International Review of Law Computers & Technology, Volume 19, No. 3, Pages 235–252, November 2005

Routledge
Taylor & Francis Group

Does Lessig's Criticism of Digital Rights Management Target One Technology That the Information Industries Desire More Than They can Actually Provide?

YU-LIN CHANG

ABSTRACT *According to Lessig's idea of 'code is law', digital rights management (DRM) is seen as a technology with perfect control and has great potential for offering persistent and permanent protection for the digital content that information industries own. Moreover, some consider that DRM is powerful enough to replace copyright law in protecting digital products. Clearly, such a conclusion about DRM is problematic. As we know, perfect control is impossible because no technology is 100% secure. Some circumvention cases can provide evidence of this. Paradoxically, Lessig's criticism of DRM seems to have come true. Backed up with the force of anti-circumvention provisions, although there are lots of technological flaws and ongoing legal arguments, DRM has been one technology that information industries desire more than they can actually provide.*

Introduction

Do you fear someday not being allowed to use the materials in the library for free, to browse the books of shelves in a bookshop at will, to make several copies of the compact disc (CD) you bought for enjoying them in your car and in your office, to record the film on the television to watch it later or to collect information on the Internet for the purpose of research and education? According to Lessig, with the emergence of the copyright management scheme now better known as 'digital rights management' (DRM), whatever we have taken for granted will soon be impossible.

Correspondence: Yu-Lin Chang, School of Law, Queen's University of Belfast, Belfast BT7 1NN, UK. E-mail: ychang03@qub.ac.uk

ISSN 1360-0869 print/ISSN 1364-6885 online/05/030235-18 © 2005 Taylor & Francis
DOI: 10.1080/13600860500348028

Since publishing the book *Code and Other Laws of Cyberspace* in 1999, Lessig's idea of 'code is law' has given rise to lots of scholarly discussions. His criticism draws our full attention to concern about the dark side of the Internet while we are enjoying its convenience. Lessig reminds us that what a cyberspace composed of programs means is not openness, but control. The Internet of the past was a place the libertarian desires: however, now, through software, commercial interest will absolutely control the Internet with the support of governments. At worse, code writers dominated by corporations such as Microsoft are seen as lawmakers because their code can make the Internet what they desire and regulate what people can and cannot do according to the commercial purpose.

In the context of intellectual property, Lessig takes, for instance, the trusted system, one of the most important technologies of the DRM system, for proving how perfect a tool of control the DRM technology is. As the combination of the DRM solution and click-wrap licence becomes the primary method of purchasing digital products, although originally DRM was designed for the purpose of preventing against rampant online piracy, it also has great potential for offering persistent and permanent protection for the digital content. In this regard, Lessig worried whether it will become an uncontrollable monster that enables the information industry too much control over the information markets in a completely unregulated environment.

Followed by the Lessig's criticism of the trusted system, this paper tries to look at what the DRM technology really is, how it works and what it impacts on. Initially, the first section is aimed at offering an overview of the nature and emergence of DRM and its application in the information industries. Next, by discussing access rights, fair use and technological standards, the DRM technology will be further examined as to how it enables the information industry, with the temptation to maximize private interest at the expense of public interest. Finally, the analysis will lead to a conclusion that DRM has the ability to work as a technology that information industries desire rather more than they can provide mainly due to anti-circumvention provisions.

Digital Rights Management

The Nightmare of Information Industries: Online Piracy

As the world economy shifts from a manufacturing-based economy to a service-based economy, the importance of information increases.[1] Traditionally, information has been stored in physical form and physically delivered. With the development of new technology more and more information is available in electronic form. Digital information products have become a valuable commodity that provides information industries with the means for exploiting new business opportunities with access to a new system of wealth and leads to the dimensions of the knowledge game.

This is different from the traditional retail market where free-riding is virtually more difficult because the seller can use physical dominion over the goods for controlling distribution.[2] However, digital information productions, by the click of a mouse, can be easily copied and distributed without degradation in quality or quantity. Furthermore, the Internet makes it possible to copy and distribute anything rapidly, anonymously and undetectably.[3]

The features of digital information, non-rivalry and non-exclusivity, enable the customer to misappropriate without the compensation. According to the research undertaken

by Seybold, which carried out a survey amongst publishing industries, more than three-quarters of survey respondents downloaded software applications, articles and images. However, no more than one-third of the respondents paid for the use because consumers are used to downloading digital content for free.[4]

Apart from small-scale and unorganized copying from individuals, information industries are also worried about the duplication of their copyrighted work created by organized crime at a lower cost due to a lack of start-up investment or by the hacker, whose behaviour can cause copying of Napsterization effect. In particular, the latter will result in the damage of break once, break everywhere.[5] According to Schneier, secure measures work against average users, but not hackers. Once a hacker successfully creates a program to break the secure measure and makes it available on the Internet, then average users can use it to defeat the secure system. As a result of available break tools, the average user is as good as the hacker at accessing the unauthorized content.[6] Clearly, online piracy has become a potentially terrible nightmare for the information industry.

Of all information industries online piracy presents the greatest challenges to music industries. Link sites offer lots of lists of hyperlinked file names for downloading, thereby infringing files from other servers. Hacking sites teach users how to break the technological measures applied to copyrighted materials.[7] The free file-sharing services further facilitate unauthorized copying of music files. It is estimated that, in 2002, approximately 500 million pirated music files were available on free-sharing services.[8]

The Motion Picture Association of American (MPAA) also complains that piracy has led to the loss of approximately $3 billion annually, not including the Internet piracy losses.[9] While enjoying the new revenue from the rental of cassettes, video cassettes and digital video discs (DVDs) motion picture industries originally were not much worried about the piracy issue because, different from music, converting films into digital format calls for much more storage space and good network connections. However, with the improvement in network technologies, including compression, broadband and cheap digital storage, motion picture industries have also started to face the Napsterized piracy threat that happened with the music industries.[10]

In order to recoup their investment and maintain their competitive priority in the international knowledge game, information industries have developed a variety of legal and business strategies for fighting against online piracy. Apart from enhancing copyright protection, they rely on click-wrap licences to restrict the access of digital content. More importantly, under the DMCA (Digital Millennium Copyright Act), information industries are entitled to use electronic self-help for disabling access in the event of piracy, that is it allows the information industry to fight the piracy technology with technology. In this regard, DRM is no doubt a desirable option for information industries because of its perfect control over access to digital content.

The Emergence of Digital Rights Management

DRM is expected to make an effective increase in the piracy cost by making the access, copying and distribution of material significantly more difficult and inconvenient, with the purpose of protecting high commercial value digital products against unauthorized use. In the new electronic economy, the combination of DRM and click-wrap licences has become the primary method of purchasing digital services and products on the Internet. To date the DRM solution has been mainly applied in the publishing industry,

entertainment industries and the protection of non-copyrightable factual databases. Although the DRM implement may vary from industry to industry, the typical DRM architecture involved in business transactions is similar.

How does DRM work? A simplified process of DRM-secured click-wrap license is that, after filling out the personal information and bill information, the user submits a click-wrap licence in order to order the digital product. If the user passes the authentication, the information industry will place a watermark and usage rules into the product the user bought, encrypt it and then send it to the user. In click-wrap license the information industry usually forces the user to activate a special DRM-enabled device into the user's computer or storage media. While making sure that the user is entitled to use the digital product, the DRM-secured device decrypts the product and then the user can download and use it. If the content is transmitted or copied to a different device, the new usage rule and required payment will again appear for access to the content. As licences and business models change, the DRM technology is also capable of reflecting new relationships and new revenue requirements.[11]

In comparison with conventional technologies used only for preventing and eliminating the unauthorized distribution of digital content, DRM solutions can simultaneously satisfy the requirements for copyright protection, ownership assertion, digital content authentication, access control and secure communications with more flexibility and lower cost. This is because the DRM system is not a single technology, but a collection of coordinated technologies that can detect, track and possibly stop this illegal transmission of digital content.

Authentication, including personal identification and device identification, means a sort of access control for confirming that the content is only used by those authorized and for detecting and excluding the unauthorized.[12] An invisible digital watermark, acting as a monitoring technology, such as the secure digital music initiative (SDMI), is permanently embedded into the digital content for copyright protection and ownership assertion.[13] Usage rules, which are commonly referred to as 'rights', define how the content can be used and are delivered independently from the content.[14] These rights are expressed in a language such as XrML.[15] The encryption is aimed at copy protection and secure transmission by using a 'public key' algorithm for locking up information and making it inaccessible.[16]

On the client side, the special DRM-secured device, such as Adobe reader, can filter the digital watermark of the content for copyright verification and check the Internet provider address information in order to determine the identity of senders and receivers. Once the transmission is found illegal, it can disable the transmission of the unauthorized content.[17] In order to secure the client side, the trusted computing platform (TCP), which was previously called the 'trusted system' by Lessig, is designed to provide a more secure personal computer (PC).[18] This means that a powerful TCP can not only make it hard to run unauthorized software in a user's PC, but also has the ability of remote control for deleting the pirated content found on the user's computer by a remote third party.[19] This is what the revised Windows Media Player attempts to do now, but has caused legal controversy.[20]

According to Bechtold's view, the DRM solutions combined with copyright law and click-wrap licenses constitute an intertwining means of protection for achieving the goal of a continuous level of high security. Typically the user must submit a click-wrap licence before accessing the digital content protected by the DRM technology. In order to make a DRM solution feasible, some terms of such a contract usually force users

to download the content only to particular DRM-secured devices, prevent users from circumventing the technological protection measures used in the DRM system or define the usage rules unilaterally designed by content providers.[21] The enforcement of anti-circumvention provisions of copyright law further puts DRM solutions in a superior position for protecting copyrighted works.

Likewise, the DRM system can be regarded as the guardian for enforcing click-wrap licences. It can reject the transaction until the user agrees all terms of the click-wrap licence. Breach of a click-wrap licence is not only subject to traditional contract law, but also detected by the DRM technology, which can disable any disobedience to the contractual obligations.[22] In addition, this behaviour is supported by the provision of electric self-help under copyright law.

Finally, the absence of global identification standards for DRM technologies curbs the interoperability of different technologies. Although open standards and freely licensable DRM intellectual property are desirable solutions, the expectation has been difficult to implement because a lot of core DRM intellectual property is protected by patents owned by companies such as Sony, Philips, IBM, Macrovision and ContentGuard.[23] InterTrust brought a suit against Microsoft for using its DRM solution in Windows XP: they later settled the patent case for $440 million.[24]

Although some consider that the lack of widely-available standards for computing devices, management engines and general-purpose rights expression language will hamper the industrial development and acceptance of DRM for digital content,[25] the DRM market is in fact developing rapidly. The *MIT Technology Review* identified DRM as one of the top ten emerging technologies that will change the world.[26] In the near future the DRM solution will predictably become a mainstream technology acting as a permanent and integral part of the corporate and Internet infrastructure.[27]

The Application of Digital Rights Management in the Information Industry

As mentioned earlier, the application of DRM ranges from simple copy-prevention technologies to comprehensive secure distribution systems. A robust DRM is expected to support the following.

1. Multiple content types such as video, audio, text and image file formats (MP3, JPEG and PDF).
2. Multiple usage rights such as price, duration, frequency of access, rendering and transfer.
3. Multiple business modes such as rental, paid download, super-distribution, subscription services, time-based access, metered usage, pay-per-view, a site licence, video on demand and free preview.[28]
4. Multiple content delivery models such as streaming, downloads, physical media or peer-to-peer file-sharing networks.

Generally speaking, a DRM solution was first applied by the publishing industry. PDF, for example, is a file format developed by Adobe for representing digital documents on your computers. It had become the *de facto* standard by the late 1990s. Owing to the feature of read-only format, the user, in general, can only print out a PDF document, but not save or edit it without permission. In addition, it needs to be viewed through a reader program embedded in the computer. To date, the most famous and widespread readers used are Adobe reader and Microsoft reader.[29]

The DRM solution was then widely used in the entertainment industries such as music, video, television, radio and the like. Of all information industries affected by the digital technologies, the industry involving the illegal distribution of digital music is affected far worse than others. As a result of fighting the piracy threat, the DRM experience of music industries is of interest to other industries.[30]

The popularity of the MP3 constitutes a free file-sharing network and this impacts heavily on music industries. It is well known that the appearance of the SDMI was in response to the MP3's surprising success.[31] Its goal is to produce a secure music format and trusted devices under which any unlicensed file, including an MP3, would be rejected as pirated.[32]

Interestingly, anything is possible on the Internet. Although eagerly fighting to eradicate the peer-to-peer file-sharing distribution, some music industries have started veering towards embrace it for generating a new business model: 'super-distribution'. It means the multiple distribution of the same content and acts as a post-sale opportunity for generating additional revenues.[33] In the real world, you can buy a CD in a music store and then send it to your friend for sharing the music. However, it is hard to share the music in the digital format under super-distribution. Your friend can still accept the file you forwarded but cannot access it. Usually a new licence will be displayed on their computer and will ask them to pay again for access to the content. Even the authorized user is also limited to use the content under special conditions, such as only listening to a music file on their computer at home, but not in the office.[34]

For motion picture industries annoyed by optical disc piracy such as VCDs (Video Compact Discs) and DVDs, the Content Scrambling System (CSS), an encryption system, is applied in DVDs in order to raise the threshold of difficulty and expense for piracy.[35] Moreover, although not limited to video files, the characteristics of streaming technologies particularly grab a significant market niche in motion picture industries. Streaming technologies developed by RealNetwork, which is famous for its product 'RealPlayer', can sort out the problem of downloaded video files always being out of the control of rights holders. This is because, although the video file is playing on the user's computer, it is never left on the user's computer.[36] Consequently, the user can only view or listen to but not possess the copy of the video file, let alone duplicate and redistribute authorized copies to others.[37] It is also capable of tracking usage habits and reporting the detailed data back to the rights holders. These characteristics allow the information industries to generate pay-per-view revenue.

With the subscription model the publishers of journals, research and reference materials and factual databases use DRM-secured licences for providing subscribers a number of service options in accordance with access permission. As a paid subscriber you can use any service offered by the content provider without limit during a specified period of time pursuant to the price discrimination, but cannot transfer the DRM-enabled content to others.[38] Now, based on the potentially commercial benefit, there are even increasing trends among academic institutions for employing DRM solutions for protecting their assets.[39]

Finally, apart from protecting the flow of content, more and more businesses and governments are also protecting their confidential documents against accidental misuse, malicious distribution or employee theft by using DRM solutions.[40] It is because the leakage of information security will lead to a loss of revenue, competitive advantage, a company's reputation and consumer confidence.[41]

In order to distinguish from the DRM for intellectual property protection, Microsoft has created a new concept of information rights management (IRM) for document security, which is the biggest selling point of Microsoft Office System 2003. For instance, in Outlook 2003 the sender can determine the intended user and the scope of use by means of a 'no forwarding' restriction foundation. The content provider is also capable of granting or altering access permission after the document has been delivered. Even though the confidential document is sent to the wrong people, IRM technologies still enable the content provider to recall and expire unauthorized documents that have been released.[42]

The Legal Controversy of Digital Rights Management

Clearly, in the digital age the pervasiveness of digital technologies has generated two irreconcilable phenomena. One is that the Internet, as a global medium, provides a far-reaching, powerful conduit for digital content and information access, distribution and sales with very low reproduction cost. As a result, information industries can only prevent unauthorized access to unprotected digital content by free-riders with difficulty. On the other hand, DRM technologies are developing rapidly. Based on the robust DRM solution for securing, monitoring and tracking access to any form of digital content, information industries have again made it possible to exclude consumers absolutely from unauthorized access.

As mentioned earlier, apart from preventing unauthorized use, DRM solutions also have the potential for offering persistent and permanent protection for digital content. At present the development of DRM markets is still at an early stage and costs money. Very few content providers, such as large information industries, are capable of applying DRM systems for protecting their productions. This will give large information industries, such as Microsoft, AOL, the MPAA and the Recording Industry Association of America (RIAA), too much control over the information markets in a completely unregulated environment. Therefore, the current dispute about DRM solutions is in fact a battle between individual users and the information industry monopoly. Some worry that a new society of information totalitarianism is looming.[43]

Rather, with the support of DRM technologies, the click-wrap licence enables information industries to exploit business opportunities on the Internet again, which is nothing new in the real world, but this could not work before owing to the network technology with the ability for free file-sharing distribution amongst users. A variety of business models are used for maximizing the value of copyrighted works that information industries own through price discrimination. However, while enjoying the over-protection and additional benefit, information industries' desire for embedding DRM technologies in business models also sparks lots of legal concerns.

Is 'Access Right' a New Author's/Publisher's Right?

Access right is nothing new. Typically, we regard it as the user's right, such as 'public access' in the library service. However, with the support of anti-circumvention provisions, DRM seems to challenge the traditional value of public access.[44]

Under anti-circumvention provisions the access controls of digital content are protected against both devices and acts of circumvention while copy controls are only protected

against devices of circumvention. In addition, the reason not to ban acts of circumventing copy control is that the US Congress intends to leave a door open for the public to continue making fair use copies of copyrighted works. Copy control technology can prevent users from copying or performing the copyrighted work, whereas the access control technology just allows users to view, hear, store or print the work in accordance with special conditions. Clearly, the DRM solution can be seen as a 'merged control' because its technologies, such as encryption, simultaneously qualify both as an access control and a copy control.[45]

Since, under the DMCA, access controls can enjoy stronger protection than copy controls and circumventing a merged control was treated as circumvention of an access control by the Realnetworks[46]and Reimerdes[47] courts, content providers will have an incentive to adopt DRM systems in order to enjoy all the protections of both access controls and copy controls, even though, like the CSS in the Reimerdes case, they in fact mainly serve as controls of reproduction and dissemination rather than access. Therefore, Reese considered that it might undermine the spirit of carefully treating two different types of controls by the US Congress.[48]

On the other hand, according to the US Congress, the anti-circumvention protection is originally expected to function as a shield rather than a sword, that is the provisions are only aimed at passively preventing misuse of copyrighted work, rather than actively extending content providers' exclusive rights.[49] As a result of abusing the technological measures of DRM systems under the protection of anti-circumvention provisions, 'access right' seems to become a new privilege of copyright owners out of the traditional exclusive rights and threatens copyright's balance of rights and limitations.[50] The argument of whether the access right is subject to author's right or user's right arises again.

Ginsburg also considered that, in theory, copyright does not reach 'use'. It is because 'access' is a precondition to 'use', particularly on the Internet. By controlling the former, the content provider has the capacity to limit or condition later use. As a result, copyright holders enjoy far more protection than copyright law now provides.[51] For instance, by streaming of audio or video files over the Internet, the content provider enables the user only to access the content on a 'pay-per-view' basis instead of owning a digital copy. For content providers the 'first sale doctrine' is not a serious issue any more because, under the UCITA (Uniform Computer Information Transaction Act), the DRM-secured contract is deemed as a 'licence' not a 'sale'. No wonder Guth considered that, since the digital content is no longer media-dependent, what the user really purchases has changed from the content itself to usage rights for the content.[52] It further causes new concern whether 'access' right will or should supplant 'copy' right for digital materials.

Based on the protection from DRM technologies, the information industry has the absolute right to control access to and use of works. In order to remain the priority for access control, they are willing to sue for any unauthorized access. DRM-secured contracts usually include the terms with the penalties for the breach of licences. Burk and Cohen worried that it will lead to the focus of the right holder's interest on penalties from unauthorized infringement to penalties from unauthorized access, regardless of whether the content is subject to the public domain.[53] At worst, the recent strategy of information industries is to lobby the government for criminalizing all activities in cases of intellectual property piracy, as section 1204 of DMCA has done.

Moreover, in this regard it is conceivable that distributors of circumvention devices would be at the risk of being sued for contributory infringement at any time because the DMCA's anti-circumvention provisions also prohibit the manufacture and dissemination

of circumvention devices. With regard to this, distributors of circumvention devices would fortunately be much relieved after RealNetworks[54] case, where the decision overrode such a claim because the court ruled that the breach of anti-circumvention provisions is not the issue of copyright infringement. Therefore, distributors of circumvention devices have no liability for contributory infringement.[55]

Moreover, the capability of tracking and prohibiting objectionable uses of information productions enables information industries to build a DRM-based private censorship.[56] Authentication gives rise to the privacy concern, such as anonymous use, data reuse and tracking the demographics and preferences of consumers. The country-coding scheme (geographical identification) embedded into DRM is also applied in order to achieve a filtering of access control.[57] The remote control software enables information industries to delete a pirated file found in a PC remotely.[58]

As to the authentication issue, Konard worried that a new digital divide has emerged between the people who give their consumer data to the vendor and the privacy zealots who refuse.[59] The country-coding scheme undoubtedly puts developing countries further in a difficult position because it enlarges the gap of a two-tier society of information rich and information poor, where only a part of the population with the ability to pay has access to the new technology and can fully enjoy its benefits.[60] If without the user's knowledge and permission, the remote control could be seen as an unauthorized access and is likely subject to a claim of electronic trespass and violation of the US Computer Fraud and Computer Abuse Act while changing something in a PC constitutes a 'damage' to the user.[61]

Does Fair Use Become Fared Use?

The relationship between DRM and the fair use doctrine is another point at issue. DRM has been criticized for hampering fair use because it can control all possible uses of content regardless of whether the use is subject to the fair use doctrine.[62]

Typically the fair use doctrine is seen as a kind of 'free use' under copyright law. However, through DRM-secured contracts information industries have developed new business models, such as subscription, pay-per-use or super-distribution, for charging every user for access to proprietary information. Combined various content delivery modes with price discrimination allow the user to access on a document-by-document basis only after paying the licensing fee.

Furthermore, in the cases of *Princeton University Press* v. *Michigan Document Services, Inc.*[63] and *American Geophysical Union* v. *Texaco, Inc.*[64] the courts recognized the loss of licensing revenue as evidence of economic injury and that it could match the requirement of the fourth factor of the fair use doctrine: 'the effect of the use upon the potential market for or value of the copyrighted work'. The Texaco[65] court even explicitly noted that '…an unauthorized use should be considered "less fair" when there is a ready market or means to pay for the use'. Clearly, the fair use defence will be subject to a system of 'fared use' under a DRM-secured contract.[66] The relationship between free use, fair use and fared use becomes a heated debate again.

Supporters claim that the DRM solution can effectively prevent market failure from free use of the fair use doctrine. Loren argued in general that information has significant external benefits: 'the greater the transformation, the greater the benefit to the storehouse of knowledge or the arts'[67] and this meshes the purpose of fair use. Therefore, the court's decisions, overemphasizing on monetary issues and undervaluing the first factor of the

fair use doctrine, 'the purpose and character of the use', will make it possible to allow information industries to eliminate all fair use as possible. Burk suggested that the copyright misuse doctrine might be employed in preventing broadening the author's right when anti-circumvention provisions seem to have created a new 'paracopyright'.[68]

There is an interesting phenomenon. Bell and Loren both depended on irreconcilable reasons in reaching the same conclusion: fair use will no longer exist soon. According to Bell's view, fair use originally existed as a response to market failure resulting from undue copying. Fair use should be given away when the DRM solution can effectively protect an author's right against the infringement of copyright.[69] Conversely, Loren explained that fair use exists on the basis of another market failure resulting from the high transaction or negotiation cost between users and content providers, that is the content provider cannot sue everyone for infringing their copyrighted work, so they tolerate some unauthorized use. Loren pessimistically considered that fair use could not survive because there is no negotiation cost any more under unbalanced DRM-secured contracts.[70]

Clearly, Bell considered fair use from the author's perspective while Loren regarded it as a user's right. Much debate is under way as to whether fair use is an author's right or a user's right. As an author's right 'fair use' in traditional copyright law is a compromise from the author in order to grant stronger protection from the government. Having no ability to protect their copyrighted work in a physical world, the author must tolerate the limitations of enacting their exclusive rights offered by copyright law. As a user's right it is regarded as an important balance between the author's interest and social interest in promoting the development of science and the arts.

In order for information industries to maximize benefits, the concept of author's right is applied to legitimate fared use under DRM-secured contracts. However, based on the policy balance, current mainstream opinion tends to support fair use functioning as a user's right and insists DRM is obliged to provide breathing room for fair use.

How to preserve 'fair use' in a DRM system? Bechtold suggested that legislation must force DRM design solutions to include a certain number of copies for private or educational purposes without permission from content providers.[71] Therien reminded us that the law must carefully regulate the differences in DRM solutions between preventing illegal use and preventing unauthorized use.[72] Burk and Cohen suggested that would-be fair users could be exempted from anti-circumvention provisions.[73] Some consider that, in theory, the best way is that the fair use requirement would be directly programmed into the DRM solution.

Although Stefik affirmatively expressed that it is possible for DRM solutions to support fair use,[74] most, even including the DRM technology expert,[75] question that it will have difficulty in reaching the expectation in the short term because the development of DRM systems is at an early stage. A static, algorithm-based approach embedded in the DRM solution is unlikely to accommodate the shadow of fair use, which is a dynamic, equitable doctrine designed for responding to changing conditions of use over time. So far it has been difficult to build a rights management code approximating the results of judicial determinations.[76]

In order to encourage content providers to release fair use in their DRM-secured intellectual property, Burk and Cohen further proposed the concept and practices of a trusted third-party escrow agent.[77] Levy compensation is also mentioned as the most feasible alternative.[78] Most European Union (EU) member states tend to continue the practice of levy schemes for digital products.[79]

Another Network Effect?

In an article entitled 'Trends in DRM' Rosenblatt mentioned that Microsoft is now working on technology, their so-called unified DRM, which will apply to all platforms, all formats and all devices. In addition, Microsoft promises to make the technology open and broadly applicable.[80] It seems good news. However, after looking at the history of Microsoft's monopoly few people will appreciate its generosity. Instead, they will be sceptical about its intention and start to worry whether it means that another network effect similar to the DRM solution is likely to surface.

The threat to the network effect also draws our attention to the technology standard issue for DRM. In theory, standards will be conducive to fostering interoperability and competition among DRM application vendors. Then we can use the better, more robust and easier-to-use applications. In this regard, DRM vendors need to cooperate with each other in promoting the development of open standards. Unfortunately, this standard-based Utopia is difficult to reach. At present, through patent fights, most DRM solutions are proprietary and incompatible.[81]

Information industries and DRM vendors have applied many business strategies in order to keep DRM solutions proprietary at the expense of interoperability. Usually, there is a collaboration relationship among content providers, developers of DRM technologies and manufacturers of DRM-related devices in order to facilitate their preferred market allocation and pricing strategies. For instance, content providers like to force users to purchase or employ special products via the DRM consumer contract, like the Reimerdes[82] case in which users could only access DVD films on a certain CSS-compliant player.

Clearly, it leads to a closed system under which licensed content is only asked to be compatible with the licensed media.[83] Samuelson and Scotchmer warned that, in such a situation, 'players and content become a "system" much like the operating systems and applications software'.[84] So far few scholars have discussed the issue of technology licences tying together several DRM technologies except Bechtold, who considered it could raise anti-trust concerns. Furthermore, he suggested, such a technology licence with unreasonable copyright limitations cannot be enforceable.[85]

Another strategy is anti-reverse engineering terms. DRM-secured contracts usually include the terms prohibiting the reverse engineering of DRM technologies even though copyright law allows reverse engineering. The validity of such a contract with anti-reverse engineering terms is controversial. In the EU it is not allowed according to the EU Directive on Computer Program of 1991. In the USA, apart from the copyright pre-emption under the UCITA, misuse of copyright,[86] anti-trust and competition law[87] and public interest[88] are suggested to apply and reject the enforceability of anti-reverse engineering terms. To date there is also no resolution in the related case law. Nimmer *et al*. proposed validating such terms in a negotiated licence, but not in a non-negotiated standard form contract.[89] Nevertheless, as the implement of anti-circumvention provisions, if reverse engineering is purported to be a kind of circumvention of technological measures it would be illegal unless it is within the exceptions of anti-circumvention provisions.

More importantly, when a DRM technology becomes the standard in the related market and such a technology standard is under the control of the likes of Microsoft it is likely to generate another network effect under which sufficient network externalities enable the DRM developer to drive out competitors and retain the market dominance.

Instead of making money directly from their DRM technology, they can benefit greatly from bundling it into DRM solutions or into their operating systems and media-rendering applications.[90] A noteworthy case is XrML, an emerging worldwide standard for rights expression, which was developed by ContentGuard and, as we know, ContentGuard is partly owned by Microsoft.

As Lessig mentioned, technical standards act as a type of law that governs behaviours in cyberspace and the technical standards are under the control of the designer. Therefore, the designer has the power to regulate behaviours via technologies by embedding usage rules in the DRM system.[91] As a result, once the control over the design of usage rights in the DRM system is dominated by the hands of private parties such as the music, film and publishing industries, they can effectively create their own intellectual property rules out of the extent of the exclusive rights granted by copyright law and without paying much attention to the interests of the user.[92]

Sometimes a proprietary standard is likely to be worse than no standard. A so-called proprietary standard can be open but not free. As a result, you cannot access anything, let alone use it, until you pay the specified royalty. Once accepted as a technology standard, DRM can further regulate what you do and what you access. Of course you can refuse to accept such a proprietary standard. However, the possible result is that you might get more freedom, but less choice. Microsoft's operating system is the significant case.

Based on these legal arguments, which are more biased towards information industries, some optimistically believe DRM will be a desirable means of replacing copyright law for the protection of digital content.[93] In reality, for the hacker community, perfect technology is not possible. Some circumvention cases provide evidence of this. In the RealNetwork[94] case the streaming technology was circumvented in order to enable users to access and download copies of RealMedia files that are streamed over the Internet. The CSS designed for protecting DVD players was easily broken by 15-year-old Johansen.[95] The SDMI created in response to MP3 piracy also could not escape being cracked by Edward Felten, who was warned by the RIAA not to release the result because his behaviour had broken anti-circumvention provisions.[96] Clearly, stronger protection of DRM systems is totally backed up by the force of copyright law, that is the unbalance results from the undue intervention of anti-circumvention provisions. Therefore, in order to reach the policy balance, the majority of law scholars like Samuelson have suggested mandating anti-circumvention provisions biased towards copyright holders.[97]

Conclusion

Lessig's idea of a 'code is law' warns us that, once computer programs function as the regulator of the Internet, the Internet will no longer be the libertarian's Utopia, but a place with absolute control. This control will be different from the previous control by the government. In the information age commercial interests, particularly information industries, have succeeded in dominating the Internet with powerful trusted systems now better known as DRM technologies.

As digital content has become a valuable commodity and lots of new revenues for information industries are exploited, DRM, owing to the feature of access control, is widely applied for protecting high commercial value digital products against unauthorized

use. The DRM solution consists of a variety of technologies such as authentication, a watermark, encryption and a TCP, which are well integrated into a work flow through the DRM system for detecting, tracking and possibly stopping the illegal distribution of digital content.

In general, the user submits a click-wrap licence in order to purchase digital content. If the authentication matches the user identity and device identification, the encrypted content will be sent to the user along with a watermark. According to the usage rules, the user can then decrypt the content and make it available in their particular DRM-secured device. Of these technologies, authentication tries to build a trusted connection between the content and the targeted user, while watermarking is used for asserting the ownership and tracking the usage of the content. The usage rules act as an access control for regulating the user under certain terms and conditions. The purpose of encryption is to lock up and make the content inaccessible. The TCP is designed for sorting out the problem of security vulnerability in the client side. It is clear that these DRM technologies promise the use and dissemination of digital content completely under an architecture of trust controlled by information industries. In Lessig's words, DRM technologies, through code, have the power to enable copy protection, access control and secure communications more efficiently than laws do.

Some might argue that Lessig's criticism of DRM is too exaggerated because he presented speculation about DRM as fact. Let us look at the current DRM application in information industries. For instance, the business model of 'super-distribution' prevents the first user from freely passing their rights to the music file in digital form to the subsequent user. Even this authorized user is only allowed to play this music file on one certain device, like the computer at home, but not in the office. The streaming technology for audio and video developed by RealNetwork enables the user only to experience the film, but not own the copy of the video file. The Microsoft media player further asks the user to agree the remote control agreement, under which Microsoft has the right to delete the unauthorized content found on the user's computer.

While these DRM-based business models bring new benefits to information industries, they also generate lots of legal debates. Explicitly speaking, with the progress of digital technologies, the DRM dispute has become a battle between individual users and the information industry's monopoly. Initially, some court decisions defined DRM as a merged control that can meet the protection of both access control and copy control of anti-circumvention provisions. Even the access control technology can get more protection than copy control technology does. With the support of anti-circumvention provisions, DRM seems to make it possible to grant information industries a new 'access right' out of the traditional exclusive rights of copyright holders. As a result, access right has a bad impact on the 'public access' of the user because originally the copyright law just protected 'use', not 'access'. The protection of access control technologies also threatens the development of related electronic industries because anti-circumvention provisions also prohibit the manufacture and dissemination of circumvention devices. The information industries would like to sue manufacturers of circumvention devices for unauthorized access rather than sue people for copyright infringement because the monitoring of piracy devices is much easier than a lawsuit for each individual user.[98] Apart from these, through authentication access control enables information industries to constitute a DRM-based private censorship at the expense of individual privacy. Moreover, it enlarges the digital divide by blocking network access unless people pay for use.

Under DRM technologies information industries' desire for generating pay-per-use revenue will come true. Some court decisions in favour of fared use further weaken the fair use defence by ruling the loss of a licence fee as a kind of economic injury. The scope of exceptions of anti-circumvention provisions is also narrower than that of the fair use doctrine in copyright law. These seriously challenge the traditional value of free use under the fair use doctrine. In order to legitimate fared use, information industries assert that fair use is an author's right, not a user's right. In their point of view, fair use in traditional copyright law exists as a compromise for limiting the enactment of the exclusive rights of copyright holders in exchange for granting stronger protection from the government because they were not capable of protecting their products by themselves in a physical world. Once DRM technologies work well in protecting their digital products, they will not be obliged to provide fair use for the user. This debate draws our attention to an issue: whether DRM is powerful enough to replace copyright law in protecting digital products. Lessig seemed in favour of such a thought. However, the conclusion about DRM is problematic. As we know, perfect control is impossible because no technology is 100% secure. Clearly, the result of perfect control of today's DRM technology is not from its technology superiority, but from the protection of anti-circumvention provisions. Therefore, fair use is still viewed as the important element in the balance between authors' interest and social interest. In such a situation, some options, such as a trusted third-party escrow agent or a device levy, have been suggested in order to compensate the author in return for releasing fair use for digital products.

As information industries have become a formidable economic force with the help of DRM, the technology standard for DRM becomes another point at issue. Although open standard usage can be easy, robust and compatible with DRM applications, in fact the expectation has been difficult to reach because at present most important DRM technologies are protected by patent. As a result of proprietary standards, you cannot access anything, let alone use it, unless you pay the royalty. Moreover, the hoarding of such a propriety standard in a few powerful hands such as Microsoft will grant these commercial giants the power to regulate our lives and select values for us. This is because a standard architecture depends on what contents information industries choose and the choice depends on what incentives they desire. Once one DRM standard has succeeded in dominating the related market, network effort will enable information industries to enjoy the winner-take-all reward solely. This encourages information industries to compete in the first-winner-wins game at the price of interoperability. Later, in order to retain market dominance, terms prohibiting reverse engineering of the DRM technologies in the agreement and technology licences building a collaboration relationship among information industries, DRM vendors and manufacturers of DRM-related devices are served in order to drive out other competitors' entrance. These developments remind us of what Microsoft's operation system has done.

To sum up, according to Lessig and his 'code' argument, DRM is powerful enough to fulfil information industries' desire of providing absolute control over their digital intellectual property without the need for law. In terms of technology it might be true for the average person, but not for those who are skilled in computing, particularly hackers. Strictly speaking, due to technological flaws and the ongoing legal arguments, DRM is still seen as a technology that information industries want but are not ready to put into use yet for protecting digital products successfully. However, to some degree anti-circumvention provisions effectively deter some who want to break DRM because of the fear of a criminal penalty. In addition, related case laws have also legitimated some legal

arguments of DRM. Backed up with the force of anti-circumvention provisions, although DRM is not perfect, it is one technology that information industries want more than they can actually provide.

Notes and References

1 Charles Brill, 'Legal protection of collections of facts', *Computer Law Review and Technology Journal*, Vol 12, 1998, http://www.smu.edu/csr/articles.html
2 Mary Maureen Brown *et al*., 'Database protection in a digital world', *The Richmond Journal of Law and Technology*, Vol 6, No 1, 1999, http://law.richmond.edu/jolt/v6i1/conley.html
3 V K Unni, 'Internet service provider's liability for copyright infringement – how to clear the misty Indian perspective', *The Richmond Journal of Law and Technology*, Vol 8, No 2, 2001 http://www.richmond.edu/jolt/v8i2/article1.html
4 Seybold Research, *Industry Survey: Digital Rights Management – Usage, Attitudes and Profile Of Users*, Seybold Seminar & Publications, Foster City, CA, 2001.
5 Peter Biddle *et al*., 'The darknet and the future of content distribution', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, p 359, 2003.
6 Charles C Mann, 'The heavenly jukebox', 2000, http://www.theatlantic.com/issues/2000/09/mann.htm
7 International Federation of the Phonographic Industry, 'IFPI music piracy report 2002', 2002, http://www.ifpi.org/site-content/library/piracy2002.pdf
8 *Ibid*.
9 The Motion Picture Association of America, 'Anti-piracy', accessed 13 December 2004 at http://www.mpaa.org/anti-piracy/content.htm
10 Clifford Lynch, 'The battle to define the future of the book in the digital world', *First Monday*, Vol 6, No 6, 2001, http://www.firstmonday.dk/issues/issue6_6/lynch
11 Gail Dykstra, Gail, 'DRM for a brave new world', 2003, http://www.econtentinstitute.org/infohighway/0303/03apr01.asp
12 Bill Rosenblatt, Bill Trippe and Stephen Mooney, Stephen, *Digital Rights Management: Business and Technology*, Hungry Minds, New York, pp 86–87, 2002.
13 Fabien A P Petitcolas, 'Digital watermarking', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, pp 81–92, 2003.
14 Susanne Guth, 'A sample DRM system', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, pp 150–161, 2003.
15 Rosenblatt, *supra* note 12, pp 114–123.
16 Gabriele Spenger, Authentication, identification techniques, and secure containers – baseline technologies', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, pp 62–80, 2003.
17 Rosenblatt, *supra* note 12, pp 82–84.
18 Dirk Kuhlmann and Robert A Gehring, 'Trusted platforms, DRM, and beyond', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, pp 178–205, 2003.
19 Ross Anderson, '"Trusted computing" frequently asked questions', 2003, http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html
20 Will Knight, 'Microsoft's anti-piracy plans spark controversy', NewScientist.com news service, 1 July 2002, http://www.newscientist.com/article.ns?id=dn2483
21 Stefan Bechtold 'From copyright to information law – implications of digital rights management', 2002, http://www.jura.uni-tuebingen.de/bechtold

22 *Ibid*.
23 Dykstra, *supra* note 11.
24 Matt Hines, 'Microsoft, InterTrust iron out lawsuit', *CNET News.com*, 12 April 2004, http://news.com.com/2100-1014_3-5189980.html?tag=nefd.lede
25 Rian A LaMacchia 'Key challenges in DRM: an industry perspective', accessed 21 September 2004 at http://www.farcaster.com/papers/drm2002/drm2002.pdf
26 'The technology review ten', *MIT Technology Review*, 2001, http://www.nicolelislab.net/NLNet/Load/Media/MITTechnologies2001.pdf
27 Josbua Dubl and Susan Kevorkian, 'Understanding DRM systems: an IDC white paper', 2001, www.intertrust.com/main/research/whitepapers/IDCUnderstandingDRMSystems.pdf
28 Association of American Publishers, 'Digital rights management for Ebooks: publisher requirements', 2000, http://www.publishers.org/digital/drm.pdf
29 Rosenblatt, *supra* note 12.
30 National Research Council, 'Music: intellectual property's canary in the digital coal mine', in *The Digital Dilemma: Intellectual Property in the Information Age*, National Academies Press, Washington, DC, pp 76–93, 2000, http://www.nap.edu/html/digital_dilemma/ch2.html
31 Lynch, *supra* note 10.
32 National Research Council, *supra* note 30.
33 R Mori, 'Superdistribution: the concept and the architecture', *The Transactions of the IEICE*, Vol E73, No 7, 1990, http://www.virtualschool.edu/mon/ElectronicProperty/MoriSuperdist.html
34 Rosenblatt, *supra* note 12, pp 70–73.
35 Mann, *supra* note 6.
36 Rosenblatt, *supra* note 12, pp 88–89.
37 *RealNetworks, Inc.* v. *Streambox, Inc.* [2000] WL 127311 (WD Wash. 2000), http://www.law.uh.edu/faculty/cjoyce/copyright/release10/Real.html
38 Willms Buhse and Amelie Wetzel Amelie, 'Creating a framework for business models for digital content – mobile music as case study', in E Becker *et al*. (eds) *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, Springer-Verlag, Heidelberg, pp 271–287, 2003.
39 Dykstra, *supra* note 11.
40 Judy Mottl, 'Digital rights management: content's secure wrapper', 2002, http://www.infowecuritymag.techtarget.com/2002/mar/features_digitalrightmgmt.shtml
41 Elisabeth Goodridge, 'Keep it confidential', accessed 12 December 2004 at http://www.microsoft.com/business/executivecircle/content/page.aspx?cID=886&subcatID=3
42 Microsoft, 'Information rights management in Microsoft office 2003', Microsoft TechNet, 2003, http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx
43 Rachel Konard, 'Trouble ahead, trouble behind' 2002, http://news.com.com/2102_1082_3-843349.html?tag=st_util_print
44 Lolly Gasaway, lolly, 'The new access right and its impact on libraries and library users', 2002, http://www.unc.edu/~unclng/the%20new%20access.htm
45 R Anthony Reese, 'Legal incentives for adopting digital rights management systems: merging access controls and rights controls', *Berkeley Technology Law Journal*, Vol 18, 2003, http://www.law.berkeley.edu/insitutes/bclt/drm/papers/reese-drm-btlj2003.html
46 *Supra* note 37.
47 *Universal City Studios* v. *Reimerdes*, 111 F.Supp.2d 294 (SDNY 2001).
48 *Ibid*.
49 Dan L Burk, 'Anti-circumvention misuse', 2002, <http://tprc.org/papers/2002/29/misuse.pdf>

50 Jane C Ginsburg, 'From having copies to experiencing works: the development of an access right in U.S. copyright law', Public Law & Legal Theory Working Paper Group, 2000, http://papers.ssrn.com/paper.taf?abstract_id=222493
51 *ibid*.
52 Guth, *supra* note 14, p 151.
53 Dan L Burk and Julie E Cohen, 'Fair use infrastructure for copyright management systems', *Harvard Journal of Law & Technology*, Vol 15, No 1, p 51, 2001.
54 *Supra* note 37.
55 John Therien 'Exorcising the specter of a "pay-per-use" society: toward preserving fair use and the public domain in the digital age' *Berkeley Technology Law Journal*, Vol 16, 2001, http://www.law.berkeley.edu/journals/btlj/articles/vol16/therien/therien.pdf
56 Tom W Bell, 'Fair use vs. fared use: the impact of automated rights management on copyright's fair use doctrine' *North Caroline Law Review*, Vol 76, 1998, http://www.tomwbell.com/writings/FullFared.html
57 Yaman Akdeniz, 'Case analysis of league against racism and anti-Semitism (LICRA), French Union of Jewish students v. Yahoo! Inc., (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000', 2000, http://www.cyber-rights.net
58 Anderson, *supra* note 19.
59 Konard, *supra* note 43.
60 Electronic Frontier Foundation, 'Digital rights management: a failure in the developed world, a danger to the developing world', 2005, http://www.eff.org/IP/DRM/itu_drm.php
61 Electronic Frontier Foundation, 'Unintended consequences: five years under the DMCA', accessed 3 March 2005 at http://www.aph.gov.au/senate/committee/freetrade-ctte/submissions/sub165att2.pdf
62 Rosenblatt, *supra* note 12, p 45.
63 *Princeton University Press* v. *Michigan Document Services, Inc.*, FED App. 0357P (6th Cir. 1996).
64 *American Geophysical Union* v. *Texaco, Inc*., 60 F.3d 913 (2nd Cir. 1994).
65 *Ibid*.
66 Bell, *supra* note 53.
67 Lydia Pallas Loren, 'Redefining the market failure approach to fair use in an era of copyright permission systems', *Journal of Intellectual Property Law*, Vol 5, No 1, 1997, http://www.lclark.edu/ ~ loren/articles/fairuse.htm
68 Burk, *supra* note 47.
69 Bell, *supra* note 53.
70 Loren, *supra* note 61.
71 Bechtold, *supra* note 21.
72 Therien, *supra* note 52.
73 Burk and Cohen, *supra* note 51, p 56.
74 Mark Stefik, 'Shifting the possible: how trusted systems and digital property rights challenge us to rethink digital publishing', 1997, http://www.law.berkeley.edu/journals/btlj/articles/vol12/Stefik/html/text.html
75 Rosenblatt, *supra* note 12, p 45.
76 Burk and Cohen, *supra* note 51, p 56.
77 Burk and Cohen, *supra* note 51, p 63.
78 Dykatra, *supra* note 11.
79 Jorg Reinbothe, 'Private copying, levies and DRMs against the background of EU copyright framework', in *Conference on 'the Compatibility of DRM and Levies'*, 2003, http://europe.eu.int/comm/internal_market/en/intprop/news/2003-09-speechen.htm
80 Bill Rosenblatt, 'Trends in DRM', 2001, http://www.giantstepsmts.com/drmtrends.htm
81 Stefik, *supra* note 68.

82 *Supra* note 47.
83 Therien, *supra* note 52.
84 Pamela Samuelson and Suzanne Scotchmer, 'The law and economics of reverse engineering', *Yale Law Journal*, Vol 111, 2002, http://www.sims.berkeley.edu/~pam/papers.html
85 Bechtold, *supra* note 21.
86 Marshall Leaffer, 'Engineering competitive policy and copyright misuse', in *University Dayton Law Review*, Vol 19, pp 1087–1108, 1994.
87 Samuelson and Scotchmer, *supra* note 77.
88 J H Reichman and Jonathan A Franklin, 'Privately legislated intellectual property rights: reconciling freedom of contract with public good uses of information', in *University Pennsylvania Law Review*, Vol. 147, pp 875–970, 1999.
89 David Nimmer, Elliot Brown and Gary N Frischling, 'The metamorphosis of contract into expand', *California Law Review*, Vol 87, 1999, http://cyber.law.harvard.edu/property00/alternatives/nimmer.html
90 Rosenblatt, *supra* note 74.
91 Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basics Books, New York, p 135, 1999.
92 Burk and Cohen, *supra* note 51, p 51.
93 Bechtold, *supra* note 21.
94 *Supra* note 37.
95 *Supra* note 47.
96 Rosenblatt, *supra* note 12, p 133.
97 Pamela Samuelson, 'Intellectual property and the digital economy: why the anti-circumvention regulations need to be revised', *The Berkeley Technology Law Journal*, Vol 14, 1999, http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm
98 Reese, *supra* note 45.