DRM Practices in the E-Publication Industry

Bong Wee Kiau
Universiti Utara Malaysia, Malaysia

Norshuhada Shiratuddin
Universiti Utara Malaysia, Malaysia

INTRODUCTION

Electronic publishing (e-publishing) is the process of publishing information to be viewed electronically or online and delivered in the form of electronic books (e-books), e-mail newsletters, Web sites, CD-ROM, wireless publishing, and most recently electronic ink (Thomas, 2004). With the recent growth of telecommunication technologies and the Internet, assisted by the development of new technologies such as high-bandwidth connections and peer-to-peer networks, digital distribution services in which clients distribute files between themselves without using a central server (Burkhalter, 2001) have vastly improved the way we produce, procure, store, redistribute, and consume digital content. At the same time, these have created several problems like unauthorized copying, modification, and redistribution by a third party. Downloading encoded files has gained acceptance among Internet-savvy users because it provides immediate access to digital content and does not rely on physical media. The ease of processing, obtaining, and transmitting information has made easier both trading in data as well as collecting information from different sources, and has resulted in information about individuals often being collected and sold without their knowledge (Banks, Dickinson, Erickson, Reynolds, & Vora, 2001).

Everyone associated with e-publishing will be concerned with how e-books are protected from unauthorized copying. Realizing the potential of the Internet as a dynamic medium for delivery of intellectual property (IP), before digital content owners will offer their copyright works for sale or promotion, a secure system that protects digital content is needed. Digital rights management (DRM) is a collective term for tools and processes whose purpose is to enable owners of copyright works to control their use. DRM technologies impose constraints on the use of digital objects or IP that correspond to the terms of the agreement between publisher and consumer during digital content commerce (Clarke, 2000). DRM promises a secure framework for digital content distribution and enables an electronic marketplace where previously unimaginable business models can be implemented. At the same time, it particularly ensures content providers; copyright owners receive adequate remuneration for the creation of the content that is distributed over the DRM system. It manages the commerce, IP ownership, and confidentiality rights of digital content creators and owners, as content travels through the value chain from creator to distributor, then to the consumer, and from consumer to other consumers.

Protection of IP is as critical as protection of any physical asset that society, individual authors, and publishers value and hold. The information industry and society are realizing the potential of the Internet as a dynamic medium for delivery of IP, coming to appreciate the difficulties in how those assets are to be managed and the complexities in providing easy access in the electronic environment while protecting intellectual property rights (IPR) (Slowinski, 2003).

There are many reasons for wanting to manage the rights associated with IP. Authors and artists wish to control what can be done with their creations, scholars wish to ensure that they receive proper attribution, commercial enterprises wish to support business models that involve licenses and fees, and consumers want an environment free of legal worries and unexpected costs. Although rights themselves are not technological in nature, they are defined by laws, beliefs, and practices (Downes, Mourad, Piccariello, & Robson, 2003). Technology can be used to transmit, verify, interpret, and enforce rights as they apply to digital content and services.

Currently, as tools such as local and national digital repositories come online and are widely developed, more and more of these valuable resources are going to be stored and shared digitally. These resources are

already subject to IPR law, but storing and sharing them in this new and very public manner makes it important to ensure that these resources comply with IPR law and can be protected by it. For those who want to share their content with others, it is also important that they understand the legal environment that they are operating in.

Research undertaken indicates that digital content providers often spend a great deal of time managing tasks like obtaining legal advice, adding features to protect copyright, managing online user payment, income stream to rights holders, monitoring and tracking users and payers, and the use of existing and new materials. Thus, DRM has emerged to manage the commerce. Trust and control are core issues related to DRM. A DRM system deals with encrypting content and information, and is integrated into an organization at an infrastructure level (Duhl & Kevorkian, 2001). A company that implements DRM uses a trusted vendor's technology to manage encrypted data, keys, and information about users. Companies, therefore, need to trust that a DRM vendor and system will not only support their business rules, policies, and interests, but also do so in such a way that remains under their control. Adopting an effective DRM system that manages rights clearances and payments can make extra time available for developing new products and delivering them in new and different ways (DCITA, 2003).

Introduction to DRM

"Digital rights management" is the term for new business trust assurance processes designed to unleash the tremendous capabilities of the Internet. DRM is fairly new, but the business challenges it addresses are many centuries old. If the Internet is considered as the latest invention that has disrupted established markets, then DRM is the latest solution for reestablishing equilibrium for opening up lucrative new sources of revenue for market participants. DRM becomes essential anytime digital information is deemed important or sensitive enough to be protected by laws, rules, or policies (Coffee, 2003).

There are several well-known definitions of DRM. Slowinski (2003) defines DRM as "a set of actions, procedures, policies, product properties and tools that an entity uses to manage its rights in digital information according to requirements." The Association of American Publishers (2004) defines it in two different definitions, "the technologies, tools and processes that protect IP during digital content commerce" and "the technology, legal and/or social mechanisms used to protect the copyrights in digital content." According to Einhorn (2001), "DRM entails the operation of a control system that can monitor, regulate and price each subsequent use of a computer file that contains media content, such as video, audio, photos or text." Lyon (2001) defines DRM as "a system of information technology components and services that strive to distribute and control digital products."

Open eBook Forum (2000) describes DRM as:

the definition, protection or enforcement of rights pertaining to content produced, delivered or accessed electronically." Finefrock (2000) characterizes DRM as a process involving the safekeeping and copyright protection of e-books, while the American Library Association (2004) defines DRM as a term used for technologies that control how digital content is used. Finally, the Information and Communications Unit of the European Commission Directorate General Information Society (2002) defines DRM systems as "technologies that describe and identify digital content protected by IPR and enforce usage rules set by rights holders or prescribed by law for digital content. DRMs are thus an important complement to the legal framework.

DRM historically has been viewed as the methodology for the protection of digital media copyrights. In more formal terms, 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 rights holders' relationships. It identifies the rights and rights holders associated with particular works and keeps track of their use. For publishers, more complex DRM systems can record, track, and monitor rights for a range of existing and newly created materials. The content will be protected by security features that are unlocked after agreements for use have been reached and payment made.

Generally, DRM systems make use of at least two security techniques, cryptography and identification techniques, to protect and detect the content from unauthorized access and to link DRM-protected content to a seller (Jonker, 2004). Encryption is a protection method that scrambles the information embedded