Digital Rights Management –a Technological Measure for Copyright Protection and its Possible Impacts on Libraries

Dr. Sabuj Kumar Chaudhuri
Librarian, Basanti Devi College, 147B, Rash Behari Avenue, kolkata-700 086
Sabooj_c@yahoo.co.in

1.0 Introduction

Intellectual property (IP) deals with creations of the human intellect. Intellectual property is a cluster of legally recognized rights associated with innovation and creativity – the works of the mind, as against physical products, land and other tangible resources. Even though it is intangible, intellectual property is often recognized as personal property, to be sold and traded like other forms of property. IP is categorized as **Industrial Property** (Patent, industrial designs and trademark), and **Artistic and Literary Property** (Copyright). Intellectual property rights (IPR) are the rights awarded by society to individuals or organizations principally over creative works: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. They give the creator the right to prevent others from making unauthorized use of their property for a limited period.

With the advent of information technology, managing intellectual property rights especially copyrights in content industries has become very difficult, and thus Digital Rights Management (DRM) is being applied in the publishing and information industries. Copyright is the foundation of the publishing industry as well as all content industries, and DRM can supplement copyright protection as well as support mutually agreed licensing arrangements.

Publishers and libraries have a common respect for copyright law but view copyright from different perspectives. The institutional mission and operating models of libraries are different from those of authors and their publishers. Libraries have a unique mission and operate under a distribution model that emanates from the exceptions and limitations provided under copyright law.

Technological protections against copyright infringement are one component to digital rights management. Although DRM probably will not replace the traditional framework of intellectual property law, it can be designed to supplement that framework. DRM does not implement copyright. DRM is technology that establishes and enforces to varying degrees certain permissions and restrictions on access to and use of content. These permissions and restrictions are not, and in the current state of technology could not be, an embodiment of copyright law.

The combination of powerful computers, content that can be ripped, very large storage media and file sharing has conspired to produce an extremely difficult situation for rights holders. All content is now vulnerable to illegal copying and distribution over the Internet, irrespective media type. What began with the infringement of CD-Audio has now spread to films, books and many other type of content that can be digitized. The situation has become critical for all kind of content industries, as their revenue decline in the face of widespread content piracy. It is for this reason that the content industries are looking to Digital Rights management (DRM).

2.0 What is DRM?

Digital Rights Management-- a term commonly reduced to the acronym “DRM”.

Digital Rights Management is a collective name for technologies or a range of techniques that prevent one from using a copyrighted digital work beyond the degree to which the copyright owner (or a publisher who may not actually hold a copyright) wishes to allow one to use it . It is actually a range of techniques that use information about rights and rightsholders to manage copyright material and the terms and conditions on which it is made available to users.

In terms that are more formal DRM has been described as ‘a way of addressing the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over tangible and intangible assets, including management of rightsholders’ relationships.’

Two possible interpretations of the term digital rights management are:
Management of digital rights: The responsibility of expressing and managing the rights to content in electronic or digital form, as a corollary to content in print. *Digital management of rights*: The ability to physically manage intellectual property and proprietary rights in content by way of an electronic system or process, associated with copyright management systems.’Digital’ refers not to rights in information but to the medium in which the information is expressed. The rights one is managing are not digital. It is the content of the work that is in digital form.
Digital Rights Management systems can be used to protect high-value digital assets and control their distribution and usage. A DRM system offers a persistent content protection against unauthorized access to the digital content, limiting access to only those with the proper authorization. It should be flexible to manage usage rights for different kinds of digital content (e.g. music files, video streams, digital books, images) across different platforms (e.g. PCs, laptops, PDAs1, mobile phones) and control access to content delivered on physical media or any other distribution method (e.g., CD-ROMs, DVDs, flash memory).

2.1 Functional Aspects of DRM

Thus DRM has two functional areas:

1. The identification and description of intellectual property, rights pertaining to works and to parties involved in their creation of administration (digital rights management)
2. The (technical) enforcement of usage restrictions (digital management of rights)

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

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

An *access control* system manages a user’s access to content, usually achieved through some kind of password protection. However, once access to the content has been granted, no further protection is applied.

A *copy protection* system is designed to signal the extent of allowed copying and serial copying , if any , that is defined by the associated “usage information” with respect to any instance of delivered content , and to implement and enforce the signaled behavior in consumer equipment . The notion of copy protection can be extended to control the movement of content within and outside the user domain, encompassing re-distribution over the internet.

A fully enabled *intellectual property rights management system* covers the processing of all rights information for the electronic administration of rights, sometime including contractual and personal information, to enable end-to-end rights management through out the value chain.

2.2 Perspectives of DRM

The Open eBook Forum, a leading ebook standards organization, suggests that DRM should be viewed from three perspectives: *technical*, *social* and *legal*.

The *technical perspective* involves rights specification language, electronic package controls and trust infrastructure.

It is the technical perspective most people think of when they talk about DRM. The technical DRM perspective involves a number of elements that are often used in combination to secure content. Most are based on the mathematics of cryptography. These include:

- Encryption
- Public/private keys
- Digital certificates
- Watermarks
- Access control
- Authentication
- Secure communication controls
- Secure content storage
- Rights specification language
- Trust infrastructure

The *legal perspective* involves

- Legislation
- Compliance
- Investigation
- Enforcement

One DRM technology that holds promise from the legal perspective is digital watermarking. Digital watermarks are conceptually similar to traditional paper-based watermarks. Unlike their paper counterparts, however, digital watermarks are often made from an invisible stream of digital bits buried in a document or image. The digital watermark bits can be made to contain identifying information such as the original publisher, or even the name or credit card number of the purchaser. The digital watermark may not be visible to humans, but can easily be read by special software. Other software called web crawlers can also scour the web to locate illegal content.

Digital watermarking technology does not prevent the illegal distribution of intellectual property, but it does enable the detection of illegal copies and can, therefore, enable compliance, investigation and enforcement of current legislation. DRM encryption and even digital watermarking cannot guarantee completely secure digital content. A sufficiently motivated attacker, given sufficient time, money and other resources, can defeat most, if not all, encryption schemes.

The *social perspective* involves expectations, mores and education. It is technically possible for consumers to acquire high-quality copies of copyrighted works without compensating the copyright holders, but it may not be legal. Downloading is not freeloading, and yet many ebook consumers fail to make the distinction. Some do not understand that a distinction exists, and others choose to ignore it.

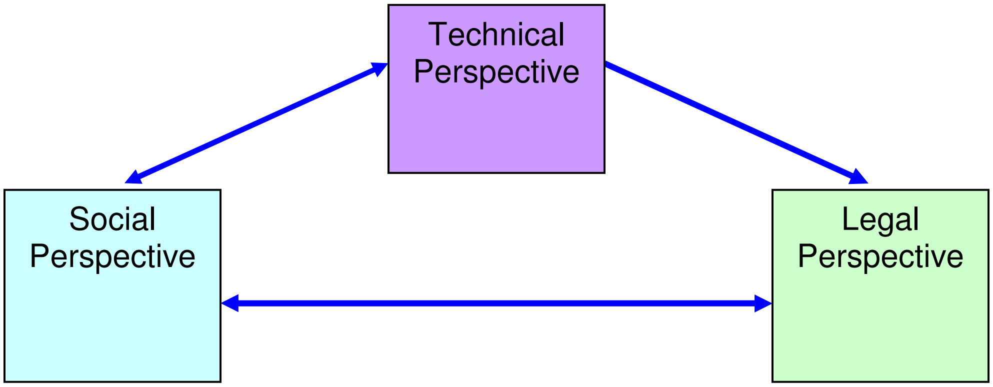

Figure 1: Three perspectives of DRM

2.3 Benefits of DRM

- ✓ Protection of digital content
- ✓ Secure ebook distribution
- ✓ Content authenticity
- ✓ Transaction non-repudiation
- ✓ Market participant identification

2.3.1 DRM Provides Protection of Digital Content

By scrambling, or *encrypting*, content, DRM enables authors and publishers to send digital content across an unsecured network, like the Internet, so that the content can be read only by the intended recipients - - ebook consumers. DRM uses a computer program called a *cryptographic algorithm* to encrypt ebook content. The cryptographic algorithm needs a secret key, a particular phrase or string of numbers, to encrypt the content. Only the holder(s) of this key can later unlock the content and read it.

Since all key holders can readily access the encrypted content, it is quite important to properly manage keys, and much of DRM is concerned with this.

2.3.2 DRM Enables Secure Ebook Distribution

Once ebook content is protected via DRM encryption, the proper key is needed to decrypt the content and render it readable. Without the key, the file is unintelligible. Anyone can have access to the encrypted content, but it will be of no use without the decryption key.

Long keys are better than short keys, just like a combination lock using three numbers, say “36-27-12,” is better than one that unlocks anytime “12” is selected on the dial. Today, 128-bit keys are in common use.

2.3.3 DRM Ensures Content Authenticity

It is not very easy to modify the content of a physical book and pass it off to unsuspecting consumers as an original. In contrast, tainted ebook content could be made to blend seamlessly with the original bits. To protect content authenticity, the content provider creates a message digest when the original, authentic ebook content is published. This “official” message digest is then stored in a safe place, but made available to consumers who want to verify the authenticity of acquired ebook content.

2.3.4 DRM Provides for Transaction Non-repudiation

In both physical and electronic markets, it is important for participants to be able to prove that any given transaction actually took place. In practice, two mathematically related keys are used, one private and one public. The private key is owned by a transaction participant and kept secret. A participant “signs” the transaction when he encrypts (a piece of) it with his private key. Anyone interested in verifying the authenticity of the transaction can obtain the participant’s public key and attempt to decrypt the signature. If the decryption operation is successful, market participants trust that the private key holder participated in the original transaction.

2.3.5 DRM Supports Participant Identification

In the physical world, it is fairly easy to determine who the participants in a transaction are. On the Internet, of course, it is not so simple. Without much difficulty, anyone can create a web site that appears to be entirely legitimate. Most are; some are not. DRM provides the ability to identify market participants using *digital certificates*. A digital certificate functions much the same way as a birth certificate or a social security number. A digital certificate is created using a cryptographic technique that binds a person’s identity with his or her public cryptographic key. A digital certificate is created by combining an individual’s public key, other identity information and one or more digital signatures.

2.4 DRM System

The core concept in DRM is the use of digital licenses. Instead of buying the digital content, the consumer purchases a license granting certain rights to him. A license is a digital data file that specifies certain usage rules for the digital content. Usage rules can be defined by a range of criteria, such as frequency of access, expiration date, restriction of transfer to other devices, copy permission etc. These rules can be combined to enforce certain business models, such as rental or subscription, try-before-buy, pay-per-use and a lot more. Protected content can be distributed though a client/server system, super-distribution, digital audio/video broadcasting, or CDs. Without possessing digital license to the content, digital content is a sequence of scrambled bits. Often digital content and licenses are stored separately, which makes the system more flexible in a way that protected content can be freely distributed amongst users and license requests can take place later. Through digital licensing, content providers can gain much more control over what the consumer can do with the content.

2.5 Various Components of DRM

Different DRM vendors have different DRM implementations, names and ways to specify the content usage rules. However, the basic DRM process is the same, which usually involves four parties: the content provider, the distributor, the clearinghouse and the consumer. Usually a DRM system is integrated with an e-commerce system that handles financial payments and triggers the function of the clearinghouse.

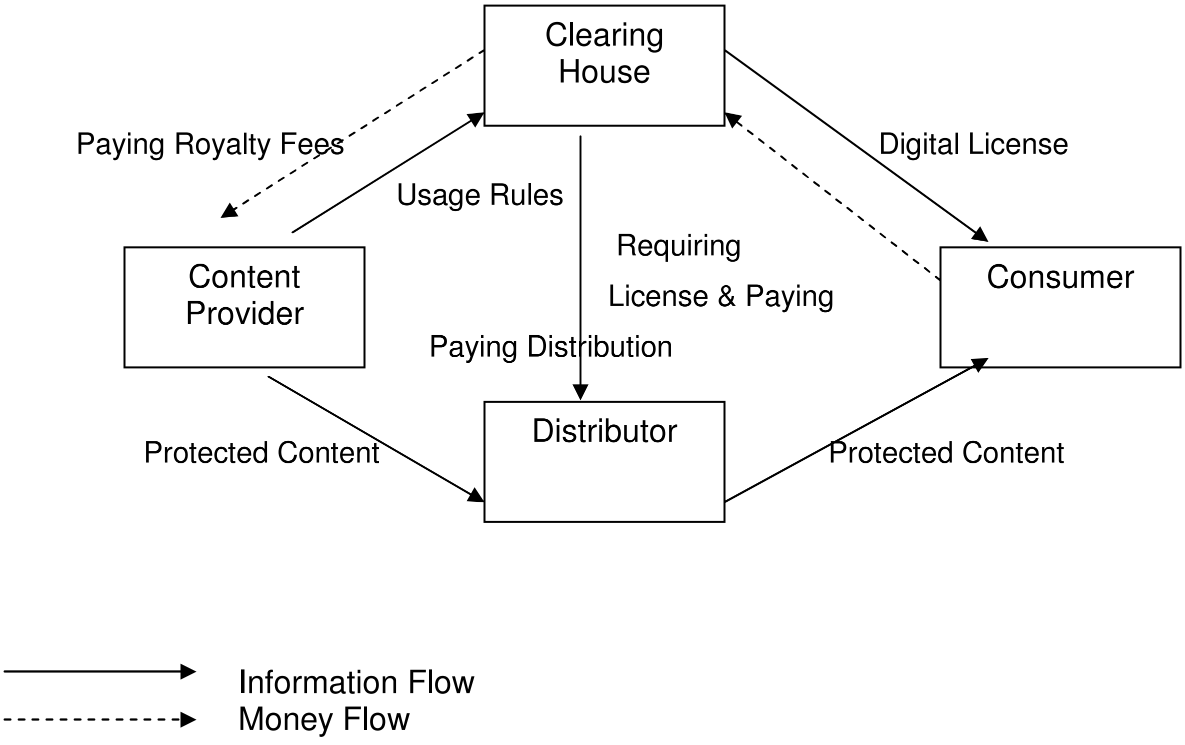

Figure 2: The Basic Components of a DRM System

• **The content provider** such as a publishing house holds the digital rights of the content and wants to protect these rights.

• **The distributor** provides distribution channels, such as an online shop or a web retailer. The distributor receives the digital content from the content provider, creates a web catalogue presenting the content, and rights metadata for the content promotion.

• **The consumer** uses the system to consume the digital content by retrieving downloadable or streaming content through the distribution channel and then paying for the digital license. The player/viewer application used by the consumer takes charge of initiating license request to the clearinghouse and enforcing the content usage rights.

• **The clearinghouse** handles the financial transaction for issuing the digital license to the consumer and pays royalty fees to the content provider and distribution fees to the distributor accordingly. The clearinghouse is also responsible for logging license consumptions for every consumer.

A typical DRM model used by current DRM implementations works as follows: Firstly, the content provider encodes the digital content into the format supported by the DRM system. Different DRM systems provided by different DRM vendors may support different content formats. The digital content is then encrypted and packaged for the preparation of distribution. The content provider may use watermarking technology to embed digital codes into the digital content that can identify the ownership of the content and the usage rules. Next, the protected content is transferred to the appropriate content distribution server, e.g. web server or steaming server, for on-line distribution. The digital license containing content decryption keys and usage rules is sent to the clearinghouse. The usage rules specify how the content should be used, such as copy permit, pay-per-view, a one-week rental, etc. At the other end of the process, the consumer downloads the digital content from the web server or requests streaming content from the streaming server. To be able to consume the protected content, the user has to request a valid license from the clearinghouse. After receiving the license request, the clearinghouse verifies the user's identity for example by having the user present a valid digital certificate, charges his account based on the content usage rules, and generates transaction reports to the content provider. Finally, the license is delivered to the consumer's device after the consumer has paid through the e-commerce system, and the protected content can be decrypted and used according to the usage rights in the license. In this model, consumers can pass along received digital content to other people through super-distribution, which lets vendors market their digital content to a vast amount of potential customers without direct involvement. Although digital content can be freely distributed, to utilize the content, the recipient has to contact the clearinghouse and provide whatever information or payment required for the license.

3.0 DRM Systems

DRM systems are software packages or technological restraints that restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.

DRM systems take at least three approaches to securing content. The first is "containment" or the wrapper, an approach where the content is encrypted in a shell so that it can only be accessed by authorized users. The second is "marking" or using an encrypted header, such as the practice of placing a watermark, flag, XML or XrML tag on content as a signal to a device that the media is copy protected. The third is the secure container, such as a dedicated reading device.

These systems enable the definition of different usage rights for different business models, and to categorize different types of users. Consumers/users, classes of individuals, library patrons, and library consortia. The authors transfer rights to the publisher; the publisher decides which of those rights to set to rules in the system as applied to a particular work. The technology, software, and administrator do the rest. Other business models, license arrangements, and usage agreements become redundant or even irrelevant.

3.1 Characteristics of DRM

DRM systems are based on systematic identification and recording of information about the legal rightsholders (copyright owners) and about the legal rights associated with the content. This is often managed through the use of metadata and rights management information (RMI) or Digital Object Identifiers (DOI).

3.1 .1 Metadata

Metadata is information that is held about a particular piece of content. Various metadata formats have been developed, but common to all is that they are structured around a set of key words and data category descriptors. Consistent use of metadata can be a valuable aid in locating material and establishing basic information about the material. It has been common practice for many organisations to create metadata using keywords that make sense to them at a particular point in time.

3.1.2 Security Features and Copyright Protection

There are numerous techniques that can be used to reduce the likelihood of infringement of Intellectual Property through the application of DRM systems. Each has different strengths and weaknesses as well as acquisition, integration and maintenance costs. While no technological system is 100 per cent secure, DRM can provide relatively high levels of protection for copyright materials. The most common protection techniques are encryption and digital watermarking.

Encryption

This scrambles the information embedded within a digital object so that it cannot be used without a password. Software is often protected this way.

Copyright protection technologies

Various technological means are available to protect copyright works from unauthorised access and use. They may involve encoding the terms and conditions under which works can be used, embedding them in the file and allowing use of the material only when the conditions are met. Typically, the embedded information includes Rights Management Information (RMI) about the object such as author, title, copyright and links to a key required to unscramble the information. Users need a license to access the key. The license specifies the user's rights. Often the key is locked to the characteristics of the user's computer so that it cannot be moved to another computer. This is sometimes called 'node locking'.

Digital watermarking and signatures

This embeds information (usually about author, publisher, terms, and conditions of use) into the data. It can be removed but only with severe degradation to the quality of the data. If it is effective, the watermark will be identifiable even if the quality of the data deteriorates. Watermarks can be visible or invisible. Watermarks can be used to personalise a particular instance of a work to a user to reduce the likelihood of that person passing it on or duplicating it. Some watermarks can be searched for over the Internet using special 'spiders' or web crawlers.

3.1.3 Personalisation

This involves tailoring content to particular user requirements in terms of size, format, content (such as extracts from a larger work) and often the embedding of a personal, visible watermark. A University course-pack made up of a number of selected chapters from a range of books and magazines with a visible watermark of the name and year of the course is a powerful form of personalisation. It is unique and therefore any leakage can be easily tracked back to the source.

3.1.4 Granularity

Granularity describes the capacity of a DRM system to deliver small chunks of targeted information to an end user or to other digital content creators and producers who can use these bits and bytes to create new works. This pooling and blending of ‘granules’ of digital content is fundamental to the production of new media in its many forms.

3.1.5 Interoperability

In a commercial digital environment, creators, producers and traders of digital content need systems that can ‘talk’ to each other. Producers and users need to be able to use work for any legitimate purpose from different sources and in different formats. This requires compatible systems.

The Digital Object Identifier (DOI)

The DOI system is comparable to the bar code system adopted to identify items in the physical world. Each bit or byte of content – the digital object – is allocated a number through a registration agency and metadata describing the digital object is recorded. Changes to the metadata can be made providing a relatively simple way of keeping track of the object and its ownership. Every DRM system requires persistent content protection, meaning that protection has to stay with the content. In order to manage and protect intellectual property, it is essential to have adequate identification and description pertaining to content available (i.e., metadata). One such persistent identifier is Digital Object Identifier (DOI). The International DOI Foundation states, “The Digital Object Identifier (DOI) is a system for identifying and exchanging intellectual property in the digital environment. It provides a framework for managing intellectual content, for linking customers with content suppliers, for facilitating electronic commerce, and enabling automated copyright management for all types of media.” The DOI is a "persistent identifier of intellectual property entities". Unlike a URL, it does not point to a location. The DOI specification was originally developed by the

Corporation for National Research Initiatives based on their "Object Handle" specification.

Rights expression languages

Various forms of interoperable languages creating vocabularies for the expression of terms and conditions for use of digital content, regardless of its form (websites, text files, images, music, pdf files and streaming media) are being developed. Prominent among these are the Open Digital Rights Language initiative (ODRL) and the Extensible Rights Markup Language (XrML).

3.1.6 Ease of Use

A major reason to adopt DRM systems is that legitimate users find the experience relatively easy. The technological controls embedded in the content (the metadata) can be unobtrusive and can facilitate easy access for authorised users and consumers without requiring them to complete additional forms or documentation.

3.1.7 Payment Systems

DRM systems can offer different methods of payment and, as in the physical world, no one method is suitable for all situations. The most common method of payment on the Internet is by credit card where payments for higher amounts often incur significant merchant fees, while smaller payments can cost more in fees than the purchase price of the work.

Subscription

Subscription accounts involve payment in advance by prepaid credit, usually via a credit card. Customers are informed when credit runs out, prompting another payment request. As a payment system, subscription is inexpensive to establish and maintain, especially when it is managed digitally as part of a DRM system.

Aggregated Payments

The customer is charged for small access or use payments when the aggregated payment amount becomes worth processing. Billing is in arrears and can be by credit card charge or invoice.

Payement Clearing Houses

A centralised clearinghouse using a prepay or invoice system for multiple vendors overcomes the reluctance of customers to commit to one vendor and solves the problem of merchants holding a lot of small uncharged payments.

Electronic Cash

There have been several attempts to create an electronic equivalent to cash to overcome the cost overhead of credit card merchant fees. Whilst some have been theoretically achievable, none have survived nor flourished commercially.

4.0 DRM for Various People

4.1 Creators

A major challenge faced by creators such as writers, illustrators, designers, and animators, is how to keep track of work in the digital environment. Adopting some form of DRM can help them to manage the material online to ensure that their work is protected and that its commercial use is paid for. As individual creators, DRM offers a way of making works commercially available in a relatively safe and protected environment. Done well it should allow creators to reach more potential customers than through normal distribution channels.

As part of a larger DRM system, creators can:

□ make their works available on selected terms and conditions
□ access other works available for use and re-use
□ make all or part of work/s available on a fee or free basis
□ make use of whatever technological protection is offered by the system.

4.2 Publishers

When publishers prepare content for delivery to customers they may choose to manage the content in a protected format aimed at preventing unauthorised copying. This may be in the form of watermarking, encryption, or password access. They may also contract with users to provide access to the works on a fee or free basis, depending on the rights associated with the work being accessed. Granularity is important here, as the works provided to users may be collections of content from many different sources bundled together into a single product. An MP3 file is a common example of one such bundle.

4.3 Content Traders

Digital technology has brought with it an enormous extension in the potential market for content traders (including producers and publishers).
DRM may be helpful to content traders in the following way:

□ use technology to protect works from unauthorised and unpaid use

□ use the internet as the marketplace to provide access to more users/consumers

□ provide an opportunity to deliver new products that would not be cost effective in traditional forms or channels

□ streamline rights management to provide better remuneration to creators and producers

□ implement managed payment systems such as pay per use, subscription or micropayments that enable the content to be marketed and priced differently and in more innovative ways

□ track and record payment and usage for royalty payments and information to rights holders

□ manage security issues.

5.0 Software of DRM

Deployment of DRM is still at an early stage. There are a number of DRM solutions on the market. Among these solutions, Microsoft's Windows Media Rights Manager (WMRM), IBM's Electronic Media Management System (EMMS), InterTrust's Rights|System, and RealNetworks's RealSystems Media Commerce Suite (RMCS) are the most promising ones. Apart from the above major DRM providers, there are many other companies delivering DRM solutions including Adobe (www.adobe.com), IPR Systems (iprsystems.com), Liquid Audio (liquidaudio.com), Alchemedia (alchemedia.com), Digital World Services (dwsco.com), ContentGuard (contentguard.com), SealedMedia (sealedmedia.com) and many more.

6.0 Standards

The usability problem in current DRM implementations is caused by the deployment of non-standardized protection mechanisms. To guarantee wide acceptance and interoperability between different DRM systems, standard definition for different components of a DRM system is required. Using a standard DRM architecture and rights language, different DRM vendors can work together and end users will not be locked up into a particular DRM system. Several organizations and initiatives are working towards the definition of standards, such as the Open Digital Rights Language Initiative, World Wide Consortium, Open eBook Forum, Secure Digital Music Initiative, Internet Digital Rights Management, etc.

7.0 Publishers and Libraries Using DRM

DRM has been used by organizations such as the British Library in its secure electronic delivery service to permit worldwide access to substantial numbers of rare (and in many cases unique) documents which, for legal reasons, were previously only available to authorized individuals actually visiting the Library's document centre at Boston Spa in England. This is an interesting case, one in which DRM has actually increased public access to restricted material rather than diminished it. The British Library has experimented with several forms of electronic delivery over the last twenty years and the Ariel® system has been used for the last ten years. Internally, this was a stand-alone system and it was impossible to integrate into the automated request processing systems. Furthermore, Ariel is not much liked by publishers as they claim that there is little, if any, control possible. It is also not possible to transmit documents directly to the end-user without the addition of further action on the part of the intermediary. Publishers such as Thomson Education, Harper Collins and Wiley have now adopted the DRM system.

8.0 DRM and Libraries

Libraries have a fundamental role to play in the development of a democratic society by enabling access for all members of the community to a wide range of knowledge, ideas, opinion as well as cultural, scientific and educational information. Access to information is essential in education and research and has a direct impact on literacy levels, economic growth and quality of life.

ICTs and digital information have opened up great new opportunities to access to essential content and provide innovative services e.g. libraries in developing countries are gaining affordable access to the wealth of international academic journals and databases. Libraries provide access to digital material through a variety of legal constructs; license agreements, exceptions under national copyright law, legal deposit, the public domain. DRM poses a threat. At worst, it can block access, at best it can inhibit by making access time-consuming and costly to arrange.

Libraries in the west are already experiencing the problems associated with DRM. Material bought and paid for by the library has become inaccessible through technical protection measures, while the supplier has since gone out of business or it is not profitable for the vendor to correct the problem and the sums of money are too small for the library, even if it has the financial resources to pursue legal action. The result is that the material is effectively removed from the library collection. Anti-circumvention laws prevent libraries from availing themselves of their lawful exceptions under national copyright laws. This can prevent or place restrictions on copying or sharing or lending material, current awareness services, book reviews, exhibitions, sending information to students who cannot come into the library. In short, libraries have fewer rights in the digital environment than in the print world. Instead, libraries are having to negotiate special agreements with individual rightsholders to obtain DRM-free material or permission to circumvent in restricted circumstances. This is an option realistically enjoyed only by the largest and best resourced libraries. The result is that the digital divide will increase as under-resourced libraries or those in smaller, rural or underprivileged communities (ironically standing to benefit most from digital technologies) lose out on their statutory rights.

9.0 Key Concerns for Libraries

The principal policy issues for libraries are not derived from DRM technology, itself, but from the business models, the content industry chooses to enforce. DRM has uses far beyond simply enforcing traditional and long-standing protections extant in current law. By embedding controls within the product, providers can prevent the public from use that is non-infringing under copyright law as well as enforce restrictions that extend far beyond those specific rights enumerated in the Copyright Act (or other laws). Thus, DRM changes the fundamental relationship between the creators, publishers, and users, to the detriment of creators, users, and the institutions that serve them. DRM, if not carefully balanced, limits the ability of libraries to serve the information needs of its patrons.

9.1 Eliminating the "First sale" Doctrine

DRM eliminates the "First sale" limiting the secondary transfer of works to others. First sale has been for centuries a bedrock principle governing the balance of rights between consumers and sellers of information products. It is first sale that allows people to share a favorite book or CD with a friend and that creates secondary markets for works. It is first sale that allows libraries to loan lawfully acquired works to the public.

9.2 Enforcing a "Pay-per-use"

If it becomes the dominant or even sole mode of access, will be contrary to the public purposes of copyright law. It should not be the business of government to favor or enforce any particular business model in the information marketplace, particularly one that raises major issues of equity and potentially severe economic consequences for public institutions.

9.3 Artistic Creation. It has long been understood that the creation of new artistic works may require the excerpting or transformation of older ones; DRM may be used in ways that prevent such excerpting or transformation from happening.

9.4 Preservation and Archiving

Many market models of DRM distribution systems envision content that essentially disappears after a specific period of time or number of uses. DRM technologies can also prevent copying content into new formats. Such controls will prevent all kind of libraries from preserving and providing long-term access to the knowledge products of our society. From the days of the Great Library of Alexandria, society has turned to such institutions to preserve its cultural heritage and provide access to it. There is no evidence that alternative organizations currently exist or will form to play that role in the digital pay-per-use world. Libraries and archives play a crucial role, and some have a legal mandate, to preserve and make available our cultural and scientific heritage for future generations. DRM jeopardizes this role as they have the potential to lock away covered material forever. The issue of long-term preservation carries a real urgency as media must be adapted regularly to new data formats, operating systems and data carriers. In addition, data (e.g. music, software, electronic journals) stored in propriety DRM formats is at much greater risk of being lost once the playback media is no longer available. Under DRM, there is a great risk that the public record of the future may be distorted.

9.5 Historiography. Historical research fundamentally depends on being able to access and quote older documents and other kinds of works -- DRM can be implemented in ways that make historiography far more difficult, if not impossible, in many contexts.

9.6 Eliminating "Fair Use"

DRM technology can prevent normal uses of works protected by copyright law, such as printing or excising portions for quotation. For libraries to serve their educational, research, and information roles, the public must be able to use works in the full range of ways envisioned by the Copyright Act in its limitations and exceptions.

9.7 The use of Shared Materials in Learning Environments

DRM may make it more difficult, or even impossible, for works to be used in otherwise lawful ways in both real classrooms and"virtual" ones (e.g., distance learning).

10.0 Possible Impacts of DRM on Libraries

There is no doubt that DRM has the potential to have a tremendous impact on libraries and how they do their work. Exactly what the impact will be is hard to predict today because of this is a technology in the early stages of its potential development. But it is possible to present some general cautions based on current experience with protected works.

The good news is that there is nothing about DRM that would inherently prevent library lending. As a matter of fact, the systems that have been and are being developed for the sale of works can be transformed into systems for lending, since lending is virtually identical to a short-term sales transaction. We already have lending of digital works in systems like netLibrary's [11] for ebooks and in recently developed systems for libraries by FictionWise [12] and OverDrive [13]. More sophisticated DRM systems may allow libraries to provide additional services beyond lending, such as integrating digital library materials into courseware at educational institutions. But DRM is likely to provide significant challenges as well, especially in these areas:

10.1 Local Control

Rights management systems, especially when embedded in trusted computing systems, will be on the cutting edge of computer technology for at least some time. These systems require strong security end-to-end, from the producer of the digital product to the end user. Because of their technical requirements it is unlikely that a fully trusted digital rights management function will be included in library computer systems, at least not in a way that is affordable to most libraries.

This means that the content and the control of the content will remain in vendor systems, and libraries will "outsource" access to the digital materials to these vendors. This is not unlike the situation in libraries today in relation to online databases and digital reference materials, but the impact of this model should be expected to increase as the technology grows in complexity and expense. Implications of this model range from the library's right to archive materials to issues of patron privacy.

10.2 Contracts and User Support

With hard copy works, there is one set of rights that pertains to all. A digital rights management system with a fully developed rights expression language could provide a different set of rights for each publication, and if not for each publication than at least for each publisher. At the extreme, libraries could find themselves negotiating for user rights on a title-by-title basis. More realistically, there will be classes of works with different sets of rights, and classes of users who can exercise different rights. Some amount of time will be spent by library staff mediating between the users and the rights packages, especially as users gain experience with the restrictions imposed by DRM. You can imagine a time when a user comes to the reference desk looking for a book on a topic but specifying that it must be one that allows some printing, or that can be rendered in large type on a particular device. The user support overhead for libraries must be calculated into the cost of purchasing and managing these materials.

10.3 Archiving and Future Use

There is an interesting contradiction taking place today when it comes to digital materials. Although some titles are available on a term-limited licensing basis, many titles are being offered for sale to libraries. Sale in this case meaning a permanent acquisition. Sale is what makes sense to libraries, who insist on the ability to purchase electronic materials even if they do not physically acquire the digital files. Sale also makes sense to publishers whose entire business model is based on units sold. But we are not even sure how to archive and provide some guarantee of future access to digital files that have no rights management controls applied to them, and the addition of DRM into this future makes matters much worse. If it takes an entire complex system to allow a user to open and read a book, what happens twenty or fifty or a hundred years from now when that system no longer exists? When the default is that usage rights must be positively granted, a loss of that granting system means that no use can take place. DRM in itself does not make digital archiving impossible, but it does compound the problem. The bottom line is that digital works are in our future, and that digital works need protection because they can be easily copied. This we cannot change. But librarians can have an impact on the development of DRM technologies by participating in the discussions taking place in standards organizations and the research arena. It is our professional duty to take part in the development of technologies that will affect the future of reading and information access.

11.0 Concluding Remarks

Digital Rights Management is emerging as a formidable new challenge, and it is essential for DRM systems to provide interoperable services. DRM, if broadly and indiscriminately applied, may throttle the advance of personal-computer technology itself. What this means is that, in addition to the problems that DRM may create for libraries and librarians in limiting the use of content, it also might limit the creation and use of more refined and advanced information-retrieval tools.

The bottom line is that the widespread use of computer networks and the global reach of the World Wide Web have added substantially to the information sector's production of an astonishing abundance of information in digital form and these digital contents need protection because they can be easily copied. This we cannot change. It is inevitable. But librarians can have an impact on the development of DRM technologies by participating in the discussions taking place nationally and internationally in standards organizations and the research arena. It is our professional duty to take part in the development of emerging technologies that will affect the future of reading and information access as a whole.

Selected References

Australian Interactive Multimedia Industry Association (2003). *A Guide to Digital Rights Management.*Canberra: DCITA.

Cunard, J. P. & et.al. (2003). *Current Developments in the Field Of Digital Rights Management.*Geneva: WIPO.

Innella, R. (2001).Digital Rights Management (DRM) Architectures. *D-Lib Magazine*, 7(6), Retrieved February 2, 2006, from http://www.dlib.org/dlib/june01/iannella/06iannella.html

Liu, Q., Naini, R S., & Sheppard, N.P. (2003). Digital Rights Management for Content Distribution. *Australasian Information Security Workshop*. Adelaide: Australian Computer Society.

Nisbet, M (2003).*Digital rights Issues*. Washington D.C.:ALA.

Important Websites

http://www.ala.org/ala/washoff/WOissues/copyrightb/digitalrights/digitalrightsmanagement.htm

http://en.wikipedia.org/wiki/Digital_Rights_Management

http://www.overdrive.com/news/pr/12162003.asp

http://www.drmblog.com/

http://www.iprsystems.com

About the Author

Author is a First Class First M.Sc in Marine Science from the University of Calcutta. Then Completed Associateship in Information Science from INSDOC (presently NISCAIR) of CSIR, New Delhi with the specialization in Patent Information System. Author also did MLIS from Annamalai University, Tamilnadu. Then received Junior

Research Fellowship Award from the University Grants Commission [UGC(JRF)NET], Govt. of India and with this financial grant he submitted his PhD on Intellectual Property Rights (IPR) in the Department of Library & Information Science, Jadavpur university, Kolkata. Author also had served in West Bengal Civil Service (WBCS), Govt of West Bengal. He writes many research articles in peer reviewed journals on IPR and written study material for IGNOU for their course –P.G. Diploma in Intellectual Property Rights (IPR). Recently received Best Performance Award from UNESCO in International Workshop on GSDL held in IIMK, Kozhikode by UNESCO-DSIR-IIMK.