Technological Protection Systems for Digitized Copyrighted Works: A Report to Congress

I. INTRODUCTION

A. Background

On November 2, 2002, the President signed into law the "Technology, Education and Copyright Harmonization Act of 2002" (the TEACH Act), which updates certain provisions of the Copyright Act to facilitate the growth and development of distance education, while introducing new safeguards to limit the additional risks to copyright owners that are inherent in exploiting works in a digital format.[1] For information purposes only, the TEACH Act requires the United States Patent and Trademark Office (USPTO), after consultation with the Register of Copyrights, to submit a report to Congress on technological protection systems to protect digitized copyrighted works and to prevent infringement, including those being developed in private, voluntary, industry-led entities through an open broad-based consensus process.

Over the last several years, the educational opportunities and risks associated with distance education have been the subject of extensive public debate and attention in the United States. In November 1998, the Conference on Fair Use (CONFU), convened by the Administration's Information Infrastructure Task Force, issued its final report, which included a proposal for educational fair use guidelines for distance learning.[2] Following the enactment of the Digital Millennium Copyright Act of 1998 (DMCA),[3] the Copyright Office was tasked with preparing a study of the complex issues involved in distance education and to make recommendations to Congress for any legislative changes. In May 1999, the Copyright Office issued an extensive report on copyright and digital distance education.[4] After hearings before the Senate Judiciary Committee (March 13, 2001) and before the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property (June 27, 2001), Congress passed the TEACH Act as part of the "21st Century Department of Justice Appropriations Authorization Act."

[1] Pub. L. No. 107-273, 116 Stat. 1758 (Nov. 2, 2002).

[2] *See* The Conference on Fair Use: Final Report to the Commissioner on the Conclusion of the Conference on Fair Use (U.S. Patent and Trademark Office, November 1998). The report is available at: http://www.uspto.gov/web/offices/dcom/olia/confu/confurep.htm.

[3] Pub. L. No. 105-304, 1122 Stat. 2860 (Oct. 28, 1998).

[4] *See* Report on Copyright and Digital Distance Education: A Report of the Register of Copyrights (U.S. Copyright Office, May 1999). The report is available at: http://www.copyright.gov/disted.

B. Overview of the TEACH Act

Subsection (b) of the TEACH Act amends section 110(2) of the Copyright Act to allow for the inclusion of performances and displays of copyrighted works in digital distance education under appropriate circumstances and subject to certain limitations. The Act expands the categories of works exempt from the performance right in section 106(4) of the Copyright Act, from nondramatic literary works and musical works to "reasonable and limited portions" of any work and permits the display of any work in "an amount comparable to that typically displayed in the course of a live classroom setting." The Act removes the concept of the physical classroom, while maintaining the requirement of "mediated instructional activity," which generally requires the involvement of an instructor. The exemption is limited to mediated instructional activities that are conducted by governmental bodies and "accredited" non-profit educational institutions. Subsection (c) of the TEACH Act amends section 112 of the Copyright Act to permit transmitting organizations to store copyrighted material on their servers in order to allow the performances and displays of works authorized under amended section 110(2).

The TEACH Act contains a number of new safeguards to limit the additional risks to copyright owners that are inherent in using works in the digital format. The Act limits the receipt of authorized transmissions to students officially enrolled in the course or to Government employees as part of their official duties "to the extent technologically feasible." With respect to "digital transmissions," transmitting institutions must apply technological measures that reasonably prevent "retention of the work in accessible form by recipients of the transmission … for longer than the class session" and "unauthorized further dissemination of the work in accessible form by such recipients to others." The statute also prohibits transmitting institutions from engaging in "conduct that could reasonably be expected to interfere" with technological measures used by copyright owners to regulate the retention and further unauthorized dissemination of protected works.

C. The USPTO Report

Subsection (d) of the TEACH Act requires the Under Secretary of Commerce for Intellectual Property, after consultation with the Register of Copyrights, and after a period for public comment, to submit to the Committees on the Judiciary of the Senate and the House of Representatives a report on technological protection systems to protect digitized copyrighted works, including those being developed in private voluntary industry-led entities through an open broad-based consensus process. The report, which is intended solely to provide information to Congress, is due not later than 180 days after the date of enactment of the Act.

Congress specifically directed the USPTO to include information "on technological protection systems that have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including upgradeable and self-repairing systems, and systems that have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad based consensus process." Congress also directed the USPTO to exclude "any recommendations, comparisons, or comparative assessments of any commercially available products that may be mentioned in the report."

Subsection (d) of the Act further states that the report "shall not be construed to affect in any way, either directly or by implication, any provision" of the Copyright Act in general or the TEACH Act in particular, including the requirement of transmitting institutions to apply certain technological controls and not to engage in conduct that could be reasonably expected to interfere with technological measures used by copyright owners (discussed more fully above), or "the interpretation or application of such provisions, including evaluation of the compliance with that clause by any governmental body or nonprofit educational institution."

Finally, the legislative history of the TEACH Act sheds some light on the purpose, benefits and possible limitations of the USPTO report. Some lawmakers noted that a report on technological protection systems would "only provide a snapshot in time," while others noted that such a report would be "out of date by the time it is finished due to continual advances in technology."[5] In preparing this study, USPTO became well aware of these inherent difficulties. Nonetheless, Congress also noted that such a study could be "useful in establishing a baseline of knowledge for the Committee and our constituents with regard to what technology is or could be made available and how it is or could be implemented."[6] In that spirit, this report is respectfully submitted to Congress.

D. Public Comments and Public Hearing

Under the TEACH Act mandate, and to assist in the preparation of the report, on December 4, 2002, USPTO solicited written comments from interested parties and scheduled a public hearing on February 4, 2003.[7] Written comments were due January 14, 2003. In particular, USPTO requested information in response to the following questions:

(1) What technological protection systems have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems?

(2) What systems have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process?

[5] Congr. Rec. S5991 (June 7, 2001).
[6] Id.
[7] 67 Fed. Reg. 72,920.

(3) Consistent with the types of information requested by Congress, please provide any additional comments on technological protection systems to protect digitized copyrighted works and prevent infringement.

In response to these questions, USPTO received written comments from the following organizations: Infraworks Corporation; Blue Spike, Inc; Macrovision Corporatio n; OverDrive, Inc.; ContentGuard; Copyright Clearance Center, Inc.; NDS Americas, Inc.; 4C Entity, LLC; Protexis, Inc.; Association of American Universities; The Walt Disney Company; Digimarc; Motion Picture Association of America, Inc.; Software & Information Industry Association; Digital Transmission Licensing Administrator, LLC; and Information Technology Industry Council. Copies of the public comments are available on the USPTO web site at http://www.uspto.gov.

On February 4, 2003, USPTO conducted a public hearing to assist in the preparation of the TEACH Report. The following persons testified: Mr. William Krepick, President and Chief Executive Officer, Macrovision Corporation; Mr. Steven Potash, Chief Executive Officer, OverDrive, Inc.; Mr. Michael Miron, Chief Executive Officer, ContentGuard; Mr. Troy Dow, Vice President & Counsel, Technology & New Media, Motion Picture Association of America, Inc.; Mr. Bruce Funkhouser, Vice President of International and Business Operations, Copyright Clearance Center, Inc.; and Mr. Mark Bohannon, General Counsel and Executive Vice President, Government Affairs, Software & Information Industry Association. A transcript of the hearing is available on the USPTO web site at http://www.uspto.gov.

II. TECHNOLOGICAL PROTECTION SYSTEMS

A. Introduction

The 1996 World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) (collectively the WIPO Treaties) require signatories to provide "adequate legal protection and effective legal remedies against the circumvention of effective technological measures."[8] The U.S. legislation implementing the WIPO Treaties, the 1998 Digital Millennium Copyright Act (DMCA),[9] generally divides technological measures into measures that prevent unauthorized *access* to a copyrighted work and measures that prevent infringement of a work. Although the term technological protection system is not defined in the TEACH Act or in the DMCA, it is generally used in this report to refer to a range of technological methods to control unauthorized access to and copying of digitized

[8] WIPO Copyright Treaty ("WCT"), Article 11, adopted December 20, 1996, WIPO Doc. CRNR/DC/94; WIPO Performances and Phonograms Treaty ("WPPT'), Article 18, adopted December 20, 1996, WIPO Doc. CRNR/DC/95; Agreed Statements Concerning the WIPO Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/96. The Treaties also require adequate legal protection and effective legal remedies for the protection of the integrity of copyright management information. WCT, Art. 12; WPPT, Art. 19.

[9] Pub. L. No. 105-304.

copyrighted works. This section briefly introduces some of the core technologies that underlie such technological protection systems.[10]

B. Core Technologies

1. Encryption

Encryption is a process that "scrambles" data using sophisticated mathematical equations in order to protect it and keep it private. In very general terms, encryption algorithms convert human readable data, such as a word processor document, into encrypted or scrambled data. The encrypted data can be made readable again by decrypting it with a corresponding decryption key. If the decryption key is given only to authorized parties and if the encryption algorithm used is sufficiently strong, unauthorized access to the data by the casual user is prevented. The whole point of encryption is that an encrypted work cannot easily be manipulated without authorization. A secret key or pair of keys, as discussed more fully below, is required for the encryption or decryption of the scrambled file. Encryption technology can be used to protect data and works transmitted over computer networks (such as e-mail and database information), or more broadly in connection with other information delivery systems, including telephone, satellite and cable communications.

Broadly speaking, encryption algorithms may be characterized either as "secret key" encryption (sometimes called "symmetric key" encryption) and "public key" encryption (or, "asymmetric key" encryption). Secret key encryption involves the use of a single key to encrypt and to decrypt the content. A common example of the use of secret key encryption to control access to content is pay-per-view television. In this illustration, the television program is encrypted using the secret key, and only paying customers have access to the secret key. Of course, as its name suggests, the successful application of secret key encryption to protect copyrighted works depends on keeping the key secret. Wide distribution of the secret key to numerous parties may result in compromising such a technological protection system. Thus, public key encryption, as explained below, is generally used as for distribution of content to a wide audience.

Public key encryption uses an algorithm requiring two keys – a "public" key and a "private" key. The data is encrypted using the public key, which is then made widely available to the public. The private key is kept secret by individuals. The fundamental point is that the encrypted content or secret message can only be decrypted using the corresponding private key. For example, a copyright owner could encrypt a work using the public key of the intended recipient. Once the recipient receives the encrypted transmission, he or she could use the private key to decrypt the transmission. No private keys need to be exchanged in this transaction. Without the private key of the intended

[10] For an earlier introduction to these technologies, *see* Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (1995). For a more recent survey of these technologies, s*ee* "Protecting Digital Intellectual Property," Chapter 5, in Committee on Intellectual Property Rights and the Emerging Information Infrastructure, National Research Council, Computer Science and Technology Board, *The Digital Dilemma: Intellectual Property in the Information Age* (1999).

recipient, the work cannot be read, manipulated or otherwise deciphered easily by casual users.

The Content Scrambling System (CSS) illustrates how encryption technology is integrated into a technological protection system. First, using CSS, digital audiovisual content (including the keys that enable a DVD player to access that content) is encrypted on a DVD disk. Second, only DVD players licensed by the DVD Copy Control Association (DVD CCA), a private industry-led non-profit organization that is discussed later in this report, may decrypt the encrypted content. Third, under DVD CCA's license requirements, licensed players must, among other things, protect against copying, protect against disclosure of the decryption keys, and not pass the content over unprotected digital outputs.

2. Digital Watermarking

Although encryption is an important tool to control access to and transmission of content, encryption alone does not solve all digital copy protection and prevention problems. At the receiver's end, for example, decrypted content is subject to unauthorized use, manipulation and further distribution. One approach to addressing this problem is to directly embed control information into the media itself, a process commonly referred to as "digital watermarking."[11] Originally, digital watermarking was the term used only for techniques to embed copyright markings (the "originator's mark") into a digitized work. The term "fingerprinting" generally is used for watermarking techniques that reveal the identity of the recipient of the protected content (the "recipient's mark"). More broadly, digital watermarking today refers to any technology aimed at concealing data in media content.

In its basic form, a digital watermark contains information about the origin, status or destination of the host data. A digital watermark may be embedded in almost any kind of digitized visual or audio data, including broadcast data, without perceptibly degrading or interfering with its quality.[12] The hidden information cannot be removed from the associated data without introducing perceptible distortions or significantly reducing data quality. Thus, digital watermarks can be an important mechanism for content owners to monitor, audit, and index works in the digital environment. Digital watermarks also can be used to identify the source and destination of data, thereby providing rights owners with a useful tool to authenticate content when copyright infringement is suspected. Finally, digital watermarks can be used to detect the unauthorized manipulation of content, thereby providing a means to control the integrity of digital content.

[11] For a comprehensive treatment of the subject, see Ingemar Cox, Jeffrey Bloom, and Mathew Miller, *Digital Watermarking Principles & Practice* (Morgan, Kaufman 2001). *See also* Christophe de Vleeschouwer, Jean-Francois Delaigle, and Benoit Macq, "Invisibility and Application Functionalities in Perceptual Watermarking—An Overview," 90 Proceedings of the IEEE (January 2002).

[12] Digital watermarks may be either "perceptible" (to humans) or "imperceptible." A "fragile" watermark becomes undetectable even after minor modifications of the work in which it is embedded. A "robust" watermark is capable of surviving manipulations over its lifetime such as compression, image processing, or printing/scanning. A "semi-fragile" watermark is fragile against certain distortions and robust against others.

Digital watermarking technology can be integrated into technological protection systems in a variety of ways. They potentially can be used to recognize and screen out music watermarked as "no copy." Digital watermarks also can be used in connection with copy and playback controls in playback devices such as DVD players. DVD players employing the Content Scrambling System (CSS) search for watermarks in a motion picture on a recordable DVD, refusing to play back a disk that does not include the required watermarks.

3. Authentication

Technologies used to identify devices and authenticate the identity of users are important elements of modern technological protection systems. One method to control user access to protected resources in a centralized network is through the use of IP (Internet Protocol) addresses, commonly referred to as "IP authentication." To facilitate access to protect content from off-site locations, however, a resource provider may need to provide password accounts to users. User information (such as user names and passwords) also may be stored in a cookie, a text string or small file that is placed on an end user's hard drive. The use of digital certificates is another tool to authenticate the identity of users. Under this approach, a certificate authority (CA) issues a personal digital certificate, which contains the name of the owner of the certificate, the owner's public key, the expiration of the public key, the name of the certificate issuer, the serial number of the certificate, and the digital signature of the certificate issuer.

Technologies to authenticate the integrity and source of digital content are also important components of technological protection systems. As it has become easier and easier to tamper with digital works without detection, techniques to ensure the integrity of digital content have become more important. For example, a publisher of a medical text may depend on content authentication techniques to ensure that textual data (such as dosage amounts) or visual data (such as medical illustration) have not been altered. One common cryptographic solution to the problem is the use of digital signatures, a technique that authenticates both the contents of a message and the person who signed it. Digital signatures may be transmitted along with the work as "metadata" (encoded identifying information about the content, discussed more fully below) or embedded directly into the work as watermarks. More broadly, encryption technology may be used to authenticate the integrity of license terms and conditions associated with copyrighted digitized work.

C. Digital Rights Management (DRM) Systems

Today advances in technology (both hardware and software) permit content owners to assert much finer-grained control over digital media embodying copyrighted works, authenticating users and the integrity of content, and developing new business models for digital content in addition to simply deterring piracy. The general term Digital Rights Management (DRM) is commonly used to refer to technologies or systems used to achieve these objectives.[13] Although there is no generally accepted definition for DRM,[14] such technological protection systems typically incorporate the following controls or functions: access controls, use controls, and tracking functions. For purposes of this report, the term DRM is used to refer to a broad range of technical, legal and business issues pertaining to copyright management and control of works in a digital format. This section briefly introduces some of the key concepts and elements underlying DRM systems and technologies.

1. Trusted Computing

A trusted computer system combines hardware and software (meeting certain security specifications approved by the content provider) to create a secure trusted platform for the exchange of digital content and information. The conceptual underpinnings of trusted computing technologies trace back to Dr. Mark Stefik's pioneering work at Xerox PARC.[15] In very general terms, Stefik defined a trusted system as a system that can be relied on to follow certain rules. In the DRM context, a trusted system is a computer (or other device) that can be relied on to follow and enforce rules governing the access and use of protected digital content. The server relies on "trusted" elements of the recipient's device to identify the recipient, to transmit only accurate information about the recipient, and to limit the recipient's ability to manipulate any content it receives from the server in ways that exceed its authorization.

2. Rights Models and Rights Expression Languages

Rights models and rights expression languages are two mechanisms that can be used to facilitate transactions involving copyrighted works in the digital environment. In broad outline, a rights model specifies the types of rights, types of users, extent of rights, and associated costs. The rights model may specify such rights types as print, view, or play. Examples of users that can be specified in a rights model include subscribers, enrolled students, or site licensees. The extent of rights may be specified either as a period of time or number of times (for example, print 5 times, view for 10 days, or play for 48 hours). The rights model also expresses costs associated with the exercise of specific rights. In practice, the rights model is implemented through a "rights expression language" (REL), which defines a structure for expressing permissions in machine (and human readable form) and a "rights data dictionary," which precisely defines the meaning of the permissions and conditions expressed. An example of a modern REL is Extensible Rights Markup Language (XrML), which is discussed later in this report.

[13] For a very useful introduction to DRM technologies and systems, *see* Bill Rosenblatt, Bill Trippe, and Stephen Money, *Digital Rights Management: Business and Technology* (New York: M&T Books, 2002)

[14] One commentator broadly defined DRM systems as "technology systems facilitating the trusted and dynamic management of rights in any kind of digital information, throughout its life cycle, irrespective of how and where the digital information is distributed." *See* N. Garnett, "Outline of Presentation of Nic Garnett, representing InterTrust Technologies," ALAI Congress 2001.

[15] *See generally* Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication," in *Internet Dreams: Archetypes, Myths, and Metaphors* (MIT Press, 1996). *See also* Stefik "Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing" 12 Berkeley Tech. L. J. 137 (1997).

Electronic rights transactions also require the unique identification of each item of digital content. Such encoded information about a digital work (such as author, title, date of creation, and other identifying information) is commonly referred to as "metadata."

3. DRM Architecture

Although DRM systems vary widely depending on their purpose and function, the overall architecture of a DRM consists of three major components.[16] First, the "content server" consists of the actual digital content, along with information about the products and/or services that the content provider wants to distribute digitally after secure packaging. The content server typically includes a "content repository," a file server or a database that holds the content, along with associated metadata. The content server also usually includes a "DRM packager," which is used to prepare the content for secure distribution (for example, by encrypting the content and/or inserting metadata), create specifications of rights associated with content, and create encryption keys to authenticate users and decrypt content, before passing the information along to the license server.

Second, the "license server" contains information that identifies the digital content, specifies the rights associated with that content (for example, "play" or "copy"), and establishes the terms and conditions for the exercise of those rights (such as an expiration date), whether by a user or a device.[17] Third, on the "client" side of a DRM, the "DRM controller" receives the user's request to exercise rights with respect to specific content, gathers information about the identity of the user, obtains a license from the license server, authenticates the application that performs the rights exercise, retrieves the encryption keys, decrypts the content for the appropriate "rendering" application (such as playing a song or viewing a movie).

4. Types of DRM Systems

A wide range of DRM options are available in the marketplace today, probably reflecting the fact that no single technology or solution can fulfill the remarkably diverse requirements of the digital marketplace. In broad outline, DRM systems may be hardware-based, software-based, or hybrid systems combining software and hardware elements. Hardware-based DRM solutions embed the technological protection in the hardware itself. Examples of hardware-based DRM systems are DirecTV, smartcards and many conditional access systems, which are used in a variety of delivery systems, including direct broadcast satellite, digital cable television, and digital terrestrial television.

Software-based DRM technologies have been and are being developed to provide for secure delivery of content over the Internet and adherence to copy control instructions and usage rules in the PC and home-network environments. Many companies have

[16] This section relies on Rosenblatt and others, *Digital Rights Management* (n. 13 above).

[17] Digital content protection technologies help support a variety of "copy control states," including "copy never" (used in pay-per-view, video-on-demand, and pre-recorded media), "copy once" (used in pay TV and basic and extended cable), and copy control not asserted, but no redistribution (free-to-air TV).

developed such software-based DRM solutions, including ContentGuard, Intertrust Technologies, Liquid Audio, Microsoft, and Real Networks, which are discussed in the next section. A number of these products (such as Microsoft's "Windows Media Rights Manager") include a built-in renewability feature, which enables the content owner to respond quickly to security breaches by renewing the protections that apply to all other copies of the content. Finally, the CSS system, discussed above, is an example of hybrid DRM solution, using CSS-enabled DVD players to inspect DVDs for embedded code.

III. COMPANIES AND PRODUCTS

A. Introduction

Based on public comments submitted to the USPTO, the agency compiled a list of more than 100 companies that have developed, are proposing to develop, or offering technological protection systems (including components thereof) to protect digitized copyrighted works and prevent infringement. A complete list of these companies is attached as Appendix A to this report. Many companies are constantly entering (and leaving) the rapidly evolving market for technological protection systems. Thus, as Congress itself recognized, any attempt to report on developments in this changing arena will "only provide a snapshot in time" because of the continual advances in technology.[18]

Solely to provide information requested by Congress, this section of the report briefly discusses selected technological protection systems that are under development or currently available in the marketplace. All descriptions of commercially available products in this section are distilled from information that is made publicly available by the companies. The USPTO has not conducted an independent analysis of these products and services and makes no recommendations, comparisons, or comparative assessments of the technological protection systems discussed in this section or included in the list attached to this report as Appendix A. Almost all the products and services discussed in this section are registered trademarks.

B. Companies and Products

Adobe Systems, Inc.

Adobe Systems is a provider of graphic design, publishing, and imaging software for web and print production. Adobe offers a line of software products for managing information of all types. The Adobe Portable Document Format (PDF) is a format for secure and reliable electronic files. Adobe Acrobat software enables users to create PDF files, which prevent unauthorized viewing of documents. The "Adobe Acrobat eBook Reader" is software that displays Adobe PDF-based eBooks on notebook and desktop computers. The "Adobe Content Server" is a system that allows publishers, distributors, retailers, and individual authors to prepare, secure, and license eBooks in Adobe PDF directly from their web sites. More information on Adobe Systems and its products is available at: http://www.adobe.com.

[18] Congr. Rec. S5991 (June 7, 2001).

Aladdin Knowledge Systems, Ltd.

Aladdin Knowledge Systems offers products used to manage network security, including applications for managing content and guarding against computer viruses. Aladdin's products are incorporated into virtual private networks, intranets, and extranets. Aladdin also offers software protection systems that enable software developers to securely distribute and manage software licenses and other electronic content. Aladdin's products include: “HASP and Hardlock,” hardware-based software security systems; “Privilege” software commerce solutions, “eToken,” a powerful two-factor authentication USB device and the “eSafe” suite of anti-virus and content security solutions. More information on Aladdin Knowledge Systems and its products is available at: http://www.ealaddin.com.

Alchemedia

Alchemedia is a supplier of security software, focusing on the needs of customers in the pharmaceutical, biotechnology, high technology, and manufacturing sectors. Alchemedia’s “Mirage Enterprises,” which is comprised of the “Mirage Server” and the “Mirage Client,” enables users to view and collaborate on documents in a secure environment. The Mirage Server is software (installed on web servers) that flags documents for protection by encoding policy limits and/or enciphering the data. The Mirage Client is software that decrypts data sent to it by the Mirage Server and enforces limitations on what authorized users can do with the data. More information on Alchemedia and its products is available at: http://www.alchemedia.com.

Alpha-Tec, Ltd.

Alpha-Tec is a research and development company providing digital image and video processing software, including watermarking products for images, video, audio, and 3D graphics. More information on Alpha-Tec and its products is available at: http://www.alphatec.com.

AlpVision

AlpVision provides digital watermarking, image processing, security products, and other services. AlpVision’s video watermarking technology, which is applicable to digital and analog video, can be used for tracking, fingerprinting, and copyright infringement detection. AlpVision’s “Signit!” is digital image processing software used to embed and retrieve registration numbers from signed images. AlpVision’s “LabelIt!” is an application that can be used to embed a string of 20 characters in a scanned image. The Company’s “CD-Check” application provides secure access to CD-ROMs. More information on AlpVision and its products is available at: http://www.alpvision.com.

Authentica, Inc.

Authentica is a provider of DRM technology for electronic documents, web pages, and e-mail. Authentica's products include "PageRecall" (for electronic documents, "NetRecall" (for web content), and "MailRecall" (for e-mail). The Company's products are built around Authentica's patented "Active Rights Management" technology, which combines content security and DRM technology within its client-server architecture. Authentica's "Content Security Server," is a web application for securely distributing and controlling e-mail and attachments. More information on Authentica and its products is available at: http://www.authentica.com.

CenterSpan Communications Corporation

CenterSpan Communications develops and markets secure software-based Internet and intranet content delivery solutions for media and communications service providers and corporate customers. CenterSpan's "C-StarOne" is a content delivery solution designed for delivering large files such as digital audio, video, executables, and data files. The C-StarOne service is capable of supporting a variety of DRM technologies that enable content owners to set their own "usage rules" for copyrighted materials. Value-added services complementary to C-StarOne delivery include content preparation, publishing, security, and data analysis. More information on CenterSpan Communications and its products and services is available at: http://www.centerspan.com.

Certicom Corporation

Certicom Corporation is an encryption technology company specializing in security solutions for mobile computing and wireless data markets, including mobile e-commerce. Certicom's "movianDM" provides centralized policy management for secure mobile devices, which can be used by network administrators in connection with other Certicom products to centrally manage, deploy and enforce common handheld security devices. More information on Certicom and its products is available at: http://www.certicom.com.

Cisco Systems, Inc.

Cisco Systems provides networking solutions that connect computing devices and computer networks, allowing people to access or transfer information without regard to differences in time, place, or type of computer. Cisco Systems developed the Open Conditional Content Access Management (OCCAM), an encryption-based open technology standard for use in protecting digital content from unauthorized copying, distribution, and playback, which can be used to protect content during transmission and storage in any public, private or home network. More information on OCCAM is available at: http://www.senate.gov/~commerce/hearings/022802bechtolsheim.pdf.

ContentGuard, Inc.

ContentGuard, a DRM technology company, developed and promoted a standard digital rights language known as Extensible Rights Markup Language (XrML), a means of defining and controlling the rights and conditions associated with the use of copyrighted materials, which is discussed more fully below. ContentGuard offers version 2.0 of XrML, which extends the range of rights-enabled business models applicable to digital content as well as web services. Using XrML 2.0, a single digital rights language can be used to assign fine-grained rights and conditions to both digital content and services. More information on ContentGuard and its products is available at: http://www.contentguard.com.

Copyright Clearance Center (CCC)

The Copyright Clearance Center (CCC) is a voluntary, not-for-profit, industry-led organization that offers licensing and infringement protection services for both electronic and paper-based works. Created in 1978 at the suggestion of Congress, CCC today is a clearinghouse for processing rights for copyrighted text materials, with bilateral contracts with almost 20 counterpart organizations in other countries. Beginning with a simple transactional service by which rights holders and users could exchange permissions and royalties relating to the licensing of photocopying, CCC has developed a suite of licensing services to provide materials for education in colleges and universities. In 2000, CCC launched its "Rightslink" service, a technology protection system that allows publishers to engage in point-of-content licensing of materials published on web sites. More information on CCC is available at: http://www.copyright.com.

Digimarc Corporation

Digimarc Corporation is a provider of patented digital watermarking technologies that allow imperceptible digital code to be embedded in the printed or digital version of visual content, to deter counterfeiting and enhance Internet access. Digimarc's "ImageBridge" provides notice of copyrights and licensing opportunities for producers and distributors of commercial photographs. The Company's "MediaBridge" provides the means to link directly from printed materials to specific Internet sites by showing the enabled document to an imaging device. Digimarc's "Excalibur" contains a covert packaging security feature intended to deter counterfeiting, tampering and diversion of consumer packaged goods. More information on Digimarc and its products is available at: http://www.digimarc.com.

Digital World Services (DWS)

Digital World Services (DWS), a subsidiary of Bertelsmann AG, provides DRM solutions to the entertainment and publishing companies. DWS developed the "ADp2RA System," which is the foundation for its digital distribution solutions and services. When a digital content product is sold, this system grants initial consumer content rights, administers and manages the renewal, revocation and backup of those rights, and securely transfers the secure digital content throughout the digital distribution process. More information on DWS and its products is available at: http://www.dwsco.com.

DMDsecure

DMDsecure is a developer of server-side software components, frameworks and solutions. The company's "DMDfusion" is a DRM system that enables the creation, management, and delivery of licenses to entities offering access to protected content through trusted media players and devices. DMDfusion is used to manage and control the rights to high-value digital learning materials such as multimedia tutorials, video presentations, and textbooks. DMDsecure's "DMDaccess," a server side delivery rights enforcement solution for the delivery of live and on-demand streaming content, includes flexible rights settings such as time limitations and expiration dates. More information on DMDsecure and its products is available at: http://www.dmdsecure.com.

Elisar Software Corporation

Elisar Software is a supplier of DRM software applications. Elisar's "MediaRights" client is a digital enforcement technology that allows all forms of multimedia content to be safely displayed and distributed across intranets, extranets, and over the Internet. The application protects web site content by preventing unauthorized users from copying, forwarding, saving or printing images, multimedia files, documents, and other on-line information. MediaRights operates as a software service in conjunction with industry standard viewers. More information on Elisar Software and its products is available at: http://www.elisar.com.

eSynch Corporation

eSynch is a software development company that designs and delivers turnkey and customized solutions for the digital delivery of rich media contents. eSynch's products include "MediaOffice," a suite of browser-based administration tools allowing flexible, secure and intelligent Internet distribution of business media content; "Media Rights Manager," an integrated DRM system for secure Internet distribution of video content; and "SiteStreamer," a software toolkit that allows web sites to stream video in a more intelligent fully branded environment. More information on eSynch and its products is available at: http://www.esynch.com.

FileOpen Systems, Inc.

FileOpen Systems is a DRM technology provider. The "FileOpen Publisher" is a desktop DRM solution for managing access to PDF documents. The FileOpen Publisher has two components: "File Open Author" (for encrypting documents and setting permissions) and "File Open Client" (an Acrobat plug-in which enforces security settings on end-user computers). More information on FileOpen Systems and its products is available at: http://www.fileopen.com.

Gemplus International, S.A.

Gemplus International is a provider of technology, products and services that enable wireless network operators to offer their customers secure communications transactions through smart cards and related software. More information on Gemplus and its products and services is available at: http://www.gemplus.com.

Info2Clear

Info2Clear is a DRM company assisting authors, content creators, and rights owners in the secure distribution of digital content. The company also provides technology for secure e-mail exchange. Info2Clear's products include: "get-a-seal" (for registration and certification of copyrightable content) and "get-a-copy" (an infrastructure for selling reproduction rights). Info2Clear offers a digitally signed, forgery proof registration certificate with a time stamp to provide evidence to defend rights. Info2Clear's "get-a-view Publisher" is a DRM solution for publishers interested in entering the eBook market. Info2Clear's "eBookSuite" is an eBook-making tool set for publishers, which includes DRM technology. More information on Info2Clear and its products is available at: http://www.info2clear.com.

Infraworks Corporation

Infraworks Corporation is a supplier of DRM products based on its patented "InTether" technology, which enables organizations to create and securely share digital files. The "InTether File Security Series" is a collection of applications that protect digital files both inside and outside an organization. InTether File Security Series is comprised of two components: the "Packager" (which generates encrypted packages) and the "Receiver" (a client-side application that controls access and enforces permissions). The Series includes: the "InTether Desktop" (providing for secure e-mail), the "InTether Server" (providing for secure distribution over the Internet), and the "InTether SecureCD" (providing for secure distribution of CD-ROMs). More information on Infraworks and its products available at: http://www.infraworks.com.

Intel Corporation

Intel Corporation, a maker of semiconductor chips, supplies the computing and communications industry with chips, boards, systems that are integral components of computers, servers, and networking and communications products. Intel developed the High-bandwidth Digital Content Protection (HDCP), a technology to protect uncompressed digital content as it travels over Digital Visual Interface (DVI) links to computer monitor or television displays. More information on HDCP is available at: http://www.digital-cp.com.

International Business Machines Corporation (IBM)

IBM creates, develops and manufactures advanced information technologies, including computer systems, software, networking systems, storage devices, and microelectronics. IBM's Electronic Media Management System (EMMS) is an integrated DRM system that enables users to process media business data to package content with associated digital rights into encrypted containers for distribution to EMMS content delivery networks, retailers and enterprise portals. More information on IBM and EMMS is available at: http://www.ibm.com/us. IBM's Digital Media Solutions, a portfolio of applications that incorporates an open and standards-based framework, assists companies to create, manage, distribute, transact and protect their content. More information on IBM Digital Media Solutions is available at: http://www.ibm.com/industries/digitalmedia.

InterTrust Technologies Corporation

InterTrust Technologies developed a general purpose DRM platform, allowing for the protection and management of rights and interests in digital information including music, videos, software, games, publications and images. InterTrust's "RightsSystem" DRM platform is designed to implement a range of DRM functions, including persistent protection of digital information of all types and support for simple to complex business models. The RightsSystem consists of three elements. The "Rights/System Packager" enables content owners, distributors, and service providers to create digital content and package the products for distribution. The "Rights/System Server" allows content owners to establish and maintain the secure infrastructure for the system and authorize and deliver rights to the users of the system. The "Rights/System Client" enables consumers to access and use protected content on a variety of devices, including PCs, mobile phones and communicators, set-top boxes, and music players. More information on Intertrust and its products is available at: http://www.intertrust.com. Note: InterTrust was recently acquired by Sony of America, Koninklijke Philios Electronics N.V., and another investor.

Liquid Audio, Inc.

Liquid Audio is a provider of software, infrastructure and services for the secure digital delivery of media over the Internet. Liquid Audio's open platform enables the digital delivery of music over the Internet, giving artists, record companies, web sites and retailers the ability to create, syndicate and sell recorded music with copy protection and copyright management. Liquid Audio's digital distribution system is based on patented DRM technology and technologies for secure content transfer to portable devices, as well as the ability to honor territorial restrictions for digital music content. More information on Liquid Audio and its products is available at: http://www.liquidaudio.com. Note: In 2002, Liquid Audio sold its domestic and foreign rights to its patents to Microsoft, and Liquid Audio received a royalty-free license to continue to use the technology. In 2003, Liquid Audio sold its digital music fulfillment business to Geneva Media, LLC.

LockStream Corporation

LockStream Corporation creates software that secures distribution of content, products and services across all platforms and wireless devices. LockStream's "Secure Package Creator" takes content in its native format (for example, MP3) and secures it for digital distribution by converting a raw media file into a secure file. LockStream's "License Generator" creates and validates licenses for content packaged and secured in the LockStream format, setting forth the rules governing how digital media can be played or rendered across various consumer devices. LockStream's "Secure Package Reader" authenticates media before it can be rendered for playback on various devices. More information on LockStream and its products is available at: http://www.lockstream.com.

Macrovision Corporation

Macrovision Corporation produces copyright protection and video scrambling technologies for commercial videocassette duplicators, software companies, set-top decoder manufacturers, and major motion picture studios. Macrovision's video products prevent unauthorized copying and viewing of programs stored on videocassette and DVD or broadcast on pay-per-view cable and over satellite networks. A major supplier for Hollywood studios, over the past few years Macrovision has broadened its focus to include copy protection and DRM for other media, including multimedia computer software on CD-ROMs, electronic license management, and encryption. The company's products include: "MacroSafe;" "SafeDisc;" "FlexLm;" "SafeAuthenticate;" "SafeCast;" "SafeWrap;" "SAM Solutions;" "GT Licensing;" "Cactus Data Shield." More information on Macrovision and its products is available at: http://www.macrovision.com.

Microsoft Corporation

Microsoft Corporation develops, manufactures, licenses and supports a range of software products, including scalable operation systems, server applications, worker productivity applications and software development tools. Microsoft's core DRM technology is "Windows Media Rights Manager," an end-to-end[19] system that supports the secure delivery of digital media content as it travels across the Internet and between devices. Rights Manager supports a broad array of distribution and business models, including real-time streaming of digital content. Product features include: secure packaging and distribution, flexible licensing rules, and the ability to upgrade and repair. Microsoft's "Digital Asset Server" is Microsoft's solution for electronic publishing. More information on Microsoft and its products is available at: http://www.microsoft.com.

MediaSec Technologies, LLC

MediaSec Technologies develops and commercializes products and solutions based on its patented digital watermarking technology. MediaSec's products include

[19] The term "end-to-end" generally refers to a technological protection system that permits control over content at all times.

"MediaSignPrint" (providing protection against the counterfeiting of documents such as bank notes, identity cards or credit cards); "MediaSignDigitalWatermark" (an authentication product for digital images and videos used with digital surveillance systems); "MediaTrustTrusted" (a product combining digital watermarking with digital signatures for verification of printed paper copies of digitally signed documents); and "SysCoP" (a copyright information protection product designed for multimedia content, still images, and audio). More information on MediaSec and its products is available at: http://www.mediasec.com.

NDS Group PLC

NDS provides conditional access, broadcast control software and products and services for the management, control and secure distribution of entertainment and information to television (satellite, terrestrial and cable) and personal computers. NDS's "Synamedia" system, used to protect Video-on-Demand (VOD) over broadband networks using encryption technology, includes the "XTV Encryptor" (a content preparation station) and the "XTV Server" (ensuring that only authorized viewers can view encrypted VOD content). More information on NDS and its products is available at: http://www.nds.com.

Ness Technologies, Inc.

Ness Technologies is an information technology company specializing in the development, consulting and integration of software solutions. Working with television production companies in the United Kingdom, Ness Technologies developed "iRights," a software module that helps television, publishing, film, music and other media entities manage their rights, contracts and royalties. More information on Ness Technologies and its products is available at: http://www.ness-europe.com/irights.

On-Demand Distribution (OD2)

On-Demand Distribution (OD2) enables record labels to sell music on-line by providing the secure fulfillment of their music content to chosen retailers. As an enabling technology for the music industry, OD2 manages a catalogue of music content from several record labels. More information on OD2 and its services is available at: http://www/ondemanddistribution.com.

OverDrive, Inc.

OverDrive is a provider of technology services for the protection of digitized copyrighted works. The Company operates the Content Reserve digital rights clearinghouse and distribution service (www.contentreserve.com) that provides copyright protection and DRM services for over 30,000 works from approximately 300 commercial publishers. OverDrive also serves as a DRM service provider for a number of educational and digital content providers in the United States. The Company provides copyright management services to Internet college bookstores and educational web sites in the United States and abroad and deploys DRM technologies in connection with a broad range of materials used for educational purposes. More information on OverDrive is available at: http://www.overdrive.com.

Palm Digital Media (PDM)

Palm Digital Media (PDM) is a division of PalmSource, the software-licensing unit of Palm. PDM has developed several eBook products for the Palm operating system, including the Palm Reader for desktops and handheld devices. The Palm "Retail Encryption Server" is the centerpiece of Palm's DRM technology. The DRM system uses a hardware identification number, which has been assigned by the Palm Reader eBook application to a handheld or desktop computer. The Server uses the identification number to lock an eBook to a specific device. More information on Palm Digital Media and its products is available at: http://www.palmdigitalmedia.com.

Philips Digital Networks

Philips Digital Networks provides end-to-end solutions incorporating high performance MPEG-2 compression and multiplexing for satellite, cable and terrestrial transmission systems. The Company's technologies are applicable to broadcasting, enhanced and interactive TV for the home, as well as for Internet and mobile content delivery. Philips Digital Networks is developing audio/video streaming software, including MPEG-4 streaming video application software. The Company's content delivery products incorporate secure conditional access, watermarking and DRM technologies. Philips Digital Networks also is a supplier of set-top boxes and home gateways. More information on Philips Digital Networks and other Philips products and services is available at: http://www.digitalnetworks.philips.com.

Phocis, Ltd.

Phocis is a digital security company, providing services that control and manage the capture, processing and distribution of sensitive and confidential digital information. The Company's "Secure Digital Exchange" (SDX) allows users to revoke information and offers persistent protection throughout the lifetime of a document. The Company's "Secure Publishing Exchange" (SPX) is a DRM system that allows publishers to prepare, package and manage digital content in any format. More information on Phocis and its products is available at: http://www.phocis.com.

Rainbow Technologies, Inc.

Rainbow Technologies is a provider of digital content and transaction security solutions for the Internet and eCommerce. The company designs, develops, manufactures and sells anti-piracy, license management, distribution and tracking products, and satellite and network communications products using encryption technology. Rainbow's products include secure web server acceleration solutions; anti-piracy, and Internet software licensing and distribution solutions; public key infrastructure-based security solutions; voice, data and satellite information security, telecommunications and information security, authentication and USB-based web authentication keys. More information on Rainbow Technologies and its products is available at: http://www.rainbow.com.

RealNetworks, Inc.

RealNetworks develops end-to-end solutions that allow a broad range of users to create, send and receive audio, video and other multimedia services over the Internet. The Company's "Helix DRM" is a set of products for the secure licensing, delivery and rights management of digital media Helix DRM was designed to provide high-quality content delivery to trusted media players across all major platforms (including Internet media formats and standards-based formats such as MPEG-4) to multiple devices, including PCs, mobile devices, and home appliances. More information on RealNetworks and its products and services is available at: http://www.realnetworks.com.

RSA Security, Inc.

RSA Security is a provider of electronic security solutions. The company helps build secure, trusted foundations for electronic businesses through the use of its two-factor user authentication, encryption, and public key management products and solutions. RSA offers a number of authentication products (employing software and hardware tokens, smart cards, and digital certificates) to ensure the authenticity of people, devices, and transactions. RSA's "Web Access Management Solution" is designed to provide secure access to multiple based applications and services. RSA's Developer Solutions offer a range of software components to secure data in any format, wired or wireless. More information on RSA Security and its products is available at: http://www.rsasecurity.com.

SCM Microsystems, Inc.

SCM Microsystems designs, develops and sells hardware, software and silicon that enables users to securely access digital content and services, including content and services that have been protected through digital encryption. SCM provides, among other products, reader technology for access control systems deployed on the digital television and PC platforms, including conditional access modules and interface technology used by digital television operators to secure access to encrypted digital television broadcasts for paying subscribers. SCM also provides smart card readers and interface technology used to control access to PCs, computer networks and the Internet to facilitate computer and network security and secure on-line transactions. More information on SCM Microsystems and its products is available at: http://www.scmmicro.com/flash.html.

SealedMedia

SealedMedia is a DRM provider for publishers of all kinds of digital content (including text, images, audio and video) on the Internet. There are three software components to the Company’s “Sealed Media” solution: the “Sealer,” the “License Server,” and the “Unsealer.” The software components can be used to support digital content in a wide range of formats (including HTML, PDF, MP3, and MPEG-4). Access to sealed documents may be limited to authorized users and cease after a specified expiration date. Rights can be granted, changed or revoked at any time. More information on SealedMedia and its products and services is available at: www.sealedmedia.com.

SunnComm Technologies, Inc.

SunnComm Technologies, a firm that develops technology to limit the unauthorized copying of music compact disks (CDs), was the first company to commercially release a content-protected CD. SunnComm’s “MediaCloQ” is a technology designed to limit unauthorized copying of optical media using a personal computer by introducing alterations in the control area of the CD. More recently, SunnComm introduced its “Media Max CD3” technology, which builds on the Microsoft Windows Media 9 Series Digital Media Platform. More information on SunnComm Technologies and its products is available at: http://www.sunncomm.com.

Sony Corporation

Sony Corporation is a diversified company operating in the motion picture, game, and electronics industries (including the development, design, manufacturing and sale of electronics equipment). Sony also manufactures and distributes recorded music and image-based software and is one of the world’s largest producers of compact discs. Although Sony’s “key2audio” copy control technology prevents computer playback, Sony offers other products that allow owners of original CDs to play music on a PC or MAC. More information on the key2audio technology is available at: http://www.key2audio.com. Sony's DRM and distribution technology, "OpenMG X," will be applicable to a growing number of network-connected devices, including PCs, OpenMG-related products, and PlayStation 2. Note: Sony of America, Koninklijke Philios Electronics N.V., and another investor recently acquired InterTrust Technologies, which is discussed above. More information on Sony and its products is available at: http://www.sony.co.jp

Spectra Systems Corporation

Spectra Systems is a developer of limited play CD, CD-ROM and DVD products for the entertainment, software, and advertising industries. The Company developed MediaCoat, a marking technology that allows the placement of text and graphics on the play side of CDs and DVDs without interfering with playback performance. More information on Spectra Systems and its products is available at: http://www.spectra-science.com.

Thomson, Inc.

Thomson (formerly Thomson Multimedia) provides technologies, systems, finished products and services to consumers and professionals in the entertainment and media industries. Through its digital media solutions, Thomson provides digital video networking systems for the secure delivery of content from the studio to the consumer. The Company also offers key applications and media management services that provide the tools for content owners, network operators, and consumers to manage, access and retrieve streaming entertainment, news, sports, and information. More information on Thomson and its products is available at: http://www.thomson.com.

Savantech, Inc.

Savantech is a provider of digital distribution management services to media and entertainment companies. Savantech's "Photon Commerce" suite of products allows users to create a single unifying view of metadata and assets stored in disparate repositories across multiple divisions. Savantech's "Photon Rights Management" product provides intellectual property owners with a convenient mechanism for searching and requesting rights. More information on Savantech and its products is available at: http://www.savantech.com.

TTR Technologies, Inc.

TTR Technologies develops anti-piracy technologies that prevent illegal reproduction of software, music, games, and other media for the software and entertainment industries. TTR designs and develops digital security technologies that provide copy protection for electronic content distributed on optical media and over the Internet. TTR's "SafeAudio" software, which the company incorporates into encoding systems for optical media, adds to audio CDs, CD-ROMs, and DVD-ROMs an indelible digital fingerprint that prevents unauthorized consumer copying or professional remastering. More information on TTR and its products is available at: http://www.ttrtech.com.

Wave Systems Corporation

Wave Systems develops, produces and markets hardware and software-based digital security products for the Internet and e-commerce using encryption technology. The centerpiece of Wave Systems is the "Embassy Trust System," a trusted computing infrastructure that combines client hardware and software and a back-office infrastructure that manages its security functions. The client hardware consists of the "EMBASSY 2100" security chip, which may be embedded in such user devices as computer keyboards, smart card readers, PC motherboards, PC and/or cable modems, personal digital assistants, cable set-top boxes and a wide variety of other user devices. More information on Wave Systems technology and products is available at: http://www.wave.com/technology/trustedpc_1.html.

Verance Corporation

Verance Corporation provides systems for content management, airplay verification and connectivity solutions for the entertainment, media, wireless telecommunications and Internet industries. Verance also develops advanced audio watermarking (including the standard for SDMI Phase 1 and DVD-Audio) and wireless communications technologies. More information on Verance technology and its products is available at: http://www.verance.com.

VeriSign, Inc.

VeriSign provides digital trust services used by web sites, enterprises and individuals to conduct secure communications and electronic commerce on-line. The Company's code signing digital IDs (or certificates) allow content publishers, including software developers, to digitally sign their content including software and macros for secure delivery over the Internet. VeriSign's "Authentication Services" allow users to authenticate the identities of consumers, professionals and business entities at the beginning of a trust relationship for on-line transactions. Verisign also provides managed public key services. More information on VeriSign and its products is available at: http://verisign.com.

IV. ORGANIZATIONS

A. Introduction

The development of modern technological protection systems for digitized copyrighted works through private, voluntary, industry-led entities often takes place within a complex, dynamic organizational environment that also includes formal and informal standard-setting organizations, trade associations, non-profit research organizations, governmental and inter-governmental bodies. The non-exhaustive list of organizations that follows is intended to provide introductory information about the efforts of private companies and organizations to develop technological protection systems through an open, broad-based consensus process, including their interactions with other entities within this network. All descriptions of the organizations and their activities in this section are distilled from information that is made publicly available by the entities.

B. Private, Voluntary Industry-led Initiatives

4C Companies

Four companies (IBM, Intel, Matsushita, and Toshiba) (the "4C" companies) have developed a number of technologies for the protection of digitized copyrighted works. The 4C's Protection for Pre-recorded Media ("CPPM") and Content Protection for Recorded Media ("CPRM") protect digitized copyrighted works distributed or stored on portable storage media. CPPM, which uses encryption and watermark detection to protect content in pre-recorded digital media, has been adapted for works distributed in the DVD audio format.

CPRM protects audiovisual, literary and other copyrighted works stored on a variety of optical and flash memory-based storage media, including DVD-R, DVD-RW, DVD-RAM, SD Memory Card and Secure CompactFlash. CPRM provides for encryption of "copy once" content and includes the obligations to recognize and respond to watermarks and copy control instructions in content entering unprotected inputs. Both CPPM and CPRM include robust encryption of copyrighted material and implicit authentication of recording and rendering products via storage media-based broadcast encryption. The cryptographic cipher used for both CPPM and CPRM (the "C2" cipher) is licensed separately by the 4C Entity for certain uses, such as encrypting content stored on a fixed hard drive for "time shifting" purposes.

The 4C companies have proposed a framework for the integration of otherwise independent content protection technologies – the Content Protection System Architecture (CPSA). CPSA combines encryption, authentication and watermarking technologies with licensing agreements. Under the CPSA model, content is encrypted and transmitted digitally only via protected outputs and only to devices that are bound to provide a minimum level of persistent protection and, in some cases, to respond to usage rules conveyed by associated watermarks. CPSA includes Digital Transmission Content Protection (DTCP) technology developed by the 5C companies (discussed below). More information on the 4C companies is available at: http://www.4centity.com.

5C Companies

The 5C companies (Intel, Hitachi, Matsushita, Sony, and Toshiba) work together to develop technologies to protect copyrighted works in digital format. The 5C companies designed Digital Transmission Content Protection (DTCP) technology to protect audio and audiovisual content from unauthorized copying, interception and tampering within a localized network. DTCP technology is used to protect compressed content from unauthorized access as it travels over digital buses. By way of illustration, DTCP technology may be used to protect the "link" between a set-top box receiver and a DVD recorder or a digital television monitor. DTCP technology is used to ensure that DVD content is sent via digital outputs only to devices that will recognize and follow any associated copy control instructions. The Digital Transmission Licensing Administrator (DTLA) licenses DTCP technology. More information on DTLA is available at:

http://www.dtcp.com and on DTCP technology at:
http://www.dtcp.com/data/wp_spec.pdf.

Advanced Television Systems Committee (ATSC)

The Advanced Television Systems Committee (ATSC) is the international, non-profit organization that develops voluntary technical standards for high definition television. ATSC has developed and adopted a specification for an ATSC Redistribution Control Descriptor (or "Broadcast Flag"), which may be embedded into digital broadcast television content to guard against unauthorized redistribution. The Federal Communications Commission (FCC) currently is conducting a rule making (MB Docket No. 02-230) regarding the need for a regulatory regime within the limited sphere of digital broadcast television and on whether the FCC should adopt rules or create some other mechanism to resolve any outstanding compliance, robustness and enforcement issues related to the Broadcast Flag. More information on ATSC is available at: http://www.atsc.org.

CableLabs

CableLabs is a nonprofit research and development consortium that is dedicated to pursuing new cable telecommunications technologies and to helping its cable operator members integrate those technical advances into their business objectives. The goal of Cable Labs' OpenCable Initiative is to establish hardware and software specifications to create a common platform for the deployment of advanced interactive cable services. More information on CableLabs is available at: www.cablelabs.org.

Corporation for National Research Initiatives (CNRI)

The Corporation for National Research Initiatives (CNRI) is a non-profit organization that undertakes, fosters and promotes research on the strategic development of network-based information technologies. CNRI's Handle System is a distributed computer system that stores names, or handles, of digital items and which can quickly resolve those names into the information necessary to locate and access the items. The Handle System was designed by CNRI as a general purpose global system for the reliable management of information on networks such as the Internet over long periods of time and is currently in use in a number of prototype projects. More information on CNRI is available at: http://www.cnri.reston.va.us.

Copy Protection Technical Working Group (CPTWG)

The Copy Protection Technical Working Group (CPTWG) is an informal forum for content creators and owners, consumer electronics and computer companies, and interested consumers and consumer advocates to discuss technical issues related to content protection. CPTWG seeks consensus on technological solutions for various content protection challenges, including protecting in the DVD home video market from casual piracy. The CPTWG began by launching an encryption approach called Content Scrambling System (CSS) in 1997.

In November 2001, the CPTWG established the Broadcast Discussion Group (BPDG) to address the protection of digital broadcast television signals against unauthorized redistribution. More than 70 representatives of the motion picture, consumer electronics, computer and information technology, cable and broadcast industries, as well as individuals and representatives of consumer and civil liberties groups, participated in that process. In June 2002, the BPDG completed a technical evaluation of the Broadcast Flag technology, which provides a means of preventing unauthorized redistribution of digital broadcast television content outside the personal digital network environment. As noted above, the FCC currently is conducting a rule making with respect to a number of technical and enforcement issues related to the Broadcast Flag. More information on CPTWG is available at: http://www.cptwg.org.

Digital Video Broadcasting (DVB) Group

The Digital Video Broadcasting (DVB) Group is a private, voluntary industry group that develops technical specifications for the delivery of digital television. The consortium is composed of over 300 broadcasters, manufacturers, network operators, software developers, and regulatory bodies. Although the DVB's principal focus is on Europe, participants from over 40 countries are working on global standards for the secure delivery of digital television. Proposals for specifications are developed through collaboration of DVB Members in numerous Working Groups. Although DVB does not have standard-setting authority, its specifications are referred to international standard setting organizations such as the European Telecommunications Standards Institute (ETSI) (discussed below) for possible adoption as a global standard.

Since 1991, DVB has provided a forum for broadcasters, consumer electronics manufacturers and media interest groups interested in the development of digital television in Europe. By 1997, many DVB standards were adopted worldwide. DVB has been active in the following technical and commercial areas: Multimedia Home Platform (MHP), Copy Protection (CP), Personal Video Recorders (PVR), Broadband Satellite Systems (BSS), Wireless Home Networks (WHN), Storage Media Interoperability (SMI), and Return Channels (RC). DVB is currently working on technical specifications for content control in the consumer environment. More information on the DVB Group is available at: http://www.dvb.org.

DVD Copy Control Association (DVD CCA)

The DVD Copy Control Association (DVD CCA) is a non-profit corporation responsible for licensing and enforcing the Content Scrambling System (CSS) (an encryption scheme that protects the contents of DVDs) to manufacturers of DVD hardware, discs and related products. The CSS has been adopted by the content and DVD technology community and is on many prerecorded DVD discs released today. DVD CCA is responsible for selecting and licensing technology that will carry Content

Control Information (CCI). More recently, the DVD CCA is focusing attention on the selection of an appropriate watermark technology to carry CCI for implementation in conjunction with CSS licensed DVD players to prevent unauthorized recording and playback of DVD content where the CSS encryption has been bypassed. More information on DVD CAA is available at: www.dvdccaa.org

DVD Forum

The DVD Forum is an international association of hardware manufacturers, software firms and other users of Digital Versatile Discs (DVDs). The DVD Forum was formed for the purpose of exchanging and disseminating ideas and information about the DVD format. The DVD Forum defines technical for prerecorded and some recordable formats (such as DVD-R, DVD-RW, and RAM). Its Working Group 9 (WG 9) addresses copyright protection. The DVD Forum also works to promote broad acceptance of DVD products on a worldwide basis, across entertainment, consumer electronics and information technology industries.

Membership is open to any corporation or organization that is engaged in activities related to DVD research, and/or manufacturing, or any software or other users of DVD products that are interested in developing and improving the DVD format. However, DVD Forum Members are not required to support the DVD Format to the exclusion of other formats. Founded in 1995 by ten companies, the DVD Forum today includes more than 230 member companies. The ten founding companies are: Hitachi, Ltd; Matsushita Electric Industrial Co. Ltd.; Pioneer Electronic Corporation; Royal Phillips Electronics N.V.; Sony Corporation; Thomson Multimedia; Time Warner Inc.; Toshiba Corporation; and Victor Company of Japan, Ltd. More information on the DVD Forum is available at: http://www.dvdforum.org.

Internet Streaming Media Alliance (ISMA)

The Internet Streaming Media Alliance (ISMA) is a non-profit corporation formed to provide a forum for the creation of specification(s) that define an interoperable implementation for streaming rich media (video, audio and associated data) over the Internet. ISMA is an alliance that is comprised of companies that deliver solutions for the complete value chain of authoring, encoding, capturing, managing, distributing, streaming and consuming media. ISMA builds upon existing standards to endorse an implementation specification for delivering streaming rich media over the Internet. More information on ISMA is available at: http://www.isma.tv.

Object Management Group (OMG)

The Object Management Group (OMG) is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications. The OMG was formed to create a component-based software marketplace by hastening the introduction of standardized object software. OMG advocates an object-oriented system because of its capacity to expand in functionality by extending existing components and adding new objects to the system. OMG's charter includes the establishment of industry guidelines and detailed object management specifications to provide a common framework for application development. Founded in 1989 by eleven companies, the consortium now includes approximately 800 members. More information on OMG is available at: http://www.omg.org.

Open eBook Forum (OeBF)

The Open eBook Forum (OeBF) is a trade and standards organization that develops and promotes electronic publishing. Over 85 companies and other organizations are members of OeBF, including publishers, authors, hardware and software companies, and stakeholder organizations such as the Association of American Publishers (AAP) (discussed below), the Library of Congress, and the American Foundation for the Blind. OeBF members pursue a common goal of establishing specifications and standards for electronic publishing. The OeBF conducts its standards and trade activities through the operation of Working Groups and Special Interest Groups.

The Publication Structure Working Group maintains and advances the Open eBook Publication Structure (OEBPS), an open non-proprietary, specification for the content, structure and presentation of electronic books. The Metadata & Identifiers Working Group is responsible for creating, and endorsing and adapting a framework for metadata and identifier standards. The Systems Working Group is responsible for ensuring that all OeBF standards and products fit into a unified solution for electronic publishing. The Rights and Rules Working Group is responsible for standardizing the terms used to describe DRM product features to consumers and for developing a common, computer-readable language for specifying rights and other information. Special interest working groups address the needs of businesses, libraries, and persons with disabilities. More information on the Open eBook Forum is available at: http://www.openebook.org.

Open Mobile Alliance (OMA) Digital Rights Management

The Open Mobile Alliance (OMA) is a consortium of nearly 200 companies representing the world’s leading mobile operators, device and network suppliers, information technology companies and content providers. OMA serves as a center for mobile standardization work, assisting in the creation of interoperable services across countries, operators, and mobile terminals that will meet the needs of the user. The mission of OMA is to expand the market for the entire mobile industry by removing barriers to interoperability, supporting a seamless and easy to use mobile experience for users and a market environment that encourages competition through innovation and differentiation. For example, OMA seeks to advance DRM technologies that would enable a customer to download a game to a mobile for a specified period, with the option available to acquire refreshed rights after the original rights have expired. More information on OMA is available at: http://www.openmobilealliance.org.

Protecting Accumulated Intellectual Data for Accounting in Real-Time (PAIDFAIR)

The PAIDFAIR project, which is aimed at setting a worldwide standard for payment for protected content or software use, is an initiative led by six European companies. The objectives of the project include developing demonstration systems in fields of secure electronic software distribution and Pay-Per-Use, distribution of music content, e-payment and authentication integration with Smart Card, IP Distribution through broadcast/multicast and satellite communication, biometrical authentication and secure downloads for open Multimedia Home Platform (MHP) set-top-box. The PAIDFAIR trial intends to adapt and introduce the new encryption technology CodeMeter. More information on PAIDFAIR is available at: http://www.paidfair.com/us/index.php.

Secure Digital Music Initiative (SDMI)

The Secure Digital Music Initiative (SDMI) is a forum that has brought together more than 200 companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry, and Internet service providers. SDMI's goal is to develop open technology specifications that protect the playing, storing, and distributing of digital music necessary to enable the emergence of a new market for digital music. Phase I of SDMI's work produced a standard, or specification, for portable devices. Phase II focuses on working toward the completion of an overall architecture for delivery of music in all forms. More information on SDMI is available at: http://www.sdmi.org.

SmartRight Association

The SmartRight Association is an industry consortium composed of companies from the consumer electronics, conditional access, integrated circuit and smart card industries. The aim of SmartRight is to develop a worldwide framework for copy protection within a digital home network. The SmartRight system will work in combination with conditional access systems or DRM systems, to provide end-to-end protection of digital content from the content provider to the consumer's presentation device. The system is being designed to accept content from any kind of source, including free-to-air and pre-recorded content. SmartRight is responsible, among other things, for developing and maintaining the SmartRight specification. More information on SmartRight is available at: http://www.smartright.org.

Society of Motion Picture and Television Engineers (SMPTE)

The Society of Motion Picture and Television Engineers (SMPTE) is the leading technical society for the motion picture industry. Founded in 1916 to advance theory and development in the motion imaging field, SMPTE today publishes ANSI-approved standards, recommended practices, and engineering guidelines. Through its Metadata and Wrapper Technology Committee (W25) and Digital Cinema Content Security Committee (DC28), SMPTE is refining specifications for the digital cinema content security environment. More information on SMPTE is available at: http://www.smpte.org.

Trusted Computing Platform Alliance (TCPA)

The Trusted Computing Platform Alliance (TCPA) is an industry working group of more than 170 members focused on enhancing trust and security on computer platforms. The steering committee consists of Compaq, HP, IBM, Intel, and Microsoft. The TCPA seeks to develop an industry standard specification to address trustworthiness of computing platforms and to improve the authenticity, integrity, and privacy of Internet-based communications and commerce. TCPA also promotes the adoption of the TCPA Specification. More information on TCPA is available at: http://www.trustedcomputing.org.

TV-Anytime Forum

The TV-Anytime Forum is an international association of organizations that develops specifications to enable audio-visual and other services based on mass-market, high volume digital storage in consumer platforms (commonly called “local storage”). The Forum defines specifications that will enable applications to exploit local storage independent of the means of content delivery to consumer electronics equipment. Specifications are designed for interoperable and integrated systems – from content creators/providers, through service providers, to consumers. TV-Anytime Forum is developing a standard for the secure and flexible expression and enforcement of rights holders' usage conditions for media distributed to personal digital recorders.

Formed in 1999, the TV-Anytime Forum’s membership reflects a wide variety of industries, including traditional broadcasters, Internet broadcasters, content owners, service providers, telecommunications companies, consumer electronics manufacturers, information technology companies, component manufacturers and software vendors. More information on the TV-Anytime Forum is available at: http://www.tv-anytime.org.

VWM Group

The VWM Group is a consortium that includes several leading consumer electronics and information technology companies, including Hitachi, NEC, Pioneer, Sony, Digimarc, Macrovision, and Philips. The proposed anti-piracy solution by the VWM group is being considered by various industry standards organizations, but has not yet been adopted.

C. Standard-Setting and Related Organizations

A standard is any set of technical specifications that either provides or is intended to provide a common design for a product, process, service, or system. Standards are critical components of the modern economy.[20] From automobile ignition systems to computer modem communications protocols, detailed specifications are vital to industry and commerce, crucial to the health and safety of individuals, and basic to national and global economic performance.[21] Within this broad framework, this section briefly introduces some of the standards, along with the organizations and methods (both formal and informal) used to assess conformity with those standards, for the development of technological protection systems, including standards to identify digital content, to specify rights and conditions for use of that content, and to conduct electronic commerce.[22] All descriptions of the standard-setting and related organizations and their activities in this section, and the trade associations in the next section, are distilled from information that is made publicly available by the entities.

The American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is the coordinator of the U.S. voluntary standardization system and the gateway to the international standards and conformity assessment arena. ANSI has been called upon to provide high-level consultation to both private-sector interests and the U.S. government on a wide range of issues in hundreds of industry sectors. Through ANSI's committees and working groups, the Institute facilitates the development of American standards and formulates the U.S. positions on issues before the International Organization for Standardization (ISO) and the Electrotechnical Commission (IEC). More information on ANSI is available at: http://www.ansi.org.

European Standards Committee

The European Standards Committee (CEN) is one of the three formally recognized European Standards Organizations. The Information Society Standardization (ISS) System is the department within CEN responsible for standards activity for information and communications activities. In October 2001, the CEN/ISS DRM Group was established to prepare a report on DRM standardization for the European Commission. A copy of the useful, draft report is available for public comment at: http://www.cenorm.be/isss.

European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is a non-profit organization whose mission is to produce telecommunications standards for Europe and beyond. ETSI plays a major role in developing a wide range of standards and other

[20] The Department of Commerce and, in particular, the National Institute of Standards and Technology (NIST) assists the private sector in broad range of standard-setting activities.

[21] *See* "The Role of Standards in Today's Society and in the Future," Statement of Raymond G. Kammer, Director, National Institute of Standards and Technology, Technology Administration, Department of Commerce, Before the House Committee on Science Subcommittee on Technology, September 13, 2000.

[22] NIST previously canvassed DRM organizations. This section builds on the Gordon E. Lyon's "A Quick-Reference List of Organizations and Standards for Digital Rights Management," which remains a valuable resource.

technical documentation as Europe's contribution to worldwide standardization in telecommunications, broadcasting and information technology. Specifications for DRM systems developed by consortia of private companies are reviewed by ETSI for possible adoption as international standards (such as the recent proposal of the Digital Video Broadcasting proposal discussed above). More information on ETSI is available at: http://www.etsi.org.

Extensible Rights Markup Language (XrML)

Extensible Rights Markup Language (XrML) is a language to specify rights and conditions to control access to digital content and services. With origins in the Xerox Palo Alto Research Center (PARC), XrML has evolved through industry review, comment and product implementation. In 1996, the Xerox Corporation introduced Digital Property Rights Language, a forerunner of XrML, and took the product to market through Xerox Rights Management, which later would become a separate company called ContentGuard, Inc. ContentGuard, as discussed more fully elsewhere in this report, has developed a number of tools to support XrML. The OASIS Rights Language Committee currently is considering the adoption of XrML as a worldwide standard for digital rights language standard. OASIS is discussed more fully below.

XrML provides a universal method for specifying a right (for example, “play” or “copy”) or a condition (such as a time limit) that is associated with a particular work. XrML may be used by content owners to specify royalty arrangements, ownership, listening limitations, or context pricing (such as sale or rental). Encryption technology may be used for the authentication and protection of such expressions of rights and conditions. XrML has been designed to support a number of business models and to be interoperable within larger systems. XrML is based on open standards, with industries invited to collaborate and further develop the language. The language is said to be “extensible” because it is designed to incorporate new terms and business models as they develop. More information on XrML is available at: http://www.xrml.org or http://www.contentguard.com.

Information and Content Exchange (ICE)

Information and Content Exchange (ICE) is a communications protocol that supports content syndication relationships, facilitating the automated licensing of content over the Internet. In general, the ICE standard facilitates communications between syndicators (who make collections of content available for subscription) and subscribers (who browse, select and pull content from the web sites of syndicators). For example, “a syndicator” such as a magazine publisher might use the ICE standard to automatically transfer content and rights to multiple subscribers in a trusted relationship. The terms of the transaction (such as pricing) are negotiated and enforced by written contract rather than technology. The ICE standard was developed and is overseen by the Vignette Corporation, Microsoft, Sun Microsystems, Adobe and several other technology and media companies. More information on ICE is available at: http://www.icestandard.org.

Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE) is a nonprofit technical professional society of 350,000 members with close ties to the International Organization for Standardization (ISO), discussed below. In a variety of ways, the IEEE plays an important role in the development of technological protection systems. For example, IEEE 394/Fireware specifies the standard for Digital Transmission Content Protection (DTCP) technology, which is used to protect compressed content from unauthorized access as it is travels over digital buses.

Another example is the IEEE Learning Technology Standards Committee (LTSC), which develops technical standards, recommends practices and guides for software components, tools, technologies and design methods that facilitate the development of computer education and training components and systems. For example, LTSC developed the Learning Objects Metadata (LOM) scheme, which covers a broad range of educational materials from lecture notes to full courses. The LTSC recently authorized the formation of a study group on DRM technologies to gather requirements for a DRM standard for learning technology, to conduct research on existing standardization efforts, and to recommend projects. More information on IEEE LTSC is available at: http://ltsc.ieee.org/wg12.

International DOI Foundation

The International DOI Foundation (IDF) is an open, international membership organization of commercial firms and non-profit entities interested in electronic publishing and its enabling technologies. In 2000, over 40 organizations were members of the Foundation, including publishers, technology companies, and information intermediaries (such as libraries and information aggregators). IDF manages the development and licensing of the Digital Object Identifier (DOI), a system for the persistent identification and interoperable exchange of intellectual property in the digital environment, including articles, books, images, bibliographies, videos, charts, tables, and audio and electronic files. The DOI syntax has been accepted as a standard by the American National Standards Institute (ANSI) and National Information Standards Organization (NISO), both of which are discussed elsewhere in this report.

The eBook industry is considering using the DOI in a number of applications. In 2000, the American Association of Publishers (AAP) commissioned a study that recommended the use of the DOI system as the primary means of associating metadata with eBook content. IDF is currently working with the Corporation of National Research Initiatives (CNRI) (discussed above) to expand the functionality of the DOI system. More information on the International DOI Foundation is available at: http://www.doi.org/welcome.html.

International Group for E-Commerce Standards for the Books and Serials Sectors (EDItEUR)

The International Group for E-Commerce Standards for the Books and Serials Sectors (EDItEUR) is an international group coordinating development of the standards infrastructure for electronic commerce in the book and serials industries. Originally set up by the European publishing, bookselling and library federations, EDItEUR today works with 90 members from 17 countries, including the United States, Canada, Japan, Australia, South Africa, Israel and most of the EU countries. EDItEUR standards include the EPICS data dictionary and the ONIX International dictionary. In collaboration with the US Book Industry Study Group, BISG, EDItEUR also manages the EPICS/ONIX International standards for the communication of product information. More information on EDItEUR, including ONIX Release 2.0 and related guidelines, is available at: http://www.editeur.org.

Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is an open international community of network designers, operators, vendors, and researchers developing standards and protocols for evolution and smooth operation of the Internet. Through various working groups, IETF addresses intellectual property practices (by documenting and publishing existing practices and identifying what practices need to be amended) and network and data flow security issues. The IETF also addresses problems related to the identification of content, including ongoing work on the Uniform Resource Name (URN) and persistent uniform resource locator (URL). More information on IETF is available at: http://www.ietf.org.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from some 130 countries. ISO is a nongovernmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. More information on ISO is available at: http://www.iso.ch.

International Telecommunications Union (ITU)

The International Telecommunications Union (ITU), one of the 16 specialized agencies of the United Nations, is the traditional body for the development and publication of international telecommunications standards, which involves national governments as members and strong private sector participation. Standardization of wireless Internet technologies on the cellular telephone model (third generation wireless, for example) has taken place under the auspices of the ITU. More information on ITU is available at: http://www.itu.int./home.

Interoperability of Data in E-Commerce Systems (INDECS)

INDECS (Interoperability of Data in E-Commerce Systems) is an international collaborative project to develop a framework of metadata standards to support network commerce in intellectual property. The principal focus of the INDECS project was the practical interoperability of digital content identification systems and related rights metadata within multimedia e-commerce. Practical implementations of the INDECS framework include EDItEUR/BISG's ONIX, which provided the basis for the metadata component of the DOI system. Originally funded under the European Commission INFO 2000 Programme, the work of the INDECS initiative is continuing under INDECS Framework Ltd, a consortium of companies and collective rights administration organizations. More information on the INDECS framework is available at http://www.indecs.org.

Moving Picture Experts Group (MPEG)

The Moving Picture Expert Group ("MPEG") is a working group of the International Standards ("ISO") (discussed above) that is engaged in the development of international standards for the compression, decompression, processing, and coded representation of digital audio and video content. Over the years, MPEG has implemented a number of standards for the storage and transmission of content in video CD, MP3, digital TV, DVD and other formats. In 1992, MPEG designed MPEG-1, which sets forth coding standards for digital storage moving pictures and associated audio, supporting video CDs and MP3 music files. In 1994, the Group developed MPEG-2 for digital television and DVDs.

More recently, MPEG designed MPEG-4, a standard for compressing large audio and video files for delivery over digital multimedia platforms including the Internet. In October 1998, the ISO adopted MPEG-4 as an international standard (ISO/IEC 14496). The Internet Streaming Media Alliance (discussed above) recently released an open specification for Internet streaming based on MPEG-4. MPEG-7, which complements MPEG-4, defines an interoperable framework for content descriptions that was recently adopted by the ISO.

The MPEG-21 Multimedia Framework is the most recent project of the Working Group. According to MPEG, the goal of MPEG 21 is to "define a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by different communities." MPEG characterizes the new standard as a "big picture" of how different elements of an "infrastructure for the delivery and consumption of multimedia content – existing or under development – relate to each other." More information on MPEG is available at: http://mpeg.telecomitalialab.com.

National Information Standards Organization (NISO)

The National Information Standards Organization (NISO) develops and promotes technical standards used in a wide variety of information services. NISO is a not-for-profit association accredited as a standards developer by the American National Standards Institute (ANSI), which is discussed above. NISO's voting members and other supporters include a broad base of information producers and users including libraries, publishers, government agencies, and information-based businesses. More information on NISO is available at: http://www.niso.org.

Online Information Exchange (ONIX)

The Online Information Exchange (ONIX) is the international standard for representing and communicating book industry product information in electronic form, incorporating the core content which has been specified in national initiatives such as BIC Basic and the AAP's ONIX Version 1. ONIX is a standard for describing the attributes of physical books (although a related standard for electronic books is under development). The standard provides fields for cover images, number of pages and book size. On-line book retailers such as Amazon and Barnes and Noble are using the ONIX standard. More information on ONIX available at: http://www.editeur.org/onix.html.

Open Digital Rights Language (ODRL)

The Open Rights Language (ODRL) is a proposed DRM language and data dictionary pertaining to all forms of digital content. The ODRL is a vocabulary for the expression of terms related to digital content, including permissions, constraints, obligations, conditions, offers and agreements with rights holders. ODRL is designed to be extended by different industry sectors (such as eBooks, music, audio, and software). ODRL is freely available and has no licensing requirements. The ODRL initiative supporters are committed to fostering and supporting open and free standards for the specification of media commerce rights language. More information about ODRL is available at: http://www.odrl.net.

Organization for the Advancement of Structured Information Standards (OASIS)

The Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit international consortium that promotes the development, convergence and adoption of e-business standards. OASIS produces worldwide standards for, among other things, security, web services, business transactions, electronic publishing, and interoperability within and between marketplaces. OASIS seeks to accelerate the adoption of product-independent formats based on public standards, including Standard Generalized Markup Language (SGML), Extensible Markup Language (XML), and other structured information processing standards.

Founded in 1993 under the name SGML, OASIS began as a consortium of vendors interested in developing guidelines for interoperability among products that support SGML. In 1998, OASIS changed its name to reflect the expanded scope of its technical work. Today OASIS has more than 600 corporate and individual members in 100 countries around the world. OASIS Members set their technical agenda, using an open process designed to facilitate industry consensus.

The goal of OASIS's Rights Language Technical Committee is to define an industry standard for a rights language that supports a wide variety of business models and has an architecture that provides the flexibility to address the diverse needs. For example, in March 2002, ContentGuard, Hewlett-Packard, Microsoft, Reuters, and Verisign employees submitted a proposal to the Technical Committee to consider the adoption of Extensible Rights Markup Language (XrML) as worldwide standard digital rights language. More information on OASIS is available at: http://www.oasis-open.org/committees/rights.

Publishing Requirements for Industry Standard Metadata (PRISM)

The Publishing Requirements for Industry Standard Metadata (PRISM) is a metadata standard that facilitates the on-line operations of magazine publishers. PRISM facilitates the creation, use, syndication, aggregation and reuse of content from magazines, news, catalogs, and journals. PRISM provides a framework for the interchange and preservation of content and metadata, along with a set of controlled vocabularies to describe the content. More information on PRISM is available at: http://www.prismstandard.org.

Shared Content Object Reference Model (SCORM)

The Shared Content Object Reference Model (SCORM) is a collection of specifications adapted from multiple sources to provide a comprehensive suite of e-learning capabilities that enable interoperability, accessibility and reusability of web-based learning content. The SCORM was developed by the Department of Defense's Advanced Distributed Learning Initiative (ADL) to incorporate many of the emerging standards and/or specifications into one common reference model. The Air National Guard's advanced distance learning programs illustrate how such a reference model serves the needs of distance education. More information on the ADL and SCORM are available at: http://www.adlnet.org.

Universal Description, Discovery and Integration (UDDI)

The Universal Description, Discovery and Integration (UDDI) protocol is a cross-industry effort driven by major platform and software providers, as well as marketplace operators and e-business leaders within the OASIS standards consortium. The UDDI protocol creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use web services over the Internet. UDDI also allows operational registries to be maintained for different purposes in different contexts. The sponsoring organization, UDDI.org, intends to turn over the UDDI project to an independent standards organization in the near future. More information on the UDDI project is available at: http://www.uddi.org.

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO) is one of the 16 specialized agencies of the United Nations, an intergovernmental organization with headquarters in Geneva, Switzerland. WIPO is responsible for the promotion of the protection and use of intellectual property throughout the world through cooperation among States, and for the administration of various multilateral treaties dealing with the legal and administrative aspects of intellectual property. The WIPO Digital Agenda, adopted by the General Assemblies of Member States in September-October 1999, includes as one of its aims the facilitation of "interoperability and interconnection of electronic copyright management systems and the metadata of such systems" (Digital Agenda, item 6). More information on WIPO is available at: http://www.wipo.org.

World Wide Web Consortium (W3C)

Founded in 1994, the World Wide Web Consortium (W3C) is an international industry consortium that develops interoperable technologies for the World Wide Web. Services provided by W3C include a repository of information about the World Wide Web for developers and users; reference code implementations to embody and promote standards; and various prototype and sample applications to demonstrate use of new technology. In the intellectual property area, W3C's goal is to make it easier for users to obey the law by combining payment and labeling technologies to clearly express the terms and conditions related to on-line materials and to make it easier to stop indiscriminate redistribution of protected material by establishing a labeling system for cataloging sites that are known to contain infringing materials. More information on W3C is available at: http://www.w3.org.

D. Trade Associations

Association of American Publishers (AAP)

The Association of American Publishers (AAP) is a national trade association representing the U.S. book publishing industry. AAP represents more than 300 commercial and non-profit member companies, university presses, and scholarly societies that publish books and journals across a broad range of interests. AAP's members include leading educational publishers, who produce textbooks and other educational and testing materials covering the entire range of educational and professional needs. In addition to their print publications, many AAP members are active in the emerging market for e-books, while also producing computer programs, databases, and a variety of multimedia works for use in on-line, CD-ROM and other digital formats.

AAP's programs and activities cover a broad range of issues of interest to publishers, including protecting and strengthening intellectual property and exploring challenges and opportunities related to new technology. In 1994, AAP launched the Digital Object Identifier (DOI), which focused on content identification (discussed more fully above), as part of a broader copyright management initiative. Through its Open eBook Standards Project and other efforts, AAP promotes the development and use of standards and requirements in the areas of DRM metadata and numbering that will enable an open and competitive marketplace for eBook commerce on a large scale. More information on AAP is available at: http://www.publishers.org.

Business Software Alliance (BSA)

The Business Software Alliance (BSA) is an international organization representing companies in the software, hardware and Internet sectors. BSA's priorities are enhancing trust and security in cyberspace, reducing software piracy, promoting strong policies for intellectual property protection and free trade, and educating the public about sound software management practices. The BSA is committed to working on technological solutions for protecting digital content on-line, but as innovators, software and hardware makers BSA member companies are also committed to letting the market lead. Thus, BSA participates in cross-industry efforts to develop technological protection measures to protect copyrighted works within a broad framework of shared objectives – protecting content, promoting consumer choice, and fostering innovation. More information on BSA is available at: http://www.bsa.org.

Interactive Digital Software Association (IDSA)

The Interactive Digital Software Association serves the business and public affairs needs of companies that publish video and computer games for video game consoles, personal computers, handheld devices and the Internet. IDSA members collectively account for more than 90 percent of the entertainment software sales in the United States in 2002, and billions more in export sales of American-made entertainment software. More information on IDSA is available at: http://www.idsa.com.

International Federation of the Phonographic Industry (IFPI)

International Federation of Phonographic Producers (IFPI) is an international organization comprised of 1500 record companies and distributors in 76 countries. IFPI describes its priorities as fighting music piracy, promoting fair market access and adequate copyright laws, and helping to develop the legal conditions and the technologies for the recording industry to prosper in the digital age. IFPI has been closely involved in the discussions between the recording industry and the technology and consumer electronics sectors known as the Secure Digital Music Initiative (SDMI), which is discussed below. More information on IFPI is available at: http://www.ifpi.org.

The Motion Picture Association of America (MPAA)

The Motion Picture Association of America (MPAA) and its international counterpart, the Motion Picture Association (MPA), serve as the voice and advocate of the American motion picture, home video and television industries, domestically through the MPAA and internationally through the MPA. MPAA represents the largest producers and distributors of filmed entertainment: Buena Vista International, Inc; Columbia Tristar Film Distributors International, Inc.; Paramount Pictures Corporation; Twentieth Century Fox Film Corporation; Universal International Films, Inc.; and Warner Bros., a division of Time Warner Entertainment Company, L.P.

The MPAA pursues an active agenda to confront digital piracy and facilitate the viability of a legitimate marketplace for high-quality digital entertainment, including promoting technological protection systems. Currently, the MPA's three primary goals are: (1) implementing a "Broadcast Flag" to prevent the unauthorized redistribution of "in-the-clear" digital over-the-air broadcast television, including its unauthorized redistribution over the Internet, (2) plugging the "analog hole" that results from the fact that protected digital content can easily be converted into analog form and then reconverted to unprotected digital form, making it subject to widespread unauthorized copying and redistribution, and (3) putting an end to copyright infringement on so-called "file-sharing" services on peer-to-peer (p2p) networks. As noted above, the Federal Communications Commission (FCC) currently is conducting a rule making on the Broadcast Flag. More information on the MPAA is available at: http://www.mpaa.org.

Recording Industry Association of America (RIAA)

The Recording Industry Association of America is the trade group that represents the U.S. recording industry. The mission of RIAA is to foster a business and legal climate that supports and promotes its members' creative and financial vitality. RIAA's record company members create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States. In support of this mission, the RIAA, among other things, works to protect intellectual property rights worldwide, conducts industry and technical research, and monitors domestic and international legal and public policy issues affecting the U.S. recording industry. RIAA has been closely involved in the discussions between the recording industry and the technology and consumer electronics sectors known as the Secure Digital Music Initiative (SDMI), which is discussed below. More information on RIAA is available at: http://www.riaa.org.

Software & Information Industry Association (SIIA)

The Software & Information Industry Association (SIIA) is a trade association representing over 1,400 high-tech companies that develop and market software and electronic content for business, education, consumers, the Internet, and entertainment. SIIA members represent a wide range of business interests. Numerous SIIA members create and develop new and valuable encryption technologies, use encryption technologies to protect their proprietary content, and purchase or license software and information products and other content and services that utilize encryption technologies. As a result, SIIA and many of its members are actively involved in issues relating to the protection and use of encryption technologies and the relationship between research and development activities relating to encryption. More information on SIIA is available at: http://www.siia.net.

Appendix A

In response to a request for information from Congress, and on the basis of public comments, the USPTO compiled the following non-exhaustive list of companies that have developed, are proposing to develop, or offering technological protection systems (including components thereof) for digital media embodying copyrighted works and prevent infringement. The information in this list is intended for the use of Congress. The USPTO has not conducted an independent analysis of these companies and makes no recommendations, comparisons, or comparative assessments of their products or services.

Company	**Web Address**
Adobe Systems	http://www.adobe.com
Akamai Technologies	http://www/akamai.com
Alchemedia	http://www.alchemedia.com
Aladdin Knowledge Systems	http://www.ealaddin.com
Alpha-Tec	http://www.alphatec.com
AlpVision	http://www.alpvision.com
Atabok	http://www.e-parcel.com
Authentica	http://www.authentica.com
Axeda Systems	http://www.e-parcel.com
BayTSP	http://www.baytsp.com
Blue Spike	http://www.bluespike.com
Canal Plus	http://www.canalplustechnologies.com
CenterSpan Communications	http://www.centerspan.com
Certicom	http://www.certicom.com
Cloakware	http://www.cloakware.com
Compris	http://www.compris.com
ContentGuard	http://www.contentguard.com

Copyright Clearance Center	http://www.copyright.com
CopySeal	http://copyseal.com.au
Cyveillance	http://www.cyveillance.com
Datamark Technologies	http://www.datamark-tech.com
Digimarc	http://www.digimarc.com
Digital Rights	http://www.digitalrightsllc.com
DigiTreal	http://www.digitreal.com
Digital World Services	http://www.dwsco.com
Diversinet	http://www.dvnet.com
DMDsecure	http://www.dmdsecure.com
Digital Media on Demand	http://www.dmod.com
DotEncrypt	http://www.dotencrypt.com
Elisar Software	http://www.elisar.com
eMeta	http://www.emeta.com
eRights	http://www.erights.org
eSynch	http://www.esynch.com
Ewatermark	http://www.ewatermark.com
Flexplay	http://www.flexplay.com
FileOpen Systems	http://www.fileopen.com
Gemplus International	http://www.gemplus.com
GenuOne	http://www.genuone.com
IBM	http://www.ibm.com/us
Info2Clear	http://www.info2clear.com

Infraworks	http://www.infraworks.com
InterTrust Technologies	http://www.intertrust.com
Intel	http://www.digital-cp.com
Irdeto Access	http://www.irdetoaccess.com
IP Shield	http://www.shieldip.com
IPRSystems	http://www.iprsystems.com
Liquid Audio	http://www.liquidaudio.com
Lock-Out	http://www.lock-out.com
LockStream	http://www.lockstream.com
Loudeye	http://www.loudeye.com
Macrovision	. http://www.macrovision.com
Markany	http://www.markany.com
MediaSec Technologies	http://www.mediasec.com
MediaDefender	http://www.mediadefender.com
Microsoft	http://www.microsoft.com
MTL Systems.	http://www.mtl.com
Musicrypt	http://www.musicrypt.com
Nagra	http://www.nagra.com
NDS	http://www.nds.com
Ness Technologies	http://www.ness-europe.com
NetActive Inc.	http://www.netactive.com
NetQuartz	http://www.netquartz.com
On Demand Distribution	http://www/ondemanddistribution.com

Overdrive	http://www.overdrive.com
PACE Anti-Piracy	http://www.paceap.com
Palm Digital Media	http://www.palmdigitalmedia.com
Perico	http://www.pericosecurity.com
Philips Digital Networks	http://www.digitalnetworks.philips.com
Phocis	http://www.phocis.com
PlayApp	http://www.playapp.com
Protexis	http://www.protexis.com
Rainbow Technologies	http://www.rainbow.com
RangerOnline	http://www.rangerinc.com
RealNetworks	http://www.realnetworks.com
Rights Market	http://www.rightsmarket.com
RSA Security	http://www.rsasecurity.com
Savantech	http://www.savantech.com
SCM Microsystems	http://www.scmmicro.com
SDC	http://www.digicont.ch
SealedMedia	http://www.sealedmedia.com
SealTronic	http://www.sealtronic.com
SecureMedia	http://www.securemedia.com
Smarte Solutions	http://www.smartesolutions.com
Spectra Systems	http://www.spectra-science.com
Softwrap Limited	http://www.softwrap.com
Sony	http://www.sony.co.jp

Sospita	http://www.sospita.com
SunnComm Technologies	http://www.sunncomm.com
Syncast	http://www.syncast.com
Thomson	http://www.thomson.com
Trymedia Systems	http://www.trymedia.com
TTR Technologies	http://www.ttrtech.com
Verance	http://www.verance.com
Vidius	http://www.vidius.com
VeriSign	http://verisign.com
Wave Systems	http://www.wave.com
WaveXpress	http://www.waveexpress.com
WIBU-Systems	http://www.wibu.com/us
Xat.com	http://www.xat.com
z4 Technologies	http://www.z4.com