modification chip unlawfully circumvented Sony's PlayStation 2 copy protection technology under the Copyright, Designs and Patent Act of the United Kingdom.

3.5 Japan

In Japan, the anti-circumvention provisions of the WIPO Treaties have been implemented in 1999 amendments to the Copyright Law and to the Unfair Competition Prevention Law. The Copyright Law amendments address circumvention of technologies protecting against copyright infringement. The amendments to the Unfair Competition Prevention Law prohibit both circumvention of copy control and access control technological measures that consideration in Japan of legal approaches to protecting technological measures antedates the WIPO Diplomatic Conference with the issuance in February 1995 of an interim report by the Copyright Council Multimedia Subcommittee Working Group and another interim report in February 1997. A working group of the Subcommittee launched a consultative process and studied developments in the United States of America and the European Union. In December 1998, it issued its Report on Technological Measures and Rights Management.[201]

3.5.1 Legal Framework

3.5.1.1 Anti-Circumvention Provisions

3.5.1.1(a) Copyright Law

Law No. 77 of 1999 amended the Copyright Law to prohibit various kinds of trafficking in circumventing tools, as well as the offering of a circumventing service to the public. It does not specifically bar the act of circumvention.

The Copyright Law defines "technological protection measures" as "measures to prevent or deter such acts as constitute infringements on moral rights or copyright . . . or neighboring rights."[202] As in Australia, "measures" are defined by reference to their purposes.

---

[201] The 1995 and 1997 interim reports and the December 1998 final report of the Subcommittee are cited in Koshida, note 203.

[202] Article 2(xx), Copyright Law of Japan.

The Copyright Law does not define "prevent," though a commentary accompanying the 1999 amendments to the Copyright Law states that to "prevent" means to stop.[203] "To deter" is defined in the Copyright Law as meaning to cause "considerable obstruction to the results of such acts." As in Australia, to "prevent" and to "deter" requires physical or technical means (rather than merely discouraging or having the practical effect of deterrence). The commentary states that a measure must use electromagnetic means to effect its prevention or deterrence.[204]

Circumvention devices and programs are prohibited by the penal provisions of the Copyright Law. A circumvention device or program is defined as one that has, as its "principal function," the circumvention of technological protection.[205] The Copyright Law does not define "principal function." The accompanying commentary, however, states that only devices that have a "limited practically significant function other than the circumvention" are prohibited.[206] In this, the Japanese law is consistent with other approaches to outlawing circumvention devices.

Although the act of circumvention is not prohibited, the Copyright Law does provide that a person may not circumvent a technological protection measure to reproduce a work for private non-commercial purposes.[207] Ordinarily, the Copyright Law permits such reproductions. Where, however, the reproduction is made by a person who knows that that act is made possible by circumvention or because the measure no longer obstructs the copying, the private copying exemption is no longer applicable. However, such person is not subject to the penal provisions of the Copyright Law.

This provision defines "circumvention" as the enabling of a person to "do acts prevented by technological protection measures" (i.e., prevention) or stopping the "obstructions" to the results of acts that are "deterred by such measures" (deterrence).[208] It also includes the removal of rights management information. Removal or alteration of measures or information that are essential to conversion or compression is not regarded as circumvention.

---

203 T. Koshida, *On the Law to Partially Amend the Copyright Law (Part 1): Technological advances and new steps in copyright protection* (1999), available at *http://www.cric.or.jp/cric_e/cuj/cuj.html*. ["Koshida"].

204 *Id*.

205 Article 120bis, Copyright Law of Japan.

206 Koshida, note 203.

207 Article 30(1), Copyright Law of Japan.

208 Article 30(1)(ii).

3.5.1.1(b) Unfair Competition Prevention Law

The Unfair Competition Prevention Law, like the Copyright Law, prohibits only the trafficking in devices and not the act of circumvention itself. The Unfair Competition Prevention Law protects "technical restriction means." These are defined to include "the means for restricting the playing of images and audio material, the execution of programs or the recording thereof by electromagnetic method, that is, a method of recording and transmitting signals to which playback devices specifically respond . . . or a method of recording and transmitting in recording media by converting images, audio material or programs . . . ."[209]

The definition contemplates both access controls and copy controls, to the extent that these measures restrict "recording." As with the Copyright Directive and the DAA, the reference to "recording" suggests that technical means that restrict the unauthorized exercise of copyright rights other than the reproduction right may not be covered by the Unfair Competition Prevention Law. The Copyright Law, as noted, however, contemplates protecting technological measures that may be used to protect other copyright rights.

Article 2(1)(x) of the Unfair Competition Prevention Law provides that it is an act of "unfair competition" to "convey, deliver, [or] exhibit . . . equipment that only have the function of preventing the effect of a technical restriction means and making it possible to view and listen to images and audio material sounds [etc.] . . . or record images [etc.] . . . that are restricted by commercially used technical restriction means," and includes devices incorporating such devices.[210] Online distribution of such programs is prohibited as well. The Japan Patent Office commentary states that this article covers acts that circumvent "copy restriction" technology, while Article 2(1)(xi) covers access control technologies.[211] The Serial Copy Management System is identified as an example of the former while CSS is described as an access control technology.[212] Modification chips used in connection with unauthorized playing of video games are identified in accompanying materials as circumvention devices.[213]

Article 2(1)(xi) applies, as noted, to protect access control technologies from circumvention devices. In summary, it prohibits trafficking (including through online distribution) in devices (including products incorporated in other devices) that circumvent commercially used technical means that prevent persons (other than those who are specified) from viewing and listening to images and audio works, if and to the extent such products only

---

209 Article 2(5), Unfair Competition Prevention Law. See Japan Patent Office, Asia-Pacific Industrial Property Center & Japan Institute of Innovation and Invention, *Outline and Practices of Japanese Unfair Competition Law* 22 (1999) (translating and commenting on the law), available at *http://www.apic.jiii.or.jp/facility/text/2-10.pdf* ["JPO/APIC Outline"].

210 Article 2(1)(x), Unfair Competition Prevention Law.

211 JPO/APIC Outline, note 209, at 21.

212 *Id*. at 45.

213 *Id*. See *also* Ministry of International Trade and Industry, *Amendment to the Unfair Competition Prevention Law (Draft)* (March 1999) (describing mod chips that enable playback of copied software as example of device that circumvents usage control means), available at *http://www.meti.go.jp/english/report/data/gCD1103e.html*.

have the function of enabling persons to play back images or audio works, execute programs or record images, audio works or programs that are so restricted.[214]

The text of these provisions, as well as the commentary, highlight that only devices that have the exclusive function of circumventing technical means are prohibited. None of the other jurisdictions discussed in this paper limit the scope of the prohibition to "sole purpose" products.

Japanese law implements the WIPO Treaties as follows:

	Act of Circumvention	**Circumvention Tools**
Access Control Technological Measure	Not prohibited	Prohibited (Art. 2(1)(xi) Unfair Competition Prevention Law)
Copyright Control Technological Measure	Not prohibited	Prohibited (Art. 120bis Copyright Law; Art. 2(1)(x) Unfair Competition Prevention Law)

3.5.1.1(c) Limitations and Exceptions

The Copyright Law does not contain a "no mandate" provision. The accompanying commentary, however, provides that using a "so-called non-reaction machine, which does not react to the signal used for the technological measures," is not to be regarded as circumvention.[215]

The Unfair Competition Prevention Law provides for an exception to the general prohibition in that law, making it lawful to distribute devices used in testing or research on technological protection measures.[216] The purpose of the exemption is to allow for the development of improved measures.

3.5.1.2 Remedies

Only criminal remedies are available under the Copyright Law for trafficking in circumventing technologies: a fine not exceeding one million yen or a prison term not exceeding one year. The accompanying commentary explains that there is no provision for a civil action because, at the time that a circumventing device is introduced, it would not be clear which works would be circumvented by it and, accordingly, which copyright owner would have the right to seek an injunction due to imminent infringement of its work would not yet be determinable.[217]

---

214 Article 2(1)(xi), Unfair Competition Prevention Law. See JPO/APIC Outline, note 209, at 23-24.

215 Koshida, note 203.

216 Article 11(1)(7), Unfair Competition Prevention Law.

217 Koshida, note 203.

Under the Unfair Competition Prevention Law, trafficking in circumventing devices and programs is classified as "unfair competition." Injunctive relief is available.

3.5.1.3 Rights Management Information

The Japanese Copyright Law generally follows the WIPO Treaties and other implementing legislation in the definition of "rights management information." The Copyright Law rather precisely defines rights management information as information concerning moral rights or copyright that is recorded in computer memory or transmitted electromagnetically with works, and that is used commercially in relationship to authorizing the use of works for management of copyright. Rights management information includes information that specifies works and owners and other matters that will (in the future) be specified by Cabinet Order, that relates to the manners and conditions of exploitation and that enables the foregoing "in comparison with other information."[218] The definition appears narrower than that used elsewhere in not, for example, including copyright notices and credits embedded in works.

The Copyright Law does not establish as a separate right, outside of copyright, the addition, removal or alteration of rights management information. Instead, such acts are considered to infringe the moral rights, copyright rights and neighboring rights of authors and performers. Specifically, the Copyright Law prohibits the intentional addition of false information; the intentional removal or alteration of information (other than where doing so is unavoidable); and the distribution of copies of works, knowing that there has been unlawful addition, removal or alteration of the rights management information.[219] Unlike other countries, however, there is no added requirement that the person, to be liable, must have provided, removed or altered rights management information knowingly in aid of infringement. Also, where the removal is part of a technical conversion or compression process, there is no violation. The criminal penalties for a violation of these provisions are as stated above for violation of the anti-circumvention provisions.

3.5.2 Other Laws

Other laws in Japan afford legal protection to DRM systems or other conditional access technologies. For example, the Broadcast Law prohibits any person from receiving a paid broadcasting service unless he has entered into an agreement with the broadcaster.[220]

4. DRM STAKEHOLDERS AND IMPLEMENTATIONS

4.1 Introduction

The functionality required for DRM has been explained in detail above. The users of the technologies–the stakeholders–are participants in the intellectual property rights value chain, which involves all those with an interest, either moral or financial, in the creation,

---

218 Article 2(xxi), Copyright Law.
219 Article 113(3), Copyright Law.
220 Article 52-5, Broadcast Law.

distribution and consumption of protected material. It is these stakeholders who will take advantage of DRM functionality in order to create an environment for the distribution and consumption of intellectual property in the digital environment. There have been many different view points, some essentially in agreement, some convergent and some still starkly in conflict.

This section identifies the various stakeholders and their position in the value chain, and describes their approach to the development, deployment and use of DRM to distribute, protect and consume protected content.

4.1.1 Rights Holders

Under the Berne Convention, a copyright comes into existence upon creation of a work. The owners of the copyright may be individual creators (natural persons), corporations (legal persons) or the ownership may be held jointly. In addition, a right may be licensed exclusively by the creator to a third party who, for the purposes of this section, will be treated as a rights holder.

Rights holders have a legitimate expectation that they can authorize, usually against payment, the exploitation of the intellectual property they own. In the analog domain (physical publishing, etc.), they have become used to a number of different methods by which they receive compensation for use. These include direct payment by users, payment through collective agreements which are managed by collective management societies, and payment by intermediaries, who resell to consumers.

The advent of DRM may create new opportunities for rights holders to manage their own rights. For instance, an individual creator may be able to contract with a DRM service provider (such as Overdrive or DWS) and offer her own works directly to the public. Corporate rights owners such as record companies and text publishers would also be able to make such arrangements, thus shortening the supply chain by cutting out traditional wholesale and retail intermediaries. The effect on the value chain of such changes is only beginning to become apparent and requires further study and negotiation among the participants.

4.1.2 Collective Management Societies

Collective management societies (“CMS”), which clear and administer rights for groups of authors, traditionally have played a central role in the licensing and distribution of, and the collection of royalties for, copyrighted content. Given the breadth of their experience in rights management, they naturally have had a keen interest in the use of digital technologies to manage rights. Rights management increasingly has become more complex, due both to the global nature of the exploitation and licensing of works and to the myriad of media and formats in which rights can be licensed. Not surprisingly, therefore, CMS see DRM systems as taking a significant role in assisting them in carrying out their functions. Indeed, some CMS already have used digital technologies to clear certain rights quickly and efficiently.

At the same time, some stakeholders may be of the view that the role of CMS should be more limited in a digital world particularly where rights holders might be able to license users directly. Stakeholders may also believe that the collective nature of the activities of CMS effectively or actually prevents rights holders from exercising their rights individually. The

CMS reject these views, noting that rights holders can, at least in theory, always choose between collective and individual rights management. And, the CMS believe that their critical position in the digital dissemination of content requires that their needs and functions be fully understood and assimilated in the design and deployment of any DRM systems.

CMS, perhaps concerned that the use of DRMs might obviate their role, also have argued that these systems do not substitute for the less ministerial "hands on" functions that they perform. Thus, even in a DRM-shaped world, CMS see themselves as continuing to carry out the auditing of royalty payments, as well as undertaking all the activities of a membership organization, such as engaging in collective bargaining with other rights holders and users, as well as participating fully in development of standards and public policy debates on copyright and enforcement.

CMS have pointed out that they are themselves actively involved in developing components of DRM systems, including assisting in creating standards for identifiers (e.g., ISWC) and participating in international fora to promote common standards (e.g., MPEG 21).

4.1.3 Intermediaries

When considering "intermediaries" in physical media, there is an understandable tendency to think in terms of the supply chain, particularly wholesalers and retailers–those organizations that form the distribution channel between the "content companies" and their end customers. However, any thoughtful consideration of the roles that must be undertaken in the digital value chain leads rapidly to the recognition that any organization positioned between the creator and the consumer must be regarded as an "intermediary" in the chain. This includes commercial organizations like record labels and print publishers; it also includes "public interest" organizations, such as libraries, which have traditionally performed very important aggregating and access roles in the information chain.

The traditional distribution of roles in the physical supply chain appears to have limited long-term application in the network environment. The tasks that must be undertaken in the chain can be arbitrarily disaggregated–and perhaps re-aggregated in entirely different ways.

However, the extent to which the chain can be reshaped depends to a very considerable extent on the effectiveness of communication. The network itself both provides the *physical* infrastructure for this communication and (through the "network effect") simultaneously drives the implementation of the *standards* infrastructure which enables efficient machine-to-machine communication.

If the reshaping of the value chain is to be truly effective, it is essential that this standards infrastructure be as open and non-prescriptive as possible. It is important, for example, that it makes no *a priori* assumptions about the aggregation of functions within the value chain. This may cause a substantial degree of discomfort for incumbent organizations, since there is a natural tendency for any organization to attempt to retain existing business models and practices (even though these may be inappropriate or irrelevant in the network environment).

The interests of intermediaries may therefore be in conflict with one another (and possibly also in conflict with the interests of consumers). It may prove very difficult for these

organizations to divorce their short-term interest from the long term. Nevertheless, it must be to the long-term advantage of all that DRM systems and infrastructure are designed to provide the greatest possible flexibility in terms of support for business models and digital supply chains, rather than simply providing mechanisms that mimic existing physical models.

4.1.4 Telecommunications Intermediaries

Network providers have not traditionally been involved in the intellectual property value chain. As "common carriers," they have been providers of cables on which information–phone calls or data–has been transmitted from one place to another. However, since the advent of the digital information economy, network providers have been keen to enter the value chain as Internet Service Providers in order to earn revenue from the supply of content services to their customers.

Network providers have increasingly been concerned about potential liability for any infringements of rights in content that they distribute. Traditional telecommunications carriers have not, historically, been held responsible for the transmission of infringing content. As Internet Service Providers ("ISPs"), however, both carriers and new entrants may be subject to claims that they are directly or contributorily liable when they transmit, cache and store infringing content. Both the United States of America, under the DMCA, and the European Union, in the Electronic Commerce Directive, have recognized that an ISP is not fundamentally at fault when it innocently engages in these activities. For this reason, the legal regimes in both the United States of America and the European Union circumscribe an ISP's potential liability where the ISP is notified about infringing content and then removes or disables access to it. (See Sections 3.2.1.2 and 3.3.1.2(c) above).

ISPs are extremely interested in deploying digital rights management tools that may provide them with a measure of protection against legal dangers. On the other hand, they do not wish to risk damaging their relationships with customers by establishing apparent barriers (if DRM is perceived as a barrier) to the enjoyment of the content they deliver.

4.1.5 Technology Vendors–Software

The sector of the software industry developing technologies for digital rights management has gone through a number of distinct phases. To understand how DRM software technology vendors relate to the rest of the value chain, it is necessary to understand some recent software market history. Originally, the sector was almost exclusively the preserve of small start-up companies, mostly in the United States of America. While some of them started their research and development phases during the late 1980s, the majority came into existence in the early to mid-1990s. As interest in DRM technology grew, so did the apparent fortunes of many of the companies. While they did not succeed in acquiring large numbers of customers, many of these small companies registered patents during this period. Their increasing patent portfolios were enough to bring in very substantial sums of venture capital and the sector thrived, especially during the boom days of the late 1990s. This led many of these companies to extend their business models to providing services as well as software. The expectation at the time was that the companies would make profits based on transactional fees deriving from the use of their software and services. While this was not very appealing to rights owners, it appeared at the time to be within the power of these companies.

However, just after the turn of the millennium, the market situation dramatically changed. With the collapse of confidence in the entire software sector, many of the smaller companies became insolvent, some of them entirely lacking customers. Those that remained continued to struggle prior to collapse, consolidated through mergers or were acquired, along with their patent portfolios, by larger companies.

This has resulted in a DRM software sector that is largely dominated by a few global players, such as Microsoft, IBM and Adobe. It is these companies that seem to be setting the agenda for DRM software, and the smaller companies are providing add-ons for the baseline, proprietary technologies. However, and it is a big however, rights owners have recently become very active in stating their requirements for DRM through participation in standards initiatives. It is here, in the debate surrounding the extent to which the online and offline DRM environment will be standardized, which will have a substantial effect on interoperability, that the future of software companies and the revenues they will make from deploying DRM will be determined. It should also be said that the outcome of the standards debate will determine much about the relationship between rights owners and technology companies. These subjects are discussed further in Sections 2.5.2 (standards) and 4.2.7 (interoperability).

4.1.6 Technology Vendors–Hardware

Some of the most significant developers of content protection technologies have been hardware companies, including both consumer electronics and information technology companies. Dating back to the 1980s (and even before), the technology industry had been somewhat resistant to legal limitations on copying devices, such as videocassette recorders and audio recording products.

With the introduction of digital technologies, accommodations were reached with rights holders. The main impetus for the rapprochement was the acknowledgement that new digital formats, from both a content and technology side, required the cooperation and support of all affected industry sectors. Without the support of the rights holder community, new digital recording and processing products might be stillborn. Such support would require that content protection technologies were developed and implemented in digital products.

In the late 1980s and early 1990s, fairly simple content protection schemes were proposed by technology companies. These included, as discussed above, the Serial Copy Management System ("SCMS") to limit serial copying of digital audio content. The Copy Generation Management System-Analog ("CGMS-A") was proposed to limit copying of marked analog audiovisual content by digital recording devices. From the mid-1990s to the present, the major technology companies have moved rapidly to develop more sophisticated, proprietary content protection schemes, including those described in Section 3.2.1.

To protect DVD audiovisual content, for example, Matsushita Electric Industrial Co. and Toshiba developed the CSS, which, as noted, is now being licensed through the DVD Copy Control Association, Inc ("DVD CCA"). Digital Transmission Content Protection ("DTCP"), which is used to protect content within the home, was developed by Hitachi, Intel, Matsushita, Sony and Toshiba. Intel has been the principal promoter of High-bandwidth Digital Content Protection ("HDCP"), which is being licensed to protect digital video content across buses to PC monitors and to other display devices. Matsushita, Toshiba, Intel and IBM have developed various content protection technologies for DVD Audio and associated

recording technologies, including Content Protection for Prerecorded Media ("CPPM") and Content Protection for Recordable Media ("CPRM").

Hardware companies also have been at the forefront of developing and promoting watermarking technologies. Currently, the DVD CCA is considering whether to adopt a technology for marking DVD video disks. Two technologies have been under consideration for some time. One was developed by the "VWM Group," which includes such major technology companies as Hitachi, NEC, Philips, Pioneer and Sony, as well as two smaller, but central, players in the field of content protection, Macrovision Corp. and Digimarc. Toshiba has developed the other watermarking technology.

The principal drivers for these initiatives is the business imperative of using these technologies to support the proliferation of digital products, including recording and playback devices, personal computers and associated processors. Critical to the understanding of each of the above-described technologies, which are intended to complement one another in a link-based architecture in the home, is that they are supported by comprehensive content protection schemes that are mandated by license. The terms and conditions of these licenses, in turn, are the subject of an intensive and lengthy process of collaboration, consultation and negotiation with rights holders. Because they are entrusting their valuable content to the protection afforded by these technologies, rights holders insist that no substantial changes be made to the technologies or to the associated licensing conditions without their having some rights of review or approval.

4.1.7 Professional and Commercial End Users

The requirements of end users of content (primarily information) in a professional or commercial context are not necessarily substantially different from those of an individual in his or her private life. However, the points of emphasis may be somewhat different. There are three issues that merit particular attention.

First of all, the whole issue of *authority* and *authenticity* is likely to assume a more central position: Is this document what it says it is? Does it come from a trusted source? These questions can be particularly pressing if there are issues of professional liability or reputation to be considered.

Secondly, the question of *confidentiality*, the "right to read anonymously," may take on an altogether different significance. To take a simple example, a competitor able to track the reading matter of a pharmaceutical research scientist should be able to draw fairly accurate conclusions about research directions and possible results.

Thirdly, there is a requirement for access to content mediated through the recognition of *membership of a class* of individuals, for example, being an employee of a corporation or a member of an association. Today, those mechanisms tend to be relatively crude, based on physical location and IP address authentication. The requirement for much more sophisticated management of digital identity is rapidly being recognized; however, the implications for personal privacy are potentially far-reaching. As a person may also be a member of a group that is privileged by copyright law, identifying the context in which use of copyrighted material is made may raise challenging issues about the availability of lawful exceptions to a rights holder's exclusive rights. For example, as a teacher and in the course of educational activities, an individual may make use of such material by virtue of "educational

exceptions" that exist in certain jurisdictions or such uses may otherwise be authorized as fair uses; however, those exceptions may not be applicable with respect to the same material when the individual uses it in his or her private capacity.

In discussing the application of DRM, it is essential to recognize the existence of these challenges, even if solving them currently appears to be elusive.

4.1.8 Consumer End Users

Consumers have expectations about how they are able to access and use content. Their expectations are based on their long-standing practices, both with respect to content that they acquire lawfully and content that they increasingly are able to obtain without authorization, such as through peer-to-peer file sharing.

On the one hand, consumers feel an entitlement to make copies of content that they lawfully acquire, whether from free, over-the-air broadcasts or from CDs that they purchase. Consumers also have become accustomed to being able to copy television content on recording devices, even if the content is made available on a conditional access (pay television) or pay-per-view basis. At least in the United States of America, there has been an effort to reflect these expectations and practices in the "encoding rules" that are part of the content protection schemes described above in Sections 3.2.1 and 4.1.6 and in the Digital Millennium Copyright Act.[221]

On the other hand, consumers candidly may concede that certain types of behavior–commercial piracy and massive distribution of copyrighted content even in a non-commercial context–are inappropriate. Many consumers like paying nothing for content–hence the popularity of file sharing–though most would be willing to pay something in the right circumstances and for the right product.

Not surprisingly, then, technologies that are used to restrict customary consumer behaviors are not welcomed by consumers or their representative organizations. In many jurisdictions well-focused groups represent consumer or public interests with respect to digital technology, including the deployment of DRMs. In the United States of America, for example, the Home Recording Rights Coalition has been involved in consumer and non-commercial recording issues since 1981. More recently, the Electronic Frontier Foundation and Public Knowledge, among others, have participated in public policy debates over inter-industry negotiations regarding content protection standards and DRM-related issues, and have actively intervened in discussions, before Congress and at the Federal Communications Commission, regarding the role of government in mandating industry-negotiated accords. In Europe, the European Consumers' Organization has represented user interests in DRM issues and with respect to European Community copyright initiatives.

In addition to examining the potential effects of DRM deployment on consumer practices, concerns have also been expressed about the impact of DRM technologies on consumer privacy, particularly as DRM schemes could enable rights holders and distributors to collect and use personal data about consumers' purchasing habits and their usage of copyrighted material. These privacy issues are discussed in Section 5.2.1.

---

[221] See note 56, describing the encoding rules in Section 1201(k) of the DMCA.

4.2 DRM in Action

4.2.1 Introduction

While this document sets out the legal and technological background for the use and functionality of DRM technology, users throughout the value chain are principally interested in its deployment. In this respect, it is important to say that deployment of the technology is still in the early stages. There are many reasons for this, legal, technical and commercial. For instance, the various legal instruments that will protect deployment and operation of technical measures of protection are not yet in place universally. Secondly, the commercial models through which rights owners will exploit their content are not yet elaborated beyond fairly basic schemes. And thirdly, the technology to create these models, including the standards upon which those technologies will be based, is still in the process of development.

A few relevant points can be made about current implementations, however.

a) Most implementations of DRM are currently limited to specific content sectors (such as the publishing or music industries). DRM is not yet being applied to rich multimedia content, where music, audio-visual and text are combined. Such vertical separation between sectors reflects analog content delivery where it is technically and physically difficult to combine different media types. It is expected that as DRM becomes more flexible, enabling on-the-fly combination of content types, the vertical separation between content delivery streams will start to become more porous, then invisible.

b) The business models to support the delivery of content are still fairly basic. Subscription models, pay-per-view/listen and outright purchase are the dominant modalities. It is expected that in future, there will be a proliferation of business models, many of them based on the purchase of hybrid products; such commercial peer-to-peer models where the rights holders are compensated remain rare. The majority of peer-to peer-models are dealing in unauthorized content.

c) Payment systems are still primitive, with most payments being made by credit card.

4.2.2 DRM services for Audio

A number of online music services have emerged in the last two years, led by the major record companies and online content distribution companies such as RealNetworks through its Rhapsody service. These legitimate music download services have been set up to provide an alternative to the illegitimate peer-to-peer services. It is too early to assess the success of legitimate online music services.

MusicNet was founded by BMG, Warner Music and EMI. The venture has entered into agreements with Sony and Universal. Therefore, the online music service now provides content from the five major record labels. Users have access to MusicNet’s content via distribution partners such as Rand AOL. The system allows users to download and stream DRM-enabled music content. According to the type of subscription chosen, users can save music on their hard disks and burn it onto CDs. It costs users about US$10 a month to listen to an unlimited amount of tracks from MusicNet’s online catalog.

iTunes was launched in the U.S.A. in the spring of 2003 by Apple. The service uses the Apple iPod device as its player, which stores DRM-protected tracks, downloaded from the iTunes service via a computer terminal. The service has proved extremely popular and Apple announced in June 2003 that it had sold more than five million tracks through its iTunes Music Store.

Pressplay was launched by Vivendi Universal and Sony. The service is, in principle, similar to MusicNet's business model. All the tracks distributed on the network are DRM-enabled. Pressplay has recently been purchased by the CD burning software company Roxio, which also bought the Napster assets in late 2002.

More recently, a new online music venture, named Echo, was founded by several major music retailers in the U.S.A., including Best Buy, Tower Records, Virgin Entertainment Group, Wherehouse Music, Hastings Entertainment and Trans World Entertainment.

OD2 is a European-based music download service, co-founded by the musician and performer Peter Gabriel. OD2 provides distribution services to major labels, such as Sony and BMG.

4.2.3 DRM Services for Audio-Visual

Major movie studios have recently started to provide on-demand movie services over the public Internet. The implementation of DRM represents a crucial part of their strategies. The most successful initiatives have been so far in the adult content industry. On the consumer market side, the new MovieLink on-demand portal was launched in 2002. MovieLink is a joint venture between MGM Studios, Paramount Pictures, Sony Pictures Entertainment, Universal Studios and Warner Bros. Studios. The service, which is available to U.S.A. residents only, was launched as a pilot project in November 2002. It provides a collection of 200 movies from the major movie studios.

The service allows users to pay for content with their credit card and download movies on their hard disks. Every film title is embedded with proprietary DRM technology, such as that contained in Microsoft's Windows Media Player. Once downloaded, the movie file resides on the user's hard disk for 30 days. If the file has not been played during this period, it will expire. Once the file has been played, an automatic countdown of 24 hours is activated. After the 24-hour period, the file becomes unusable.

4.2.4 DRM Services for Text

DRM initiatives have also been launched in the text industry. Microsoft has developed a DRM system for customized electronic publications called the Digital Asset Server. Its main market competitor, Adobe, is selling the Adobe Content Server. Palm's software division, Palm Digital Media, has also developed a customized DRM system for distributing its eBooks. Most major online eBook stores have incorporated the latter technologies. DRM aggregators such as Overdrive, are using technologies from several DRM vendors to build custom systems for the online publishing industry.

4.2.5 DRM Services for Software

Games consoles and online games systems are increasingly being protected with DRM systems. The Microsoft Xbox games console, for example, includes a 128bits strong hardware encryption system, which prevents users from playing pirated games and using the console for any other purpose. Sony has also included DRM in its PlayStation 2 and Nintendo in its GameCube.

However, the proliferation of so-called "mod chips," which are add-on circuits that can be installed on the main board of a console, allows users to bypass the copy protection of a games console. Although the problem posed by mod chips may not yet be as pressing as the challenges arising from unauthorized uses of music, movies and text, both videogame and software companies increasingly are concerned about the penetration of mod chips in key markets. For this reason, as discussed in Section 3, Sony has sued mod chip distributors successfully in the United States of America, the United Kingdom and (after an appeal) Australia.

4.2.6 Extending DRM to Other Industry Verticals

It is slowly being recognized that the technology for DRM can be applied in sectors other than the copyright content industries. Although the secure management of proprietary information has always been an issue in commerce and industry, there is increasing awareness that the knowledge contained within an organization is its single most important (and most valuable) asset. In this context the definition of knowledge value goes far beyond traditional definitions of intellectual property as defined by patents, copyright and proprietary databases. Increasingly, members of a corporate board of directors and senior executives are coming under pressure both from regulatory authorities and their own shareholders to demonstrate that they are exercising a proper duty of care to maintain the security of information that, in many cases, represents the majority of stakeholder value.

For these reasons, there is beginning to be an interest in the kind of technologies discussed in this paper. By employing DRM techniques, companies hope to be able to control usage of information, where before they were only able to control access. By this means, their assets will be more closely protected and in addition they will be able to track where their information is being consumed. This will provide a much greater level of information security than is currently possible.

4.2.7 Interoperability

The theme of interoperability runs through all discussions of DRM and has already been noted in the section on standards (Section 2.5). Its importance to the future of secure content distribution cannot be understated. Perhaps the best way to define interoperability is "the ability for content and rights usage rules to be supported, unambiguously interpreted and enforced across multiple *proprietary* DRM systems and end user devices." The term also refers to the ability to use datasets from different origins as though they were built to a common standard (essential for using metadata from different communities).

Currently, interoperability is not available to rights holders or users since most DRM implementations are based on "island solutions" from a particular vendor, rather than widely adopted standards. Furthermore, most implementations are limited to a single media type. This may have something to do with the traditional segmentation of the media industries, just as it may have something to do with the availability of technology.

Although standards will be essential to bring interoperability into existence, there will also be a need for business drivers represented by consumer demand. In the absence of an appropriate measure of interoperability enabling different systems to work together without inconvenience to the user (whether rights holder or consumer), it is unlikely that DRM will be entirely successful. Given the importance of interoperability, it is not surprising that questions have been raised as to whether governments properly should intervene to compel interoperable DRM systems. This issue is discussed in Section 5.2.3.

5. POLICY ISSUES RAISED BY DRM TECHNOLOGIES

The development, implementation, protection and use of DRM technologies raise many issues of policy for national governments and international institutions, including the European Commission and WIPO. Many of these have been suggested and identified in the preceding discussion. This section of the paper pulls together and discusses some of these themes.

5.1 Intellectual Property Issues

5.1.1 Implementation of WIPO Treaties

The WCT entered into force on March 6, 2002 when 30 states had ratified or acceded to it. The WPPT entered into force on May 20, 2002. Some 42 states are now (as of August 2003) parties to the WCT, and 42 are parties to the WPPT.

Implementation of the WIPO Treaties was relatively rapid in the United States of America, Japan and Australia.[222] It has been slower in the European Union, as the process of adopting the Copyright Directive has taken some time. Furthermore, in the European Union, only two of the Member States met the deadline for transposition of the Copyright Directive

[222] It may be noted that although Australia has implemented the WIPO Treaties, see Section 3.4, it has yet to ratify them.

into national law and, as of early August 2003, only five have done so. A number of other major countries have not yet implemented the WIPO Treaties.

With respect to the countries that have implemented the WIPO Treaties, and to the European Union, approaches have varied somewhat. Such variation was contemplated by the Contracting Parties and is permitted under the texts of the WIPO Treaties themselves. Several types of variations have been identified.

In most countries, anti-circumvention provisions appear to be implemented in or adjacent to copyright and related laws. In some countries, they are included in unfair competition laws. Furthermore, some countries have become parties to the WIPO Treaties without making any significant changes to their national legal regimes; those countries believe that their existing legal framework is adequate to comply with their treaty obligations.

Each implementing jurisdiction has had to determine which types of technological measures to protect, i.e., those that control access to works as well as those that limit the exclusive rights of the rights holder. Most jurisdictions appear to protect both types of technological measures.

Further, provisions that implement the WIPO Treaties generally restrict acts that are predicate to circumvention. These include the manufacture and trafficking in circumvention tools. Some implementing legislation goes further, however, and prohibits various types of acts of circumvention. In such cases, the legislation may exempt persons from liability for certain classes of circumventing acts. Or, as in the United States of America, acts of circumvention may not be prohibited in connection with technological measures that protect copyright rights, on the basis that such a circumventing act should be assimilated to copyright infringement itself.

Differences are apparent in the extent to which there are exemptions or limitations for circumventing acts or products. With respect to anti-trafficking provisions, moreover, laws differ between whether a device should be outlawed or permitted, depending on whether its "sole" or merely its "primary" purpose is circumvention.

To date, it does not appear that the speed with which the WIPO Treaties have been implemented, or the variations in the implementing statutes, have had any measurable effect on the development or use of DRMs. Over time, it can be expected that all the Contracting Parties will live up to their treaty obligations. It will then remain to be seen whether differences in implementation will have any meaningful effect on the deployment of DRMs or the protection of content delivered through DRM solutions.

5.1.2 Effect of DRMs on Copyright Exceptions and Limitations

In using DRM technologies, rights holders will need to be mindful of the exceptions and limitations in the anti-circumvention provisions and of the copyright exceptions (at least in the European Union). The fit between the technological and commercial capabilities of DRMs, on the one hand, and the legal and policy outcomes reflected in exceptions and limitations, on the other, may be uneasy.

If, for example, in the European Union, rights holders use technological measures that deprive beneficiaries of an exception, they may–at some future time–have to worry about

measures that Member States might take to ensure that those persons will, in fact, enjoy that benefit. Indeed, as contemplated by the proposed legislation in Germany, rights holders' failure to ensure that beneficiaries can enjoy the exceptions may subject them to sanction. DRMs can be developed and used with usage rules that are roughly consistent with the exceptions, but inevitably they will not be able to account for every situation where an exception is (or ought to be) available but where the DRM technology is not itself capable of accommodating or verifying the legitimacy of the beneficiary's entitlement to the exception.

Indeed, in the United States of America, the relationship between the use of DRMs and copyright exceptions was discussed at length in connection with including the concept of legitimate circumvention–based on fair uses–in the DMCA. The "fair use" doctrine is so malleable and so dependent on particular facts and circumstances that ultimately Congress determined that there could be no general "fair use" exception to the anti-circumvention provisions; however, that question is presented once again in connection with legislation currently pending in the United States of America. Similarly, unless DRMs are developed so that they are capable of authorizing usage on a case-specific basis, i.e., determining when a requested use is "fair," it will be difficult for DRM solutions to accommodate that copyright exception.

Issues of whether a technological measure can accommodate lawful private copying or fair uses have arisen on multiple occasions in the United States of America. In each case, it was noted that the law or technology made some "rough justice" accommodation to fair use concerns, while recognizing that particular legitimate "fair uses" would no longer be technologically possible.

In connection with the Audio Home Recording Act, for example, the required implementation of the Serial Copy Management System (or its functional equivalent) meant that no more than two generations of digital audio copies (even of a user's own legitimate copies of copyrighted works) would be technically possible; no digital copying from a digital copy would be possible. As to the first of these two limitations, however, such serial copying presumably would have been consented to by the copyright owner. As to the second, serial digital audio copying might in some cases constitute fair use (for such purposes as making mixes and selection recording) and should if so be lawful.

Also in the United States of America, as described in Sections 3.2.1 and 4.1.8, certain "encoding rules" have been the subject of discussion for several years.[223] These rules allow for unlimited serial copying of content in some circumstances, one-generation copying in others and no copying in yet others. Here, too, one can conceive of instances of authorized private copying or fair uses that would be stymied by the application of these rules. And, yet again, the compromises struck in these encoding rules have been thought (by some) to enable adequate amounts of private, non-commercial reproduction so that the restrictions effected by the rules are tolerable.

In a related vein, the WIPO Treaties require Contracting Parties to provide adequate protection for technological measures that are used to protect copyright and related rights. Implementing legislation generally has followed the subject matter of that mandate. What, then, is the legal status of DRMs that might be used to deliver public domain content in a

---

[223] See Marks/Turnbull, note 42.

protected manner? Are acts to circumvent, and products designed to circumvent, such DRMs lawful because the content they protect is not subject to copyright?

Consumers, educational institutions and academics have registered concerns that DRMs might be used to lock up content in which the term of copyright has expired. At that point, however, it is thought that the anti-circumvention provisions will no longer be applicable. Rights holders and DRM providers have not uniformly adopted the position that legal protections for DRMs are inapplicable where the DRM is used to protect a public domain work. Rather, in their view, so long as a particular DRM is used to protect some works that are under copyright, it would and should remain unlawful to develop tools that could be used to circumvent that DRM, even when the tool is used to circumvent technological measures applied to a public domain work. They would argue that the unlawful activity is the trafficking in a device that circumvents a DRM that is currently being used to protect a copyrighted work. In effect, therefore, the effort to limit the anti-circumvention provisions only to DRMs when and as used to protect copyrighted works might prove to be relatively impotent, because devices that circumvent such DRMs (even when applied to protect works that are out of copyright) might still be unlawful.

Whether DRMs and the associated legal protections will adequately accommodate legitimate exceptions and limitations including in national copyright laws will become clearer as those systems are implemented. It seems probable that not every instance of private copying, copying in aid of reverse engineering or copying as part of a fair use will be permitted by a particular DRM or contract. Nor, without doubt, will legislation implementing the WIPO Treaties allow for circumvention in all such situations. Inevitably, legitimate uses may be thwarted by DRMs, contracts with rights holders and distributors of content, and the laws that support them. End users and governments have been concerned that contracts might ultimately usurp statutory or judicial exceptions to or limitations on judicial rights.[224] A special note here might be made of users' concerns that among the most significant limitations on the rights of an author–the limited nature of the term of copyright–might itself be overridden by contract: will rights holders be able to exercise control over public domain works, well past the term of copyright, by conditioning access to those works (where a DRM controls access) on users complying with usage restrictions?[225]

Precedents may suggest that even an inexact accommodation by DRMs and distribution contracts of such legitimate uses may be acceptable. Rights holders may make available certain types of licenses to particular classes of beneficiaries of statutory exceptions, or they may provide content in certain formats to different types of persons. Rights holders also are likely to be keenly aware of the monitoring and implementation mechanisms being put in place with regard to the effect of DRM usage. Furthermore, should rights holders fail to accommodate private copying when implementing DRM solutions, at least in the European Union, the Copyright Directive makes quite clear that Member States always have the option

---

224 See, *e.g.*, Copyright Law Review Committee, *Copyright and Contract* (April 2002) (Australian report summarizing submissions on the prevalence, effects and desirability of contracts that purport to override copyright exceptions), available at http://www.law.ecel.uwa.edu.au/ipcr339/CopyrightContractAct.pdf.

225 See, *e.g.*, B. Hugenholtz, *Copyright, Contract and Code: What Will Remain of the Public Domain*, 26 Brook. J. Int'l L. 77, 78 (2000) (arguing that the "combination of contract and technology poses a direct threat to the copyright system as we know it").

of intervening directly (or imposing sanctions), to ensure that such practices allowed under copyright exceptions are not prevented by technological measures.

Consumers, educators, librarians and other users of copyrighted content may tolerate some imprecision in the extent to which DRMs accommodate their requirements. Their willingness to do so, however, may depend on the extent to which they perceive rights holders as not being abusive in their use of DRM technologies, and if the broader benefits of having content become available through a DRM-driven environment are manifest.

5.1.3 DRMs and Private-Copying Levies

As discussed in Section 3.3.2, in connection with the discussion of the European Commission's Digital Rights Management Workshop, considerable attention in Europe has focused on the relationship between private-copying levies and implementation of DRM technologies. (Although the United States of America applies levies on digital audio recording devices and media under the Audio Home Recording Act, the range of devices and media on which levies are imposed is relatively restricted and the elimination of these levies has not been the subject of any meaningful debate in recent times.) The historical justification for these levies is to compensate rights holders for private copying of their works not specifically authorized and for which no remuneration is otherwise directly made available. The copyright laws of a majority of the Member States of the European Union provide for levies on recording devices and/or media.

In Europe, the Copyright Directive specifically notes that with respect to non-commercial private copying, Member States shall provide for copyright exceptions "on condition that the rightsholders receive fair compensation which takes account of the application or non-application of technological measures."[226] It is recognized, therefore, that the application of DRMs will affect whether rights holders obtain "fair compensation." To the extent that private-copying levies are imposed on devices and media, it has been pointed out by consumers and the technology industry that allowing rights holders to obtain additional compensation through use of a DRM technology might result in double compensation that exceeds what is "fair."

The Copyright Directive deals directly with the relationship between national levy schemes and the use of DRMs only in its recitals. Recital 38 states that in connection with private use, Member States may allow for an exception accompanied by "fair compensation"; in this regard, "remuneration schemes" may be introduced or continued.[227] The Recital allows for continuation of the schemes with respect to analog private reproduction, but acknowledges that "digital private copying is likely to be more widespread"; that there are differences between digital and analog private copying; and that "a distinction should be made in certain respects between them."[228]

---

226 Article 5(2)(b), Copyright Directive.

227 Recital 38, Copyright Directive.

228 *Id*.

Recital 39 has been central to the discussions on the relationship between levies and DRMs. It states as follows:

> *"When applying the exception or limitation on private copying, Member States should take due account of technological and economic developments, in particular with respect to digital private copying and remuneration schemes, when effective technological protection measures are available. Such exceptions or limitations should not inhibit the use of technological measures or their enforcement against circumvention."*[229] *[emphasis supplied]*

The Recital clearly recognizes the relationship between private copying and associated levy schemes and DRMs. When DRMs that are "effective" become "available," the Copyright Directive suggests, levy schemes should be modified or even phased out. Though the concepts of effectiveness and availability may be transparent theoretically, what is effective or available may be devilishly difficult to determine in practice. Although it may be possible to ascertain when a DRM is "available," with respect to what types of content must a DRM be sufficiently "available" such that it no longer is appropriate to impose a levy for private copying of such content?

Perhaps even more difficult questions are raised by the concept of "effectiveness." Although a DRM can be "effective" in limiting unauthorized copying, what does it mean to be "effective" for purposes of modifying or phasing out a levy scheme? For example, if a DRM only permits private copying of a particular type of content on certain classes of recording devices and media, should the levy be removed from those types? But what if those same types also can be used to make private copies of content that is not subject to a DRM, content for which the rights holder otherwise obtains no compensation? Will Member States need to examine each DRM in association with each type of content and each class of digital recording device or media to effect the transition? As it now appears that these decisions will be made at the national level, how likely is it that there ultimately could be inconsistent approaches adopted within the Internal Market?

Here, too, it is improbable that there would be absolute precision between the complete protection of content through DRMs and the elimination of levies on recording devices and media used for the private copying of such content. Again, it may be sensible to adopt a "rough justice" approach that would rest on the Member States concluding that there is enough actual or potential use of DRMs in the market for digital content to provide adequate remuneration to rights holders for private copying. After surveying the landscape, Member States could reach the conclusion that rights holders are, in the aggregate, fairly compensated for such uses. In such a situation, where effective DRMs are "available" for use in some meaningful sense, Member States could consider effecting a transition away from any levy-based approach on which rights holders have been remunerated.

---

229 Recital 39.

5.2 Other Policy Issues

5.2.1 Privacy

The use of DRM technologies raises issues beyond the protection of intellectual property, including, perhaps most notably, individual privacy. As described in Section 2.4.9, the use of these technologies can be seen as having two different aspects that are, respectively, privacy enhancing and possibly threatening to privacy interests.

DRM technologies often rely on secure communications and authentication between two or more devices. Often, they ensure that content is delivered to a person who has agreed to the terms and conditions by which access to copyrighted material is made available. Payment may be made in such a manner as well. In these circumstances, the transaction between the rights holder and consumer is kept private from third parties. Similarly, to the extent that DRM technologies enable a consumer to make a legitimate transfer of a work, or of the authorization to use a work, to a third party, the DRM technologies preserve the privacy and integrity of the transaction. Finally, to the extent that DRM technologies enable rights holders and distributors to maintain records of consumer data and transaction history, the consumer's process of purchasing and receiving DRM-protected content may be made both quicker and efficient. In each of these respects, consumers may see DRM technologies as beneficial.

Consumers and privacy advocates have, however, seen a potentially darker side to the use of DRM systems. They have expressed concerns that the use of these technologies will inevitably facilitate the gathering and aggregation of consumers' personal data by rights holders and content distributors. Consumers are fearful of profiling and technologies that combine data about their usage with their identities. They worry that third parties may be able to gain access to an individual's personal computer for purposes of authenticating devices in order to ensure that they are "trusted."

A further concern is that consumers may lose their ability to make legitimate, but anonymous, use of copyrighted content. In certain "fair use" situations, for example, users of copyrighted content may want to use material without necessarily associating themselves personally with the work that they have accessed and used. DRM technologies, however, often require a bilateral transaction between a rights holder and a known consumer and the rights to use the work could travel with the content itself. Here, then, the ability of the consumer to use the content anonymously will be lost.

To be sure, consumers who are concerned about the loss of personal privacy might be able to disable these DRM systems, or simply refrain from acquiring content online. Nevertheless, concerns have been raised that by doing so, consumers may–albeit by their own choice–deprive themselves of the ability to have access to copyrighted materials that, increasingly, may be obtained only through DRM technologies.

Different governmental institutions have focused to varying extents on the relationship between the use of DRM systems and privacy concerns. In the European Community, Recital 57 of the Copyright Directive highlights the issues in stark relief: rights management systems, it is noted, "process personal data about the consumption patterns of protected

subject-matter by individuals and allow for tracing of on-line behavior."[230] The Recital warns that technical means should incorporate "privacy safeguards" as contemplated by the European Data Protection Directive, which protects personal data.[231] The Data Protection Directive sets out a comprehensive framework that applies to the collection, use, processing, disclosure and security of personal data in the Member States, as well as the transfer of such data to third countries. The Data Protection Directive applies directly to automated collection and processing systems, such as those used in a DRM system.

Under the Data Protection Directive, personal data may only be collected and used for the specified purposes authorized by the "data subject," i.e., the person whose data is at issue. Furthermore, the directive requires that data controllers implement "appropriate technical and organizational measures to protect personal data against . . . unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network . . . ."[232] Given the breadth of the Data Protection Directive and its immediate relevance to DRM systems, concerns that rights holders and distributors might abuse the data that they collect from consumers should be at least somewhat allayed.

In the United States of America, protection of personal data has often been described as a patchwork of protection, involving different federal statutes and state laws. Over the last several years, both the Federal Trade Commission and state attorneys general have been active in ensuring that companies that use technological means to protect or collect data accurately represent to consumers their security, privacy and data collection practices. These government bodies can bring suits in court and extract civil penalties from companies that do not implement adequate security measures to safeguard data on their systems.[233]

Also in the United States of America, privacy issues were discussed in connection with the passage of the DMCA, and the DMCA specifically recognizes some relationship between the use of the digital technologies and privacy concerns. As discussed in Section 3.2.1.1(c), Section 1201(i) of the DMCA creates a privacy-driven exception to the anti-circumvention provisions: it is not a violation of the statutory prohibition for a person to circumvent a technological measure that protects cookies or other copyrighted works–such as computer

---

230 Recital 57.

231 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Official Journal L 281/31, 23/11/1995 ["Data Protection Directive"].

232 Article 17, Data Protection Directive.

233 See *In the Matter of Microsoft Corp.*, FTC No. 012 3240 (2002) (see *http://www.ftc.gov/os/2002/08/microsoftcmp.pdf* (complaint filed) and *http://www.ftc.gov/opa/2002/08/microsoft/htm* (settlement) (settlement of complaint involving Passport authentication system and prohibiting misrepresentation of information practices; requiring maintenance of a comprehensive information security program)); *In the Matter of Eli Lilly and Co.*, FTC No. 012 3214 (2002) (see *http://www.ftc.gov./opa/2002/01/elililly.htm*) (settlement to undertake intensive oversight program in wake of inadvertent disclosure of e-mail addresses) (followed by settlement with eight state attorneys general); *In the Matter of Ziff Davis Media, Inc.*, Assurance of Discontinuance (August 28, 2002) (see *http://www.oag.state.ny.us/press/ 2002/aug/aug28a_02_attach.pdf*) (after erroneous exposure of customers' personal data, entry of assurance of discontinuance with attorneys general of Vermont, New York and California requiring review, monitoring and implementation of measures regarding data privacy, security and integrity, and payment to affected customers).

programs used in a DRM system–that collect or disseminate information about the person's online activities without notice.

It remains to be determined whether the exception in Section 1201(i) will have a meaningful effect on harmonizing privacy concerns and the use of DRMs. Nevertheless, the exception's impact is likely to be quite limited. It only allows for circumvention if the sole effect is to identify and disable the measure–and not to obtain unauthorized access to a work. Further, the exception applies only if the sole purpose of the circumvention is to prevent the collection or dissemination of personally identifying information.

5.2.2 Jurisdiction and Applicable Law

DRMs inevitably will be used to protect and deliver content on a cross-border basis. In doing so, questions might arise as to which jurisdiction's law "applies," both to the protection of the DRM and the underlying content. Choice of law and jurisdictional questions in the online environment, including those that arise with respect to intellectual property agreements, are being addressed in multiple international and regional fora.

Three separate, but related jurisdictional questions are raised with respect to the usage of DRM technologies.

– First, which country's anti-circumvention law would apply to the protection–or to the circumvention or hacking–of DRM technologies?

– Second, which law would apply to the use, or misuse, of content protected by a DRM?

– Third, which national law would apply to the agreements applicable to the delivery of content via DRM?

First, the anti-circumvention and conditional access laws discussed above are territorial in reach. If an act of circumvention, including the act of trafficking in a device, takes place within national boundaries, then the law of that country would apply. The country's jurisdiction could even be exercised over the online distribution into the country of a circumvention program from beyond the national borders, though it may be difficult to get personal jurisdiction over the foreign distributor.

In *United States of America v. Elcom, Ltd.*, discussed in Section 3.2.2, a foreign national and a foreign company were indicted in the United States of America for violating the anti-trafficking provisions of Section 1201(b) when they created and distributed software that decrypted Adobe eBook security software. The court, however, expressly rejected the argument that it was being asked to exercise its jurisdiction on an extraterritorial basis. It found that the defendant had sufficient connections with the United States of America such that the acts alleged occurred within that country: the offending circumvention software was offered and sold via the Internet to U.S.A. residents, the Internet server from which the software was sold was located in the United States of America and the online payment service for the software also was located in the United States of America.[234]

---

[234] *United* States *v. Elcom, Ltd.*, No. CR 01-20138 RMW (N.D. Cal. March 27, 2002) (order denying defendant's motion to dismiss indictment for lack of subject matter jurisdiction).

Second, if a person succeeds in using a copyrighted work other than as permitted by a DRM system, then such use very probably will constitute copyright infringement under the relevant national law. With respect to online access to and use of content, case law and international principles are evolving, both as to the country in which a person may be sued for a multi-jurisdictional infringing act and as to which law should govern. Applicable principles may be drawn from national law and the TRIPS Agreement; work on these matters also is underway in the context of the Draft Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters.[235] In January 2001, WIPO organized a forum on Private International Law and Intellectual Property to review, among various issues, questions of jurisdiction (over the parties and the claim) and choice of law in relationship to works transmitted over digital networks.[236]

Third, which law properly applies to an agreement by which a consumer obtains the delivery of content via a DRM implicates a host of contract and choice of law principles. In general, the law specified in the contract would be applicable. Where the parties have not chosen an applicable law, other principles might be called into play, such as the one set out in the Rome Convention of 1980: the court is to apply the law of the country where the party who is to perform the "characteristic performance" of the contract has his or her residence or its main business establishment.[237]

Further guidance as to the applicable legal principles in the European Community might be found in the Electronic Commerce Directive, which adopts a "country of origin rule." A service provider is subject to the laws of the Member States in which it is established, where establishment includes the place from which it pursues its economic activity or provides its service.[238] In the United States of America, each state has a choice of law principle that would inform a court as to which law ought to apply, in the absence of an agreement between the parties.

5.2.3 Role of Government in Standard Setting and Interoperability

A central question running through the debates over the development and implementation of DRM technologies concerns the appropriate and necessary role for governments or inter-governmental institutions. Most famously, the impetus behind the Consumer Broadband and Digital Television Promotion Act, discussed in Section 3.2.1.4, was

---

235 See *http://www.hcch.net/e/workprog/jdgm.html*.

236 Papers were prepared by Professors André Lucas and Jane C. Ginsburg. See A. Lucas, *Private International Law Aspects of the Protection of Works and of the Subject Matter of Related Rights Transmitted Over Digital Networks*, WIPO Forum on Private International Law and Intellectual Property (WIPO/PIL/01/1 Prov. December 17, 2000); J. Ginsburg, *Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks (2000 Update)*, WIPO Forum on Private International Law and Intellectual Property (WIPO/PIL/01/2 December 18, 2000), both available at *http://www.wipo.int/pil-forum/en/index.html*.

237 Article 4.2, EC Convention on the Law Applicable to Contractual Obligations (Rome 1980) ("it shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporate, its central administration").

238 Recital 19, Electronic Commerce Directive.

the concern of rights holders that the private sector was not moving rapidly enough to solve content protection issues. Supporters of the bill argued that the government should step in where industries could not themselves find technological solutions by a certain date. The European Commission DRM Workshop process discussed in Section 3.3.2 began and concluded with an inquiry into whether the Commission should or must do more to expedite the development of DRM solutions, with a particular emphasis on international standardization and interoperability.

In considering this issue, several observations may be germane. First, whereas rights holders and collective management societies have certainly been more receptive to government involving itself as a last resort, technology industries have fiercely and almost uniformly resisted any suggestion of direct government intervention in standard setting. Indeed, technology companies and most rights holders have acknowledged that voluntary, private-sector led standardization is far preferable to government. Over time, as inter-industry collaboration has increased with respect to DRM development and as work has continued rapidly on addressing such problems as the protection of digital broadcast content, the need for governmental intervention in private sector activities appears to have lessened considerably.

Second, to the extent that the various DRM solutions being adopted at present might be proprietary and not entirely interoperable, the issue has been raised as to whether governments themselves should initiate or motivate the processes of setting standards and ensuring that the technologies migrate toward interoperability. Most private sector interests, be they technology companies or developers of DRM solutions, continue to believe strongly that these matters should be left for industry to address. In their view, market forces and consumer needs are more likely drivers of compatibility and interoperability among DRM systems. Governments, by contrast, are not
well-suited to take an active and leading role in developing market-oriented solutions.

In this respect, however, governments can help in several ways. Most notably, they can continue to provide constructive fora for inter-industry discussions. At these venues, private sector participants can air and document their progress toward solutions and they can use such opportunities to educate others, including public policy-makers. In addition, governments can take a more proactive role by creating legal environments that are conducive to standardization and cooperation. Where governments hope to nurture DRM and other technology industries, as well as to encourage the widespread use of DRM technologies, they may wish to consider recognizing the importance of DRM technologies in both their competition law statutes and in their approaches to enforcing competition laws.

Third, most of the major private sector participants recognize that there is some role for government in ensuring and enforcing compliance with solutions that are agreed upon by private sector participants. The example of the WIPO Treaties and the legislation implementing those treaties demonstrates that laws adopted by governments are necessary to safeguard technological protections. Statutory antecedents outlawing hacking of conditional access systems are much in the same vein. Private sector actions and agreements between private parties are very limited in being able to find and punish those persons who seek to benefit from having access to content for which they do not pay. Laws are essential to ensure that everyone–individuals and product manufacturers alike–is playing by the same content protection rules. In this regard, the FCC broadcast flag rulemaking is an example of an appropriate role for government, the role of mandating compliance with industry-agreed solutions.

Fourth, the power of governments to issue mandates and then ensure compliance is necessarily limited by their sovereign authority. Even the institutions of the European Union, which are empowered to develop and enforce legal standards for multiple Member States, have no authority outside their borders. But, as the WIPO Treaties evidence, the need for a harmonized approach to content protection technologies, including DRM systems, is obvious. Section 3.2.1.3(b) notes, by way of example, that it might do rights holders little good for their over-the-air digital broadcast content to be technologically and legally protected from redistribution in one country if the same television signal can be received off the air in an adjoining country and then redistributed with impunity and without hindrance. Consequently, an important ongoing task for governments is to consider how they can cooperate meaningfully to facilitate a seamless approach to protecting both content and associated DRM systems.

5.2.4 Technology Licensing Practices and Obligations

Integrally related to the question of government's role in setting standards are the business practices and associated laws for licensing DRMs and, more generally, technology standards. DRM technologies and standards may be protected or governed by patent, copyright and trade secret laws.

Standards are often classified as being either "open" or "proprietary." "Open" standards may be those developed in the context of a broad-based, open body in which any interested party may participate, subject to the rules of the forum. Internationally, the ITU and the International Electrotechnical Commission are examples of "open" standard setting bodies. At the European level, the European Telecommunications Standards Institute is an example of such a body. National bodies include such organizations as the American National Standards Institute in the United States of America and the Japan Electronics and Information Technology Industries Association in Japan.

"Proprietary" standards are developed and the technologies are licensed by individual companies or groups of companies that hold applicable intellectual property rights. Specific DRM technologies, including several of those discussed above, are the product of individual or joint development activities and are being licensed on a proprietary, royalty-bearing basis.

Licensing of technologies that are included in standards established through open processes as well as those embedded in proprietary systems is governed by legal requirements. To ensure that standards are not adopted without an understanding of the patent rights that may govern, participants in a voluntary open "due process" standard setting body usually must agree that they will notify other participants if they have intellectual property rights in a proposed standard and, further, that they will license such rights on reasonable and non-discriminatory terms.[239] In the United States of America, the Federal Trade Commission

---

[239] See, *e.g.*, ETSI Intellectual Property Rights Policy (April 2003) (requiring participants to notify others of essential clams; to request that licenses be made available on reasonable and non-discriminatory terms; to seek alternatives if they are not made available on such terms; and to publish notified claims of intellectual property rights with the standard adopted), available at *http://portal.etsi.org/directives /directives_apr_2003.doc*; ANSI Essential Requirements: Due process requirements for American National Standards, Section 3.1 (March 2003) (participants

[Footnote continued on next page]

charged that it was an unfair practice for a participant in an open standard setting body to fail to disclose that it had essential patent claims until after the body had adopted a standard and resolved the matter with an order prohibiting the patentee from enforcing its patent claims against implementers of the standard.[240]

Some bodies go further and attempt to insist that any essential patent claims will be licensed on a royalty-free basis. In May 2003, for example, W3C issued a patent policy to ensure that its recommendations can be implemented on a royalty-free basis.[241] W3C attempts to ensure that it will not adopt a recommendation if a participant has essential patent claims that it will not license without charging a royalty.

Proprietary technologies (whether based on open standards or not) are made available through negotiated license agreements, which typically include matters such as royalties, scope of use, rights to future development and the like. Certain of the copy protection technologies, particularly many of those developed by hardware companies, are generally licensed on a close to "at-cost" basis, with administrative costs covered by the fees charged.

Both with respect to open and proprietary standards, licenses to DRM standards and technologies must comply with applicable law, including the competition laws of the various jurisdictions into which the intellectual property is licensed. Competition law is relevant because intellectual property laws confer exclusive rights on the owner of the intellectual property and because it is important to prevent abusive or unlawful licensing practices. Various major jurisdictions have established guidelines or regulations governing the intersection of intellectual property and technology licensing agreements,[242] with applicable laws also being fleshed out by judicial decisions.

[Footnote continued from previous page]

must avow that they do not hold any intellectual property or that, if they do, they will license on a royalty-free basis or on the basis of reasonable terms and conditions that are "demonstrably free of any unfair discrimination"), available at *http://public.ansi.org/* ansionline/Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/ER2003.doc.

240 *In the Matter of Dell Computer Corp.*, Decision and Order, No. C-3658 (May 20, 1996), release available at *http://www.ftc.gov/opa/1995/11/dell.htm*.

241 See W3C Patent Policy (May 20, 2003), available at *http://www.w3.org/ Consortium/Patent-Policy-20030520.html*.

242 See, e.g., U.S.A. Department of Justice and Federal Trade Commission, Antitrust Guidelines for the Licensing of Intellectual Property (April 6, 1995), available at *http://www.usdoj.gov/atr/public/guidelines/ipguide.htm*; European Commission Regulation (EC) No. 240/96 of 31 January 1996 on the application of Article 85 (3) of the Treaty to certain categories of technology transfer agreements, Official Journal L 031 , 09/02/1996; Japan Fair Trade Commission, Guidelines for Patent and Know-How Licensing Agreements Under the Antimonopoly Act (July 30, 1999), available at *http://www2.jftc.go.jp/e-page/guideli/patent99.htm*; Canada Competition Bureau, Intellectual Property Enforcement Guidelines (released September 21, 2000), available at *http://strategis.ic.gc.ca/SSG/ct01992e.html*.

5.3 Policy Issues: The Role of WIPO and other international organizations

In light of the business, technical and legal developments and the policy issues discussed above, the authors have considered possible actions or initiatives that WIPO and other international organizations might take, as appropriate, to promote effective implementation of the DRM-related provisions of the WIPO Internet Treaties. Consistent with WIPO's mandate "to promote the protection of intellectual property throughout the world,"[243] the authors suggest that WIPO consider the following recommendations.

5.3.1 Varying Approaches to Implementation of the WIPO Internet Treaties

Sections 3 and 5.1.1 describe several of the variant approaches that national governments and the European Union have taken to implement their obligations under the WIPO Internet Treaties. As noted above, implementing legislation to date has varied somewhat.

Recommendation One:

WIPO might undertake a comprehensive study of the different approaches available to implementing the WIPO Internet Treaty obligations. The study could summarize the choices that have been made by legislators and examine the likely effects of these different approaches on the scope and extent of legal protection for DRMs and content delivered through DRM solutions.

5.3.2 Use of DRMs and Access to Content

During the course of ongoing national and European-wide debate over the implementation of the WIPO Treaties, among the most intensely discussed set of issues is whether DRMs and their legal underpinnings will restrict legitimate consumer access to content. Concern as to whether works will be "locked up" and fears with respect to a rapidly approaching "pay-per-use" society are widespread, including in the jurisdictions that have yet to implement the WIPO Treaties and the Copyright Directive.

As noted above, both the United States of America and the European Commission have built in some regulatory and governmental mechanisms to evaluate whether and to what extent access controls are actually impairing certain uses which, though not expressly authorized by rights holders, are seen as legitimate and appropriate "fair uses" or "exceptions" to copyright. These mechanisms include periodic review by the U.S.A. Copyright Office, and periodic reports and monitoring and reviews by the European Commission. Nevertheless, consumer, library, archival and educational organizations have expressed concerns about whether the breadth and authority of these processes are adequate to make adjustments that might be needed on a timely basis.

Aside from periodic monitoring activities of the European Commission, there are no proposals to examine in any systematic way the present and future effects of access controls

[243] Convention Establishing the World Intellectual Property Organization, Art. 3(i).

on consumers. To date, however, and with limited exceptions (such as with respect to CSS and DVD disks), technological measures appear not to have had a significant effect on lawful users' right of access to copyrighted works. Over time, this may (or may not) change, depending on how DRMs are deployed by rights holders. The full impact of these effects may not yet be understood or assessed given the constrained nature of the processes that have been put in place.

Recommendation Two:

On a periodic basis, WIPO might undertake to collect data or otherwise review the extent to which DRMs are being deployed and the effect of technological measures on legitimate access to copyrighted works. The review would not necessarily duplicate the national and European-wide mechanisms that have been adopted: It could be more open-ended in scope and could more comprehensively survey the situation at the international level.

5.3.3 Statutory Exceptions or Limitations to Anti-Circumvention Provisions

The WIPO Treaties are silent on the issue of whether implementation requires–or limits–the adoption of any exceptions or limitations in connection with obligations to ensure that there exists "adequate legal protection" and "effective legal remedies" against abuse of technological measures. Nevertheless, as the preceding discussion highlights, implementing legislation has tended to include certain exceptions or limitations. These vary quite a bit, reflecting different policy preferences and the influence of different interest groups on the legislative process.

Some of these exceptions and limitations have been express, others implicit. Some have been in binding language, others in recitals or accompanying commentary. Some are exceptions that apply only to users–such as for certain types of reproduction or private copying. Others apply only to particular types of activities–such as reverse engineering and computer testing. Still other exceptions or limitations are applicable only to products and devices, such as the "no mandate" provisions (for legitimate consumer electronics, computer and telecommunications products) and the provisions relating to distribution of means for ensuring interoperability between computer programs.

In the final analysis, at the international and regional levels there is no uniformity or harmonization among the exceptions or limitations. Two sets of consequences may result. First, at least to a limited extent, consumers of content that is identical (and as to which the rights holders are identical) and that is protected by identical DRMs may have different legal abilities to access and use that content free from the anti-circumvention laws–depending on whether they fall within an applicable exception or limitation that is available in the country in which they live.

Second, the exceptions and limitations applicable to circumventing acts and tools obviously have an effect on the extent to which DRMs can protect content. In the future, as and when DRMs are deployed, if these exceptions and limitations are invoked by users and manufacturers of consumer electronics and computing products, those effects may well need to be better understood internationally. By way of example, once a person accesses content or uses it (notwithstanding a DRM) based on undertaking a lawful act of circumvention in one

country, then that content could be made available to users more broadly by ready distribution over the Internet or otherwise.

Similarly, a product or computer program that is capable of circumventing a technological measure may be lawful in one country because, for example, it has legitimate purposes other than circumvention and because that country's laws only prohibit products that have, as their sole purpose or function, circumvention. Yet, once that product is used in that country to access content that is protected by technological measures, the content is no longer protected in that country and, then being potentially subject to global redistribution, might be subject to unauthorized uses elsewhere as well.

This discussion suggests that exceptions and limitations be drafted carefully. It is vitally important that only certain legitimate activities be defined to fall within the exceptions. Guidance on how best to craft exceptions and limitations may be useful, not only to reflect legitimate needs for access and use but also to address equally legitimate concerns of rights holders about the threat posed by content that (by virtue of an exception) escapes DRM-based protections.

Recommendation Three:

As rights holders increase their usage of DRMs, the exceptions or limitations adopted by jurisdictions in implementing the anti-circumvention provisions may rise to greater prominence. WIPO could examine the international effects of disparities in these exceptions or limitations on 1) persons who seek to make lawful use of copyrighted works by invoking the exceptions and limitations, 2) manufacturers of legitimate products and 3) rights holders.

5.3.4 Modification of Private-Copying Levies in the Transition to DRMs

As noted in Section 5.1.3, several jurisdictions have in place schemes that impose levies on devices and media in respect of private copying. Over several years, discussions have centered around the questions of 1) whether there should be levies, 2) if so, on which products they should be imposed, 3) the amount of the levy and 4) to whom the levy should be paid. As the discussion with respect to the European Union makes clear, with the evolution of the digital environment, the potential expansion of levy schemes to include digital devices and media, particularly those that are multi-functional, has given rise to equity concerns from consumers and the technology industries. In particular, they have argued that consumers should not have to pay twice–once through a levy on a digital device and/or media–and once through a conditional access scheme facilitated by a DRM–for a single use of content. Conversely, it has been pointed out, where levies are maintained and expanded, there may in fact be less incentive to develop and adopt DRM solutions.

Recommendation Four:

WIPO, could assess the effect of the various private-copying levy schemes in light of the eventual widespread adoption of DRM technologies in the global digital economy. In Europe, it has been urged that the European Commission assist Member States in determining when and how to modify levies during the transition to a DRM-controlled environment. WIPO could play a neutral role in convening experts to share information to enhance the collective international understanding of the relationship between levies and DRMs. Such a process could be useful in assessing the timing of, and developing the mechanisms for making a modification, as and when appropriate.

[End of document]