Bulletin of Applied Computing and Information Technology

DRM systems: A comparative study of protecting owner and consumer rights

03:02
2005, Jul

Podder, B. (2005). DRM systems: A comparative study of protecting owner and consumer rights. *Bulletin of Applied Computing and Information Technology*, 3(2). Retrieved June 2, 2015 from http://www.citrenz.ac.nz/bacit/0302/2005Podder_DRM.htm

Abstract

The objective of Digital Rights Management (DRM) systems is the distribution of digital content in a manner that protects the rights of the content providers, distributors and consumers involved in the supply chain. Some studies supporting DRM systems have noted its success in maintaining the provisions of copyright law and have proposed mechanisms for enhancing owners' controls over digital content. On the other hand, some studies have highlighted the failure of DRM systems to protect *privacy* rights and maintain the *fair use* rights of consumers. Some of these studies have proposed solutions to protect those rights and others have recommended redesigning existing DRM systems. This study examines various protection systems that support DRM systems and identifies DRM systems as partially successful in protecting owners' rights but fail to preserve consumers' interest and thus, create a great deal of conflict between consumers and owners. In order to reduce the conflict, this study proposes changes that might benefit all parties involved and might also help system designers to understand the issues related to 'piracy', '*fair use*' and 'privacy'.

Keywords

Digital Rights Management, DRM, copyright, piracy, privacy

1. Introduction

Digital content distribution is an emerging e-business activity on the Internet. The advent of mobile networks and the availability of higher bandwidth supply consumers with faster access to digital content independent of location. Digital music, streaming video and e-books are becoming popular and important in terms of revenue generation. While there are several advantages to digital content management, such as minimal cost of reproduction, low cost of customization, marginal inventory or storage cost, faster delivery and lower initial business entry costs (Chellappa, 2000), there are disadvantages as well.

From the content owners' perspective, one of the key problems with digital content is that it is easy and inexpensive to make copies without losing quality, it can be altered and distributed to a large number of recipients, which could cause loss in revenue. Further, the freedom of the Internet has created a culture in which the consumers believe that contents that are available over the Internet are free for use and any restriction to content access is therefore considered as loss of their freedom which should be resisted (Lifshitz, 2003). This freedom and the nature of digital content have fuelled unauthorised replication of intellectual assets for commercial purposes. In fact, most content providers have not been able to make any profit from their presence on the Web so far (Fetscherin & Schmid, 2003). More than US$ 14 billion was reportedly lost due to world piracy in software and music in 2001, out of which losses claimed by the music industry amounted to US$ 4.3 billion while US$ 10 billion was lost by the software industry (Wijk, 2002). In 2003, one of the largest electronics makers, posted a huge loss ($160 million in three months) due to piracy (Liu, Safavi-Naine, & Sheppard, 2003). Though these losses are calculated on the basis of the estimated reduction in gross revenue rather than on net loss, the figures are still alarming for the digital

content manufacturers and have motivated them to take the initiative to combat copying and file sharing by implementing various protection measures within a framework.

Digital Rights Management (DRM) systems promise to offer a framework for the distribution of digital content from the producer to the consumer in a manner that protects the rights of all parties even when the content remains with the consumer. Although the current DRM systems have the capability to control piracy but function like proprietary technology. It has limited scope and flexibility: unable to manage access rights to different types of digital content across different platforms, unable to maintain copyright limitations and has failed to protect consumers' privacy. Lifshitz, expresses it this way, " *DRM technologies work like chemotherapy against cancer, which kills good cells along with the bad ones*" (2003).

The legal dimension of the protection regime continuously evolves by the sanctions of new legislation or by introduction of new terms in contracts or in licenses. For instance, the Digital Millennium Copyright Act (DMCA) has been introduced in the USA to prohibit the circumvention of technological protection measures, which means if a consumer bypasses the technological protection measures and produces an illegal copy, he/she violates the DMCA. So far the technical dimension of the protection regime has been able to make copying difficult to frustrate imitators, which is like creating a "speed bump" within the copy mechanism (Anonymous, 2002). According to Felten (2002), no one technology can prevent unauthorized copying of digital files On the other hand, Wijk (2002) argues that copy protection is controversial, as it deprives copying for 'fair use' and thus overrules the limitations of the copyright act.

In current DRM systems, once a user downloads digital content from the web and receives the access rights file from the licence-house and starts using the content, the content provider can monitor the user's activities through the cookies stored in the consumer's computer. Further, content providers collect user information for traffic modelling, infrastructure planning, quality of service enhancement, risk management and for statistical sampling. In both these instances (monitoring access and collecting data), there are risks of personal information being leaked , which might affect the life-cycle of the organization / consumer radically. For example, the merger of *DoubleClick* and *Abacus Direct* indicates the privacy implications when outsiders have access to corporate data (Catlett et al., 2001). Forrester's survey (1999) found that 90% of the online consumers in the USA want the right to control how their personal data is used after it is collected and 83% of the consumers would stop doing business with a company if that company misused their information.

From the literature review, it is understood that DRM systems implementation has given rise to two opposing positions: the owners of copyrighted products attempt to control piracy by eliminating the 'fair use' limitation of the copyright act, they argue that the limitation was intended to encourage consumers to 'try before buying' and is therefore temporary. On the hand, consumers consider 'fair use' as their right and thereby DRM systems must allow this freedom. On one side there is the property right and on the other side there is the right to freedom - these two opposing positions have diminished the prospect of digital media, causing increases in price and thus have failed to achieve the objectives (Lifshitz, 2003).

This article is organized as follows: section 2 illustrates functionalities of DRM systems, section 3 reviews theoretical background, section 4 describes possible solutions to reduce the controversy, and in section 5 conclusions are presented.

2. DRM Technologies

DRM systems are aimed at increasing the scope of control that content owners can assert over their intellectual property assets. The access rights file in DRM systems, is therefore separated from the content file to facilitate providers with greater flexibility in content distribution and management of access to the contents.

Although different DRM systems vendors have different implementations, the central functionality remains the same (Liu et al., 2003) and involves four parties : the content provider, the distributor, the clearinghouse and the consumer. The content provider

encrypts the digital content and transfers it to the distributor. He also forwards a digital license that contains decryption keys and usage rules to the clearinghouse. On the other side, a consumer downloads the content from the distributor's web site and requests a licence from the clearinghouse. The clearinghouse verifies the consumer's identity, checks account details and other related information and, if it finds it valid, charges the user's account and delivers the license. The clearinghouse generates reports for the content provider and distributor. The consumer decrypts and uses the content according to the usage rights as set out in the digital license.

Most of the DRM systems available today rely on single identification of consumer devices so that a license taken for a particular device cannot be transferred to another device. This reduces the impact caused by system attacks but creates an interoperability problem. In order to prevent copying of protected content, a special analogue protection system (e.g. serial copy management system) and a digital watermarking technology (e.g. copy generation management system) are used to make copying difficult. Some DRM systems use watermarking in their 'try-before-buying' model, where inferior quality contents are provided for consumer's evaluation. Further, DRM systems employ various techniques for identifying consumers and monitoring their usage policy and can revoke licenses and/or disable compromised devices. By employing 'audio fingerprinting' or 'robust hash' technology, DRM systems can block access to pirated contents (Bechtold, 2001). A summary of different components and protection technologies is given in Table 1 (Fetscherin & Schmid, 2003).

Component	Description / Protection Technologies
Access and Usage control	Controls who has access to the content and how content is used Protection: symmetric and asymmetric encryption, password
Protection of authenticity and integrity	Protects the authenticity and integrity and integrity of content Protection: watermarks, digital signature, digital fingerprint
Copy-detection	Searches network for illegal copies Protection: watermarking, search engines, traitor tracing

Table 1: DRM system protection technologies (Fetscherin & Schmid, 2003)

In addition to the above technological protection, legal provisions have been made to protect DRM systems. The Digital Millennium Copyright Act (DMCA) passed in 1998, which prohibits any attempt to create and distribute tools that can be used to circumvent the technological protection measures of DRM systems. The security system standards and certification act (SSSCA) is a draft bill for law, which will make it compulsory for the digital device manufacturers to produce devices with built-in DRM system functionalities. Two more laws have been passed: the European Union Copyright Directive (EUCD) and Copyright Amendment (Digital Agenda) Act (DACA) in line with the DMCA. The EUCD is more stringent than the DMCA and DACA ,while the latter has more exemptions (Liu et al., 2003).

As above, content providers can use contracts to compel consumers to use content in a particular manner. Such contracts may include usage terms to protect content as well as the DRM systems. These usage terms of contracts are expressed as metadata for controlling the access of content, which means contractual terms can be controlled by the law as well as by technology. If a consumer alters metadata, he/she would be violating legal protection (the DMCA) of the technological protection (metadata) of the contractual protection (contract). Further, DRM systems providers issue licenses to the manufacturers of electronics devices on the condition that the interest of content providers is maintained (Bechtold, 2001). Technologically DRM systems are protected by legal means i.e. by anti-circumventing regulation (DMCA) which itself is protected by technological protection i.e. by metadata. Further, metadata is protected by contracts and the contract is protected by technology licenses. In summary, various means of inter-related protection mechanisms support the DRM systems.

3. Literature Review

The debate on DRM systems' effectiveness in protecting the owners and consumers rights can be viewed from two opposing perspectives: the owners attempt to control

the piracy by eliminating 'f*air use*' while the consumers consider '*fair use*' as their right. Furthermore, the consumers are worried about the protection of personal information within DRM systems.

3.1 Piracy

Weintraub (2001), Carroll (2002), Russ (2001) and others state that DRM systems are the best solution for combating digital piracy, but Stamp (Stamp, 2003) criticises the level of protection employed by DRM systems, saying it is weak and has been broken several times in the past. The weak point in copy protection is the absence of industry-wide consensus on a technology standard (Iannella, 2001; Wijk, 2002). Attempts have been made to develop such a standard but have failed mainly due to parallel interests of the stakeholders and lack of initiative by the parties involved. For example, the Secure Digital Music Initiative (SDMI) has failed due to opposing interests of the industries involved. Another attempt was made by the Internet Streaming Media Alliance (ISMA) consortium and has so far succeeded in publishing the technical specification for interoperable media streaming based on open-standards technology (Lifshitz, 2003).

In an attempt to identify the source of piracy in the film industry, researchers (Byers, Cranor, & Cronin, 2003) identified that in 77% of cases, the source of unauthorised copying of movies was from inside the industry. Researchers, therefore, suggest that implementing DRM systems in the film production and distribution processes to secure the inside environment is difficult but distinguishable due to a smaller number of people involved, while securing the consumers' environment is nearly impossible. An empirical study (Fetscherin & Schmid, 2003) on music, film and print industries found that the film and print industries believe DRM systems would be able to reduce the piracy while half of the respondents from the music industry opined the reverse. Lifshitz (2003) indicates that DRM systems should reduce the extent of piracy as long as the content price is low, while Poddar (2003) highlights two exogenous parameters of piracy: consumers' reliability on pirated products and strictness of policy to mitigate piracy. In another study Chellapa (2000) indicates that the demand for digital product cannot predict piracy and the quality of digital products improves in the absence of piracy while quality diminishes with the increase of piracy. Code obfuscation is used for protecting software against reverse engineering where program codes at the source or at the object level is altered deliberately to make copying difficult. Cronin (2002) proposes media obfuscation like '*laserlock*', which can be used to prevent piracy in software distribution.

3.2 Fair Use

Fair use serves a critical role in limiting the rights of copyright owners and prevents them from misusing their rights in order to suppress legitimate competition. 'Fair use' provides a platform to spur innovation. For example, innovations in VCR, which allow consumers to copy their favourite programmes and view them at their leisure. Similarly the music industry is fuelled by use of 'space shifting'. In other words, fair use enables the public to make use of copyrighted works. Lohman (2002) express the view that without fair use doctrine, many activities would be infringing such as: "*public performance - whistling a tune while walking down the street, reproduction-photocopying an article for reference, quoting from a novel in a review*". He also suggests that DRM systems must leave room for the above unauthorised use of copyrighted work in order to preserve fair use in lots of tradition forms.

Stamp (2003) states that it is difficult for any computerised system to distinguish 'fair use' from others and therefore DRM systems might be working in favour of copyright holders at the expense of consumers. In 1984, the case between Sony Corp of America v. Universal City Studios in the manufacturing of 'Betamax' VCR, the U.S. Supreme Court ruled in favour of Sony Corp, stating that the owner's right to protect copyrighted work is limited: any users may reproduce copyrighted work for 'fair use' (Benton, 2004). In 2000, another case between A&M Records, Inc. and Napster, Inc. the court ruling allowed MPEG3 copying for 'fair use'.

3.3 Privacy

Most works on privacy to date have focused on theoretical research and the rest have not been tested in large-scale deployments. Even standard software solutions are not available because information considered private may differ substantially from person to person and developing a single solution covering all aspects is next to impossible (Feigenbaum, Freedman, Sander, & Shostack, 2001). Studies (Cavoukian, 2002b; Feigenbaum et al., 2001; Liu et al., 2003) recommend not collecting extra personal information that may not be required for controlling the content and, if it is collected, it should be with the consumer's consent. Moreover, privacy considerations should be inherent in the design of DRM systems rather than added externally and must give equal importance to intellectual property.

Studies have proposed certificate-based protection but none of them could address the privacy related issues successfully (Conrado, Kamperman, Schrijen, & Jonker, 2003). Although there is some benefit to using a single certificate for different purposes, users' privacy cannot be ensured (Conrado et al., 2003). In another study (Aura & Ellison, 2000) "SPKI certificates" are proposed, which provide some degree of privacy but create a burden on the consumers and the content providers to keep track of temporary and task-specific keys. Furthermore, certificate-based solutions are open to technical attacks, difficult to integrate with other content-distribution infrastructure and sometimes have high costs. An identity-based rights distribution and management system, which enables users to access content from anywhere, anytime and on any device by means of authorization certificates issued by the content provider and without compromising on their privacy (Conrado et al., 2003). But no practical test is performed.

4. Success of DRM SYSTEMS: Discussion and Recommendations

The success of DRM systems can be achieved if the tension between the consumers and owners is diminished. In other words, if piracy is controlled, 'fair use' is implemented and 'privacy' is protected, DRM systems will then be successful. But in reality it would be a Herculean task to achieve. Despite support from various inter-related means of protection, the owners of copyrighted products cannot totally rely on DRM systems as technological protections have been defeated in the past and legal protections can be unenforceable for various reasons; the major reason being the Copyright Act, which has not been implemented uniformly in the world. Content providers, therefore, urge the enhancement of the protection capabilities of DRM systems so that piracy can be controlled effectively (Fetscherin & Schmid, 2003). On the other hand, adoption of DRM systems by the consumers remains doubtful without the 'fair use' privilege and privacy protection mechanism. Furthermore, there is no valid reason found in the literature for eliminating the copyright limitation, this study, therefore, supports the views of researchers (Bechtold, 2001; Liu et al., 2003), who posit that DRM systems may require mechanisms to allow public access and reuse privileges equivalent to those deemed fair in copyright protection.

4.1 Enhancing Piracy Protection

DRM systems provide various inter-dependant technological and legal protections where, if any of the protection fails, another means of protection walks in to support the overall protection of the system. There are seven major protection technologies that support DRM systems. These are: encryption, password, watermarking, digital signature, digital fingerprint, copy detection system and payment system. A study (Fetscherin & Schmid, 2003) of protection mechanisms used by film, music and print industries identified 90% of film, music and print industries use password protection while 60% use encryption and payment protection mechanisms . But when the respondents were asked to evaluate the protection value of each system, password was polled as the least important protection mechanism (Feigenbaum et al., 2001).

The figures above indicate that the content providers who use low valued protection mechanisms need to upgrade their protection technologies to fight against piracy. They must plan to implement protection technologies that have higher protection values and must refrain from using password protection mechanism, since it has the lowest

protection capabilities. But over-protection will make content usage difficult and might discourage consumers from buying. So "*the goal must be having the right technique at the right place for the right products - as strong as needed but as weak possible*" (Fetscherin & Schmid, 2003). Several studies suggest including value added services within DRM systems to reduce the impact of piracy but Fetscherin and Schmid (2003) indicate that value added services like quality of service, additional content, customer support and superior quality does influence the impact of piracy.

Apart from enhancing technological protection to control piracy, a global convention is needed to educate consumers to respect intellectual property and also to make them aware that what they are paying is the royalty not the tax, which they do not want to pay generally. Moreover their payment goes to benefit the creator rather than the merchants, agents and Governments. Reduction of content price might reduce the motivation of piracy (Lifshitz, 2003). Further, DRM systems should be transparent and undisruptive to the consumers who purchase the content while at the same time making content as difficult as possible to freely pirate. Also, purchasing content should be as straight forward as purchasing a physical product from a regular store.

4.2 'Fair use' Limitation within DRM Systems

In order to benefit creators with an incentive to make their works available to the public, the Copyright Act grants exclusive rights (reproduction, distribution, public performance and display) to its creators. However, copyright protection has never been unlimited; '*fair use*' is protected and loosely defined by Section 107 of the Copyright Act. It states that *for the purposes such as criticism, news reporting, teaching and research, copyrighted products can be used without the permission of the creators*. In other words, it is an unauthorised reproduction of copyrighted work for which holders cannot claim any compensation from the consumer (Mulligan, Han, & Burstein, 2003). It is an automatic permission given for a specific use where forming a contract between the owner and consumer would have been costlier than the cost of the transaction. Another reason for this limitation might be for reconciling the social welfare losses; the underproduction and the underutilisation caused by higher product costs (Bechtold, 2001). Depending upon the interpretations of 'fair use', different views appear in the literature regarding implementation of the 'fair use' limitation in DRM systems.

An algorithm-based solution for '*fair use*', as formulated in current copyright law, is unlikely to be incorporated within DRM systems since '*fair use*' is irreducibly situation specific and it would be too optimistic to think that DRM systems designers will be able to anticipate the range of access privileges that may be appropriate to implement 'fair use' rights for a particular work. Thus, building automated mechanisms for 'fair use' into DRM systems would be a complex and expensive affair (Bechtold, 2001). However, in order to reduce divergence between the owners and consumers, the author proposes some changes to be incorporated within current DRM systems and these are discussed in the following sub-sections.

4.3 Changes in Technology Design

Allow copying : DRM systems should allow consumers to make a certain number of copies for private or educational purpose without seeking permission from the owner of copyrighted products (Bechtold, 2001; Mulligan et al., 2003) but only for a limited period of time and they must be asked for the consumer's authentication during every copying activity (Mulligan et al., 2003).

Allow transfer of rights: DRM systems should allow the subscriber to share a restricted copy of work with friends or with others for non-commercial use on a condition that the subscriber cannot use the content while it is being borrowed. Further, the subscriber must be allowed to use copyrighted products on devices other than his / her own device (Bechtold, 2001; Mulligan et al., 2003).

Allow quoting and modification: DRM systems should allow conversion and quoting from copyrighted content, except for the software sector where reverse engineering is not permitted. DRM systems designers can set limits on the quote file size or on the rate of quote creation in order to discourage piracy. Further creation of original content by

combining consecutive quotes can be tackled by inserting delays after every quote - this might discourage piracy indirectly, specially in the music and film industries (Mulligan et al., 2003).

4.4 Limiting Anti-Circumvention Law

DMCA was introduced to prevent circumventing of technological protection measures but has outlaw uses that are lawful under copyright law. Although DMCA is limited by several exceptions, yet benefiting from an exception is not possible because bypassing protection tools are required to be created, which is not authorised by the law and thus makes the exceptions meaningless (Bechtold, 2001). Bechtold (2001) suggests that the legislator could refute the protection by DMCA in certain cases where it opposes copyright law.

4.5 Third Party Escrow

Under this approach, consumers would not be allowed to develop or distribute tools to circumvent the technological protection of DRM system to achieve benefits from a limitation to DRM systems protection, rather an independent third party would be trusted to provide consumers with the necessary tools. However, there are some issues in such a type of arrangement that need to be addressed by the content providers such as: setting up such an arrangement depends upon the nature of distribution of the content. For example, if a provider wishes to offer content over the Internet with a condition that consumers must sign a contract to access the content, then establishing an escrow arrangement does not have any significance. Further, under the escrow arrangement, consumers will be required to contact the third party in order to obtain the appropriate circumvention tools and since there will an additional cost for every transaction that the consumer makes, consumers might opt not to use the content (Bechtold, 2001).

4.6 Separate Act for Digital Products

DRM systems can be considered as a means of protection of the intellectual property rights for digital products alone and can be designed from a different perspective since the copyright act is designed to protect the intellectual property rights of physical content, which differs from digital contents in many ways. From a business perspective, digital product has the following features: cost of reproduction is negligible, no storage cost involved, minimal distribution cost and no buy-back policy. Considering these aspects and also the social benefits, content providers can alter content prices in a manner that motivates the legal usage and also includes consumers who had been left out due to higher prices (Sundararajan, 2004).

Another proposal also found in the literature, where researchers advise content owners to price the products in such a way that the value of content diminishes with time and after a certain period of time any consumer will be able to use it for free. The 'fair use' consumers would be required to wait till the product becomes free to avail themselves of the privilege of copyright law. But there are issues like future maintenance costs and setting the time limit for content to be available freely, that need to be studied further.

4.7 Privacy Protection

Privacy enhancement should be at the core of DRM systems design, so that consumers are not required to take additional care. DRM systems should adopt fair information principles (FIP) (Willis, 1973), which is a commonly used framework for examining information-collection practices in privacy-sensitive areas. Business costs for introducing FIP into DRM systems and consumer costs for using privacy-enhanced DRM systems must be low and the system should be easy to use (Feigenbaum et al., 2001). DRM systems providers should escrow the collection of data that is not required for content protection or destroy the portion of data that will not be used in future (Mulligan et al., 2003). However, consumers should be advised of the purpose of data collection and its usage. Finally, providers must assure consumers that intellectual preferences will not be recorded and guarantee that data will be used only for an

agreed purpose (Mulligan et al., 2003) by implementing contractual licenses or privacy enhancing technologies (Bechtold, 2001).

Studies propose several frameworks and models for implementing user's privacy into DRM systems and among these proposals, recommendations by Cavoukian (2002a) to implement the privacy framework proposed by the Privacy Commissioner of Ontario, is found to be comprehensive. The framework suggests seven steps to be followed to undertake privacy analysis of any technology. Cavoukian (2002b) describes how those steps can used to embed privacy into DRM systems. Further, in step number five, the author suggests building privacy into DRM systems as proposed by Kenny and Korba (Korba & Kenny, 2002). But Kenny and Korba's work is based on the requirements of European Union data protection legislation and thereby can be applied only in European countries. There are techniques to determine geographical location, but authors (Korba & Kenny, 2002) have doubted their reliability. Moreover, electronic implementation of privacy laws is not uniform which helps in making decisions when privacy requirements differ. Detailed studies are required to examine how the requirements of other countries can be embedded within DRM systems.

5. Conclusion

DRM systems are supported by the technological and legal means to protect systems. These protection systems are interrelated in such a manner that if one of the systems fails or is circumvented by a consumer, another means of protection comes to rescue the overall protection of the DRM system. Such 'hyper protection' systems might enable the owners of copyrighted products to exercise their rights and will encourage them to develop and bring new products to the marketplace. But the question is 'Will the consumers accept the DRM systems?' The success of DRM systems equally depends upon the consumer's acceptance along with its protection capabilities. Criticism of DRM systems' incompatible platforms, dilution of fair use rights and silence on the consumer's privacy rights have already raised an alarm that consumers might not value DRM systems. Proponents of such views suggest that limiting the protection of DRM systems is not required since users will not buy them.

This study discusses the issues relating to piracy, 'fair use' and 'privacy' at length and proposes possible solutions that could be considered while developing and implementing future DRM systems. It is apparent that the proposed changes would be difficult, if not impossible; to incorporate within the current DRM systems because the means of protection are interlinked and changes to any protection system needs to be validated by the other protection systems.

Further studies can be carried out on how to implement the recommendations made in this paper. This study focused only on the issues that have arisen in maintaining the Copyright Act digitally. The technological development of DRM systems is yet to completed and problems in the areas of security, integration with existing systems and interoperability, still remain to be addressed.

How DRM systems and the law will interact will depend heavily on decisions made in the near future by organizations in the technology and content industries, legislators, participants, and other policymakers. DRM systems are not unbiased because of the interest of the content industry.

Acknowledgement

The author wishes to thank Catriona Carruthers for the thorough editing of the article in terms of style, language and grammar - which greatly improved the overall presentation and readability.

References

Anonymous. (2002). A speed bump vs. music copying. *Business Week online*(January 2002).

Aura, T., & Ellison, C. (2000). *Privacy and accountability in certificate systems*. Helsinki: Helsinki university of computer science.

Bechtold, S. (2001). From copyright to information law implications of digital rights

management. *Implication of Digital rights management*(June 2002), pp. 213-232.
Benton, L., G. (2004). The Digital Millennium Copyright Act: The Digital Copying War Between Hollywood and the Silicon Valley. *Coudert Brothers LLP*(February 2004).
Byers, S., Cranor, L., & Cronin, E. (2003). *Analysis of security vulnerabilities in the movie production and distribution process*. Paper presented at the DRM '03, Washington, USA.
Carroll, J. (2002). Who's afraid of Digital rights management. *SDNet Australia*.
Catlett, J., Rotenberg, M., Banisar, D., Mierzwunski, E., Chester, J., & Givens, B. (2001). *Open letter to Kevin Ryan*. Retrieved 10/04/2004, 2004, from http://www.junkbusters.com.
Cavoukian, A. (2002a). *7 Essential Steps for Designing Privacy into Technology*, from http://www.ipc.com.
Cavoukian, A. (2002b). Privacy and digital rights management (DRM): an oxymoron. *Information and privacy commissioner*(October 2002), pp. 1-16.
Chellappa, R. (2000). Digital Products and e-business. *The Magazine of the Marchalll school of business*, 7.
Conrado, C., Kamperman, F., Schrijen, G., & Jonker, W. (2003). *Privacy in an identity-based DRM system*. Paper presented at the 14th International workshop on database and expert systems applications (DEXA'03).
Cronin, G. (2002). *A Taxonomy of methods for software piracy prevention*. Retrieved 20/03/04, 2004, from http://www.croninsolutions.com
Feigenbaum, J., Freedman, J., M, Sander, T., & Shostack, A. (2001). *Privacy engineering for digital rights management systems*. Paper presented at the ACM Workshop in Security and Privacy in Digital Rights Management, 2001.
Fetscherin, M., & Schmid, M. (2003). *Comparing the usage of digital rights management systems in the music, film and print industries*. Paper presented at the ACM, ICEC 2003.
Iannella, R. (2001). Digital Rights Management (DRM) Architecture. *D-Lib Magazine*, 7, pp. 1-10.
Korba, L., & Kenny, S. (2002). Towards Meeting the piracy challenge: Adapting DRM. *National Research Council of Canada*, NRC 44956, pp. 118-136.
Lifshitz, Z. (2003). *Digital Rights Management - a zero-sum game?* Paper presented at the Eurocon 2003, Ljubjana, Slovenia.
Liu, Q., Safavi-Naine, R., & Sheppard, N. (2003). *Digital Rights Management for content distribution.* Paper presented at the Australian Computer Society Inc, Adelaide, Australia.
Mulligan, K., D, Han, J., & Burstein, J., A. (2003). *How DRM-based content delivery systems disrupt expectations of "personal use"*. Paper presented at the DRM '03, Washington, USA.
Poddar, S. (2003). *On the Software Piracy when piracy is costly*. Singapore: National University of Singapore.
Release, N. (1999). *Forrester Techno-graphics finds online consumers fearful of privacy violations*, from http://www.forrester.com
Russ, A. (2001). Digital Rights Management Overview. *Security Essentials*, v1.2e, pp. 1-11.
Stamp, M. (2003). Digital Rights Management: For better or for Worse? *eWeek*.
Sundararajan, A. (2004). *Managing digital piracy: Pricing and protection strategies*. Paper presented at the Second annual congress of the society of the economic research on copyright issues, New York,USA.
Weintraub, A. (2001). Content Management providers: Timetable towards DRM. *Gartner Group*, M-13-7071(July 2001).
Wijk, V., J. (2002). Dealing with piracy: intellectual asset management in music and software. *European Management Journal*, 20(6), pp. 689-698.
Willis, W., W. (1973). *Records, computers, and the rights of citizens*.

Krassie Petrova, Michael Verhaart & David Parry (Eds.)
An Open Access Journal, DOAJ # 11764120 , (✓zotero)