From Copyright to Information Law – Implications of Digital Rights Management*

Stefan Bechtold

Stanford Law School
559 Nathan Abbott Way, Stanford, CA 94305-8610, USA
stef@n-bechtold.com
http://www.jura.uni-tuebingen.de/~s-bes1

Abstract. Digital Rights Management (DRM) promises to enable a secure electronic marketplace where content providers can be remunerated for the use of their digital content. In the last few years, countless research efforts have been devoted to DRM technologies. However, DRM systems are not only technological phenomena: they pose complex legal, business, organizational and economic problems. This article tries to show that from a lawyer's perspective some of the innovativeness and potential of DRM can only be understood when one looks at it from a multidisciplinary viewpoint. The article gives an overview of the various ways by which digital content is protected in a DRM system. The intertwining protection by technology, contracts, technology licenses and anti-circumvention regulations could lead to a new "property right" making copyright protection obsolete. However, there is a danger of over-protection: questions of fair use and other limitations to traditional copyright law have to be addressed. If competition is not able to solve this tension between the interests of content providers and the interests of users or the society at large – which seems to be doubtful at least – it is the law that has to provide a solution. The legislators in the U.S. and Europe use different approaches to address this problem. By looking at DRM in this way, several patterns can be observed which are characteristic of many areas of Internet law.

1 Introduction

Digital Rights Management (DRM) promises to offer a secure framework for distributing digital content (music, video, text, rare data etc.). DRM enables an electronic marketplace where previously unimaginable business models can be implemented. At the same time, DRM ensures that content providers – particularly copyright owners –

* This article is based on an extensive treatise on Digital Rights Management written in German by the author at the University of Tübingen Law School, Germany (1999–2001), see [1].

T. Sander (Ed.): DRM 2001, LNCS 2320, pp. 213-232, 2002.

receive adequate remuneration for the creation of the content that is distributed over the DRM system.

From a technological perspective, DRM poses intricate problems that have led to large research efforts at technology companies, universities and research centers worldwide. However, DRM systems are not only technological phenomena. From an organizational perspective, DRM interoperability and standardization remain open problems to a large extent. From a business perspective, it is intriguing to look at the new business models which DRM systems could enable. From an economic perspective, DRM could challenge – jointly with other technologies surrounding the Internet – some aspects of the standard economic theory taken for granted hitherto. From a sociological perspective, DRM could have an influence on the distribution of information and therefore power in a society. From a legal perspective, DRM creates a whole assemblage of problems ranging from copyright, contract, privacy, patent and antitrust problems to freedom of speech issues.

This article intends to provide an overview of the copyright-related parts of the legal framework in which DRM systems operate. It intends neither to give a comprehensive overview of DRM in general nor to provide an in-depth analysis of all the questions being raised. It is the firm belief of the author that some of the real innovation and potential of DRM can only be understood if one looks at several disciplines engaged in the creation or analysis of DRM systems at the same time. There is a clear lack of interdisciplinary work in the DRM field. Therefore, while this article ultimately has a legal argument, it will describe some technical and economic aspects of DRM and correlate these aspects with the legal discussion of DRM systems. As used in this article, the term "Digital Rights Management" has a broad scope. It not only covers a great number of different technologies by which digital content can be secured. It also covers the protection of digital content offered by various legal instruments as well as business and economic aspects of DRM.

The article proceeds as follows. Sections 2 to 4 give an overview of the various means of protection (both technical and legal) available in a DRM system. Section 5 correlates those means with each other both from a legal and a law and economics perspective. Section 6 asks what role copyright law still plays in a DRM system. Section 7 gives an overview of how the legislators in the U.S. and Europe have responded to some of the challenges to copyright law created by DRM systems. Finally, section 8 puts the results of this article in the broader context of Internet law.

2 Protection by Technology

2.1 Overview

In order to ensure that consumers pay for using digital content and that content providers are adequately remunerated, DRM systems intend to control access to and use of digital content. This can be achieved by implementing various technological protection measures. Encryption techniques are especially important; "digital containers" enable the durable encryption of distributed content. Copy control technologies such as the "Copy Generation Management System" (CGMS) used in DVD players or the

"Serial Copy Management System" (SCMS) used in DAT and Minidisc players control the number of copies of digital content a user is able to make.

In order to facilitate the automated trading of digital content and associated digital rights, DRM systems use metadata to formally describe digital content and related parameters. Thereby, the content provider is able to control automatically in a very fine-grained way when and where which consumer uses a particular content for what purpose. Metadata systems use standards that enable the description of digital content (e.g. DOI, ISBN, ISRC, ISWC and PII), its rights holders (e.g. CAE/IPI) and its accompanying usage terms (so-called "usage rules" defined in "rights management languages" such as XrML or ODRL).[1] Either metadata can be stored in special headers of a digital content format, or they can be embedded directly into the digital content by using digital watermarking techniques.

DRM systems employ different techniques to identify consumers and trace back illegally copied content (e.g. serial numbers, digital fingerprints, traitor tracing). In order to provide a uniformly high level of security, various techniques are used that ensure the integrity and authenticity of digital content, its accompanying metadata and the hardware and software components of a DRM system (e.g. digital signatures, fragile watermarks, challenge-response protocols). Furthermore, security attacks are complicated by tamper-proof hard- and software (e.g. smart cards, code obfuscation). In order to prevent the copying of protected content after it has been transformed into an analog format, special analog protection systems and digital watermarks intend to make such copying more difficult at least.

DRM systems not only provide passive protection mechanisms. They also can employ various means that prevent or respond actively to security breaches. Specialized filters and "audio fingerprinting" or "robust hash" techniques can block access to pirated content. Fair-exchange protocols ensure technically that the consumer receives access to protected content only after having paid the appropriate price. If the DRM system detects a security breach, it can revoke and disable compromised consumer devices.

In order to be successful on the mass-market, DRM technologies have to be integrated into consumer devices in a standardized way. Various working and standardization groups try to coordinate the development process of DRM technology.[2] Today, various media systems available on the market use one or the other DRM technology. DRM components can be found in pay TV systems, DAT and Minidisc players as well as some videocassettes. The DVD system employs various technological protection measures, e.g. the "Content Scramble System" (CSS), the regional code playback control and the aforementioned CGMS. Other important DRM standards include the "Content Protection for Recordable and Prerecorded Media" (CPRM/CPPM), the "Digital Transmission Content Protection" (DTCP, protecting IEEE 1394 bus systems) and the "High-bandwidth Digital Content Protection" (HDCP, protecting digital video outputs). Furthermore, DRM solutions are being integrated into standard audio

---

[1] This is not an exhaustive listing of existing metadata standards, of which there are dozens, if not hundreds. Besides, there are numerous proprietary metadata systems.

[2] Two of the most well-known groups include the "Copy Protection Technical Working Group" (CPTWG) and the "Secure Digital Music Initiative" (SDMI).

and video software players, ebook reading software, operating systems and mobile devices.

In summary, DRM is a general term for a set of intertwining technologies that can be used to establish a secure distribution channel for digital content. The specific elements used vary from DRM system to DRM system. As understood in this article, DRM ranges from simple copy-prevention technologies to comprehensive secure distribution systems.

2.2 Supporting Protection by Anti-circumvention Regulations

Although DRM systems promise to provide a high level of technical security, no commercially viable system will be technically 100% secure. Technological protection measures have been hacked in the past and this will not change in the foreseeable future. In order to increase the overall security of a DRM system, over the last few years special legal regulations have been created that outlaw the circumvention of technological protection measures as well as the manufacturing and distribution of devices which can be used to circumvent such measures ("preparatory activities").

On the international level, such provisions can be found in two treaties adopted in 1996 under the aegis of the World Intellectual Property Organization (WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty). In the U.S., Congress enacted complex anti-circumvention regulations as part of the Digital Millennium Copyright Act of 1998 (17 U.S.C. §§ 1201-1205). Additionally, provisions of the Audio Home Recording Act of 1992 (17 U.S.C. §§ 1001-1010), of communications law (47 U.S.C. § 553 and § 605) and of trade secret law can apply. In the European Union, article 6 of the recently adopted Copyright Directive of 2001 [2] contains a detailed provision outlawing the circumvention of technological protection measures and certain preparatory activities. Furthermore, the European Conditional Access Directive of 1998 [3] protects a wide variety of conditional-access-based services against preparatory activities (e.g. pay TV, but also Internet-based services). Additional prohibitions can be found in the laws of the member states of the European Union (e.g. copyright, criminal, unfair competition, telecommunications, broadcasting and tort law).

Another set of regulations outlaw the manipulation of DRM metadata. Such provisions can be found in the aforementioned WIPO treaties, the U.S. Digital Millennium Copyright Act (17 U.S.C. § 1202) and in article 7 of the European Copyright Directive [2]. Usually, these regulations protect metadata identifying the digital content, its rights holders and its usage rules. In contrast, metadata identifying the individual consumers (e.g. by digital fingerprints or traitor tracing) are not covered by this protection due to privacy concerns.

All these provisions have little to do with traditional copyright law. They are part of an emerging body of information law regulating the access to and use of information.

3 Protection by Contracts

3.1 Overview

In a DRM system, content providers are not protected by technology and anti-circumventions regulations alone. Rather, they can use contracts to oblige consumers to use the protected content only in certain ways. In such a contractually protected DRM system, consumers are required to enter into a contractual agreement either at the time they acquire some DRM-enabled hardware or software device or at the time they want to access an individual content within the DRM system (by entering into so-called "click-wrap contracts").

Such DRM contracts may be used to protect digital content and the DRM system itself. For instance, they may include terms obligating consumers to download the content only to DRM-secured devices, not to burn it onto CD-ROMs or DVD-ROMs, not to copy and paste it and not to print out images or text. They also may define how often, when and where the protected content may be used ("usage rules"). Other terms may protect the security of the DRM system itself. Consumers may be forbidden from reverse engineering system software or from circumventing the technological protection measures used in the system (cf., e.g., [4]).

This contractual protection is only helpful if the contracts are legally enforceable. Similarities to "shrink-wrap licenses" used in the software business could suggest that DRM consumer contracts are invalid. However, at least in the U.S. a tendency within courts and legislators to consider shrink-wrap licenses as valid contracts is observable.[3] Furthermore, the legal problems of shrink-wrap licenses greatly depend on the specific design of the licenses and the accompanying business model (e.g. when and how the contract is concluded and who the parties to the contract are). The validity of consumer contracts in DRM systems raises complex legal problems that are beyond the scope of this article. However, no basic obstacles exist for content providers to contractually protect their content in a DRM system. It is possible to design a DRM system and its business models in a way that such contracts are legally enforceable.

3.2 Supporting Protection by Technology

As described above, DRM consumer contracts contain usage rules defining the ways in which the consumer is authorized to use the content. These usage rules can be expressed as metadata in rights management languages (see above at section 2.1). From a legal perspective, this is a very important feature of DRM systems as compliance to the contractual terms not only can be controlled by law, but also by technology: if the contract and the metadata of a digital content allows a user only to make two copies, any further copy will be prevented by the technological measures of the DRM system. This shows that the contractual protection is supported by a technological protection: Technology makes it harder or even impossible to disobey contractual obligations.

---

[3] Cornerstones of this development are a decision by the 7th Circuit Court of Appeals (see [5]) and the "Uniform Computer Information Transactions Act" (UCITA), see [6].

3.3 Supporting Protection by Anti-circumvention Regulations

However, this technological protection of DRM contracts is not failsafe. Once in a while, attackers will succeed in altering or deleting usage metadata. Against this attack, the law provides regulations which specifically prohibit the manipulation or deletion of metadata (see above at section 2.2). This shows the intertwining of the means of protection in a DRM system: content providers may protect their content by contracts, which can be protected themselves by various technological protection measures which are in turn legally protected against circumvention.

4 Protection by Technology Licenses

Many DRM technologies are protected by a patent or kept as a trade secret. For instance, the developer of a symmetric DRM encryption system keeps the decryption keys secret due to security reasons.[4] If a computer or consumer electronics manufacturer wants to enable his devices to process content that is protected by this DRM technology, he has to enter into a technology license agreement with the developer of the technology. Thereby, the manufacturer gains knowledge of the decryption keys and of other details of the technology. Licensees of DRM technologies include manufacturers of consumer electronics, computers, storage media and other DRM-enabled devices or components as well as content providers.

DRM technology license agreements can be used to protect the interests of content providers although the content providers typically are not the licensors of the DRM technology. In long lasting negotiations between the content, computer and consumer electronics industry, the content industry has made clear that it would be willing to distribute its content in a digital format only if an adequate level of security could be assured. As no DRM system will be successful on the market without an appropriate amount of content accessible within this system, every technology developer of a DRM solution has vital commercial interests that his technology be implemented in consumer devices in the most secure way. Therefore, DRM developers license their technology only on the condition that the interests of content providers are preserved when the technology is implemented in consumer devices. Thereby, DRM technology licenses indirectly serve the interests of content providers (see also [7, at 15, 27]).

So far, this close connection between DRM technology licenses and copyright protection has not been discussed a great deal among legal scholars. Only the U.S. Federal Communications Commission has looked at a specific DRM technology license in the pay TV sector from this angle (cf. [7]).[5] This article cannot describe any DRM technology license in detail. However, it gives an overview of some common license terms.[6]

---

[4] If consumer devices need the symmetric key for decryption, it is regularly stored in a tamper-proof environment.

[5] The FCC examined the validity of the "POD Host Interface License Agreement", a technology license of the OpenCable initiative, [8].

[6] The technology licenses analyzed for this purpose are publicly available from the respective licensing administrators or other websites. They include: the CSS License Agreement and

It is crucial for commercial success that content is protected at every stage within the DRM system. However, a DRM system is not a monolithic technology, but consists of a large number of different technologies. Therefore, numerous protection measures have to be combined to provide a continuous level of high security. To achieve this goal, technology licenses tie together several DRM technologies by requiring that the licensor of one specific DRM technology also use another DRM technology in his implementation.[7] For instance, the CSS License Agreement requires that the manufacturer of stand-alone DVD players also incorporate the region coding technology into his players. Furthermore, the players are only allowed to transmit analog video data in a format protected by analog copy protection technologies of Macrovision and equipped with CGMS copy control signals. Digital video data may only be transmitted to outputs which are equipped with copy-protection technologies (either DTCP or HDCP, see above section 2.1). Similar provisions can be found in other technology license agreements.

DRM technology licenses also require that DRM-enabled devices obey the usage rules of digital content that are determined by the content provider in metadata. Sometimes, the licenses contain default usage rules (e.g. by determining that content can only be copied once). DRM technology licenses also contain provisions to ensure that consumer device manufacturers implement the DRM technology in a robust way. For this reason, manufacturers are required to use security technologies such as encryption, self-checking and tamper-proof hard-/software in their DRM implementations. Technology licenses require that it be difficult at least to defeat the DRM protection by using professional tools such as logic analyzers, chip disassembly systems or in-circuit emulators. If the licensed DRM technology is defeated nevertheless, the licensee is required to redesign or replace its affected products within clearly defined time frames. Finally, technology licenses prohibit manufacturers of DRM-enabled consumer equipment to produce devices or software that can be used to circumvent the DRM protection.

In summary, DRM technology licenses are used to establish a comprehensive DRM environment that enables secure transmissions from the content provider to each consumer. They contain numerous terms that indirectly serve the copyright and security interests of the content providers.

5 Paradigm Shift in Protection

As this article has shown so far, the protection of digital content in a DRM system is based on various means of protection: (1) protection by technology with supporting protection by anti-circumvention regulations, (2) protection by contracts with supporting protection by technology and anti-circumvention regulations and (3) protection by technology licenses (see figure 1).

CSS Procedural Specifications, the HDCP License Agreement, the POD Host Interface License Agreement, the CPRM/CPPM License Agreement and the DTCP License Agreement.

[7] In principle, such tying arrangements could raise antitrust concerns. An analysis of this aspect is beyond the scope of this article. However, such an analysis is likely to lead to the result that the license agreements are valid to a large extent.

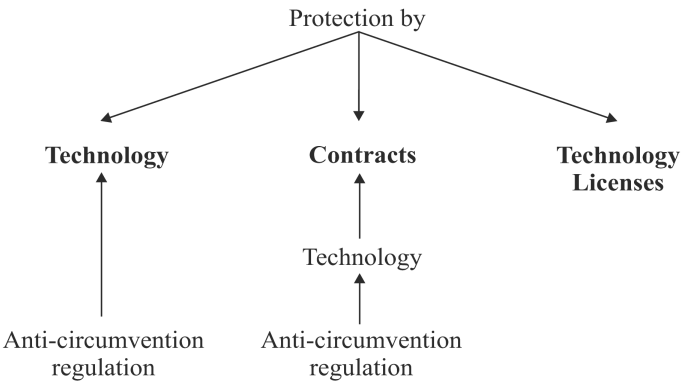

Fig. 1. Different means of protection in a DRM system (1)

In the following section, the implications of these different means of protection will be analyzed from both a legal and a law and economics perspective.

5.1 Legal Perspective

5.1.1 Intertwining Means of Protection

One of the most prominent features of the protection by DRM systems is that the various means of protection do not exist independently of each other. Only when one looks at DRM protection as a whole can one see some of the innovativeness and potential of DRM systems. The following two examples should clarify this proposition:

1. In order to prevent large-scale piracy, content providers have strong interests to hinder consumers from making unlimited copies of digital content. A fully developed DRM system provides numerous ways to realize these interests: encryption and other technologies can be employed to control the uses a consumer can make of a digital content (*protection by technology*). If an attacker is able to circumvent these technologies, he may violate legal circumvention prohibitions (*legal protection of the technological protection*). Furthermore, consumers can be required by contract to make only a specified number of copies (*protection by contracts*). Such usage rules can be expressed in metadata which are the basis for copy-control technologies such as SCMS or CGMS. Thereby, it is ensured technologically that users obey the terms of their usage contracts. Metadata can be embedded in the content by using robust digital watermarks (in each case a *technological protection of the contractual protection*). If an attacker succeeds in altering or deleting the metadata, anti-circumvention provisions may apply again (*legal protection of the technological protection of the contractual protection*). Finally, manufacturers of DRM-enabled hardware and software are obliged by technology licenses to ensure that their products obey the metadata determined by the content providers (*protection by technology licenses*).
2. A DRM system should provide the highest security that is technically possible but still commercially viable. This can be achieved by different means of protec-

tion: from a technical viewpoint, this involves tamper-proof hardware and software as well as technologies to check the inegrity and authenticity of DRM components and to revoke compromised devices (*protection by technology*). If these technologies are circumvented, anti-circumvention provisions may apply (*legal protection of the technological protection*). At the same time, users are forbidden by contract from circumventing the technological measures (*protection by contracts*). Finally, manufacturers of DRM-enabled devices are prohibited by technology license agreements from producing devices or software that can be used to circumvent the technological protection (*protection by technology licenses*).

These and many other examples show that in a DRM system, the content provider is always protected simultaneously by several means of protection. Each of these means is not 100% secure: technological protection can be circumvented, statutory prohibitions can be disobeyed, contracts can be breached. However, it is one of the most interesting features of DRM systems that these means of protection do not operate independently. If one of the means fails, another means steps in which sustains the overall protection level of the DRM system. The security of a DRM system is not accomplished by technology, law or market forces alone. Rather, it is a result of numerous different, but *intertwining* means of protection. This common feature of many DRM systems has often been underrepresented in the scholarly discussions. Regularly, critics of DRM assert that DRM ultimately will fail because it is impossible to create a technically secure DRM system. However, this criticism misses the point because it only regards one dimension of DRM protection.

5.1.2 Creation of a Privatized "Property Right"

The intertwining protection by technology, contracts, anti-circumvention regulations and technology licenses in a DRM system raises the question what the implications for traditional copyright protection are.

In a DRM system, it is possible to require that each consumer enters into a contract before accessing DRM-protected content (see above section 3.1). In principle, each of these contracts only binds the parties of the contract, i.e. the content provider and one consumer. However, if every consumer must enter into such a contract before accessing the content, no consumer exists who is not in privity with the content provider. In the U.S. legal literature, this has led many commentators to the conclusion that the contractual protection in a DRM system resembles a property right which is good against all the world.[8] The law has regularly already granted a property right to content providers: copyright law. As such, the copyright owner is entitled to exclude unauthorized persons from reproducing, distributing or performing his works. According to these commentators, the sum of consumer contracts in a DRM system leads to a similar level of protection because every consumer in a whole mass market is contractually bound to the usage terms set by the content provider.

However, this point of view captures only parts of the potential of DRM systems, as it underestimates the intertwining means of protection in a DRM system. If the content provider could only rely on a myriad of contracts to protect his digital content,

---

[8] This discussion has been fueled by a decision of the 7th Circuit Court of Appeals dating from 1996, [5].

this protection would have severe weaknesses. For instance, a consumer who obtained a pirated copy of the digital content would not be bound to any DRM contracts at all; the contractual protection would fail whereas copyright protection would still succeed. However, one has to keep in mind that in an idealized DRM system such a case would never arise: Normally, the DRM system grants access to protected content only after the consumer has agreed to a contractual agreement (*protection by technology*). If the consumer circumvents this procedure, he may violate anti-circumvention provisions (*legal protection of technology*). Furthermore, this procedure may be secured by appropriate *technology license* agreements. Through a combination of technological and legal protection a DRM system tries to ensure that a digital content can *never* be accessed or used without having agreed to the appropriate usage terms. The intertwining means of protection try to inextricably knit together content and usage terms.

Therefore, from a legal viewpoint the real innovation of DRM systems is not the protection of content by technology or unilateral contracts which bind every consumer. It is the combination of this protection with other supporting means that creates a level of protection commonly found only with traditional property rights. As with the protection by a property right, no consumer of DRM content exists who is not subject to the DRM protection. If one views this conglomerate of protection as a whole, the terms "privatized property right" and "private legislation" seem appropriate. Overall, a trend from protection by copyright law to protection by the intertwining means of technology, contracts, anti-circumvention regulations and technology licenses can be observed. This new conglomerate of protection has the potential to supplant copyright law as the primary means of protection in the digital environment.

5.2 Law and Economics Perspective

A law and economics analysis of the protection in DRM systems leads to similar results. Like any information, digital content is (to some extent) a public good characterized by its non-rivalry and non-exclusivity.[9] Because it is impossible to exclude non-paying consumers from the consumption of the content, no consumer will pay for using the content. Hiding his real preferences, every consumer hopes that another consumer will buy the content and that he can use this content as well due to its non-exclusive and non-rivalrous nature ("free rider" problem). As a result, nobody would create content in the first place, as the costs of creation could never be recouped (cf. [9]). To eliminate this market failure, the law grants the content producer a property right known as copyright. Through copyright law, the content producer is able to exclude non-paying consumers and copyists from using his content. Copyright law artificially raises the costs of copying content, thereby enabling the content producer to recover his costs of creation. To a certain extent, copyright law eliminates the non-exclusivity of content.

As was shown above, the intertwining means of protection in a DRM system enable the content provider to exclude unauthorized consumers from using protected content as well. Just as copyright law, the DRM protection eliminates the non-

[9] A good is non-rivalrous when the consumption of this good by one consumer does not diminish its availability for others to use. A good is nonexclusive if it is (nearly) impossible to exclude consumers from consuming it.

exclusivity of content to a certain extent. This could have far-reaching implications for the necessity of copyright law: the market failure which copyright law was established to remedy does not seem to exist any more in DRM systems. Seen from a law and economics perspective, the protection by DRM systems could replace the protection by copyright law to a certain extent.

6 Necessity of Copyright Law

The analysis of the previous section seemingly leads to the result that copyright protection could become useless in DRM systems. However, such a proposition would ignore several objections, some of which will be depicted in this section. Firstly, copyright law could still be needed to limit the protection offered by DRM systems (see supra 6.1). Secondly, copyright protection could serve as a kind of safety net protection (see supra 6.2).

6.1 Limitations to DRM Protection

Copyright protection has never been unlimited. Some of the most noticeable limitations to copyright protection are the fair use defense and the limited duration of copyright protection. In contrast, the protection by DRM systems is potentially unlimited. DRM systems may protect digital content that is not copyrightable or restrict acts that are exempted from copyright protection. It is a complex question whether and to what extent copyright limitations should also apply to the different means of protection in a DRM system.

6.1.1 Law and Economics Perspective

From a law and economics perspective, one has to ask what the justifications for copyright limitations are and whether these justifications are valid also in the DRM context.

There is no single economic explanation of copyright limitations. One way of explaining is to view copyright as a sort of monopoly (which is a severe oversimplification, however). According to this view, copyright law – like any monopoly – allows the copyright owner to raise the price for his work above marginal costs.[10] Thereby, fewer consumers buy the work compared to a perfectly competitive market. This can lead to a social welfare loss due to the underutilization of the work (for a detailed explanation, see [10, chapter 10], [11, at 301-305]). From this perspective, it is the goal of copyright law and its limitations to reconcile two possible welfare losses: the welfare loss due to the underproduction of content (leading to copyright protection, see section 5.2) and the welfare loss due to the underutilization of the produced content (leading to copyright limitations). This analysis can be applied to DRM systems as well. Just like copyright law, DRM systems allow the content provider to charge prices above marginal costs. Therefore, DRM systems can lead to a socially wasteful

[10] Marginal costs are the costs to produce one additional unit of a good.

underuse of the protected content as well.[11] From this perspective, the protection by DRM systems should be limited just as copyright protection should be limited.[12]

Another way to look at copyright law – which in the last few years has continuously gained support – views copyright protection not so much as a tool to induce the creation of new works, but rather as an instrument to facilitate a market for the exchange of rights to creative works that can move to their highest socially valued uses. From this viewpoint, copyright law enables copyright owners to charge consumers for access not so much to give an incentive as to determine what creative works are worth and thus to create a guide for resource allocation (cf. [15, at 309-310]). For this line of thought, copyright limitations are far less important, as the allocation of rights should be left to the market to the largest extent possible. If one applies this theory to the protection by DRM systems, limitations could play only a minor role.

Another way of justifying copyright limitations is to view them mainly as an answer to high transaction costs. If the costs involved in forming and enforcing a contract between the copyright owner and the consumer are higher than the value of the transaction, the transaction will never occur and the consumer will not use the work. In such cases, it can be more efficient to limit copyright protection so that the consumer does not have to ask for permission to use the work. As DRM systems could lead to lower transaction costs (search engines could lower search and information costs, metadata could lower negotiation and enforcement costs, the latter of which could also be lowered significantly by technological protection measures), the necessity to limit DRM protection could diminish.

It is far beyond the scope of this article to analyze the conflicting economic theories concerning the necessary limitations to copyright and DRM protection in detail. The economic explanation of such limitations and their implications on the dynamic innovation process remain one of the great puzzles of the economic analysis of copyright law. For the purposes of this article it suffices to realize that even among the proponents of a very broad copyright and DRM protection, it is a widespread opinion that the protection should be limited at least in some respects (see, e.g., [16, at 135]). External effects and other factors still require the limitation of copyright and DRM protection (see [17, at 1056-1058]).

If one accepts the notion that the protection by DRM systems should be limited in some respects – whatever those respects may be – the question arises who should determine those limits. In principle, this can be accomplished either by market forces or by the law. According to one view, DRM systems whose technological or contractual protection is biased too much towards the interests of content providers and do not take appropriate limitations into account will not be successful on the market

---

[11] The reason for this parallelism lies in the fact that the welfare loss due to underproduction, which justifies both copyright and DRM protection, results from the non-rival nature of digital content. This is not changed by the way content is protected.

[12] Some commentators argue that the DRM protection should not be limited if the content provider can engage in nearly perfect price discrimination in a DRM system. Generally, the intertwining of technological and contractual protection in a DRM system offers numerous means to engage in price discrimination. However, it is a highly contested issue whether such price discrimination would really render limitations to the protection unnecessary; see [12-14].

because consumers simply will not buy them. Therefore, no action by the legislator or the courts has to be taken to limit DRM protection because it is the competition among vendors how consumers are protected in the DRM field (see [5, at 1453]).

However, this view assumes that well-functioning competition between different DRM systems or producers of DRM-protected content exists. This is questionable at least. Within DRM systems, information asymmetries, indirect network effects and lock-ins can occur, leading to market failures and thereby preventing well-functioning competition. Therefore, many commentators argue that it is the law that has to limit the protection of DRM systems in order to preserve fair use and other public values in the DRM field.

6.1.2 Legal Perspective

From a strictly legal perspective, the necessity to limit the protection by DRM systems becomes even more obvious. Copyright limitations such as the fair use defense in the U.S. or the more differentiated provisions in Continental Europe serve important societal goals. They preserve the free flow of information, freedom of speech and functioning competition. They induce the creation of new works, serve educational and cultural purposes, enable criticism, comment, parody, news reporting and other uses in the public interest and sometimes even protect privacy interests.

The justifications for these limitations are valid in DRM systems as well. Basically, DRM systems enable the content provider to create his own copyright law and determine the scope of protection by himself. Thereby, content providers tend to protect their own interests in DRM systems without paying adequate attention to interests of users or the society at large. And in fact, recent examples in the ebook sector demonstrate that DRM systems currently available prevent uses that would be permissible under traditional copyright limitations.

Nevertheless, some commentators argue that it is not necessary to limit the protection by DRM systems because the content is always available in other, less-protected formats: If it is impossible to extract a movie clip from a DRM-protected DVD for educational purposes, the consumer can still use a much-less protected VHS version for extraction. However, this argument is flawed in two ways. Firstly, there will be more and more content which is only available in a DRM-protected format. Secondly, in numerous jurisdictions it is highly questionable whether such a "fair use defense of inferior quality" could be legally constructed.

In summary, the intertwining means of protection in a DRM system have the potential to supplant copyright protection. However, no real reason seems to be in sight why the limitations to copyright protection may become obsolete as well. While the content provider is able to protect himself by the means of protection in a DRM system, the protection of the consumers and the society at large still depends on the law. Therefore, copyright law might transform itself from a body of law that protects creators to a consumer-protection statute. As Lawrence Lessig puts it: "The problem will center not on copy-right but on copy-duty – the duty of owners of protected property to make that property accessible" ([18, at 127]).

6.2 Copyright Law as a Safety Net

Besides limiting the protection offered by a DRM system, copyright law can have some other purposes as well in the DRM context. It is an oversimplification that a content provider can effectively protect himself by using technology and contracts. There will be numerous instances in a real-world DRM system where the technological and/or contractual protection fails: Contracts can be void or unenforceable. Technological protection can be defeated; the supporting circumvention prohibitions do not cover every attack and every person involved in an attack. In such situations, a right is useful that is effective against all the world: the protection of content providers by copyright law could fill protection gaps left open by the DRM protection. However, copyright law will not serve as the primary means of protection for content providers, but will only step in as a safety net when all other means of protection in a DRM system fail (see figure 2).

7 Law as a Limitation to the Paradigm Shift in Protection

As section 6 has shown, it seems to be necessary to limit the protection of DRM systems by law. As the different means of protection are interchangeable to a large extent (see above, section 5.1), this applies to all means of protection used in a DRM system. Overall, this analysis leads to the following completed interaction of different means of protection in a DRM system (see figure 2):

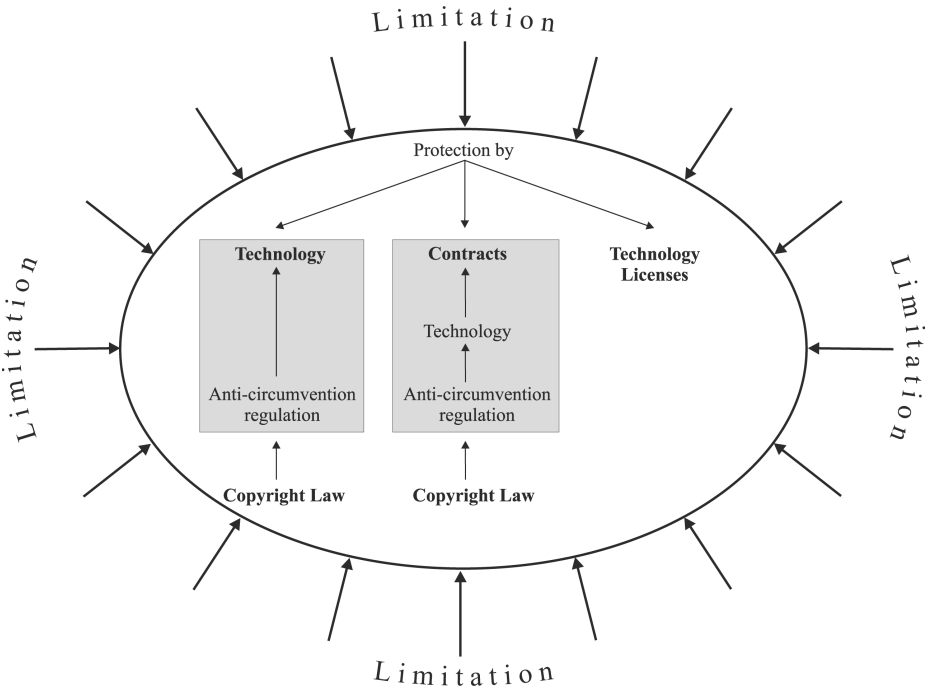

Fig. 2. Different means of protection in a DRM system (2)

In the following section, a short overview is given concerning whether and how legislators in the U.S. and Europe have responded to this need to restrict the different means of protection in a DRM system.

7.1 Limitation of the Protection by Contracts

In a DRM system, the content provider could in principle override copyright limitations such as the fair use defense by employing a contractual protection scheme. In the software sector, contractual terms forbidding the reverse engineering of software have been known for years. This raises the question whether the balance between the interests of copyright owners and the public as determined by copyright law can be altered by contractual arrangements. In the U.S., the tension between copyright and contract has attracted a significant amount of attention among legal scholars. The discussion reached its summit with an important decision by the 7th Circuit Court of Appeals ([5]) and the drafting of the public policy provision of the "Uniform Computer Information Transactions Act" (UCITA, see [6]). Under current U.S. law, DRM contract terms can be unenforceable if they are found to be unconscionable, in violation of public policy or of basics of the federal intellectual property scheme. Nevertheless, the scope of permissible DRM contract terms is still unclear under U.S. law and will probably remain so for some time.

In Europe, until now astonishingly the tension between copyright limitations and contractual arrangements has not been discussed a great deal. The European directives in the copyright area contain only very isolated provisions that prohibit the overriding of copyright limitations by contract. The recently adopted Copyright Directive of 2001 states explicitly that copyright limitations as defined in the directive should not prevent "contractual relations designed to ensure fair compensation for the rights holders" ([2, at 14]). In some member states of the European Union, blanket provisions of consumer protection statutes can limit the contractual freedom.

7.2 Limitation of the Protection by Technology Licenses

Copyright limitations can be invalidated by technology license agreements. If a hardware manufacturer is obliged by a technology license to manufacture only devices that do not allow the consumers to make personal copies of DRM-protected content, such a license term in fact abrogates copyright limitations. So far, this aspect of technology licenses has not been addressed at all in the legal discussion of DRM systems.[13]

7.3 Limitation of the Protection by Technology

Copyright limitations can be overridden by technological protection measures as well. In order to reconcile both in DRM systems, several regulatory options are available (see [19]).

---

[13] Only the U.S. Federal Communications Commission dealt with this aspect in its examination of the "POD Host Interface License Agreement", see [7, at 15, 19, and the separate statement of Commissioner Gloria Tristani].

7.3.1 Direct Influence on the Design of Technological Protection Measures

The first regulatory option for a legislator is to enact provisions that directly affect the design of technological protection measures. For instance, the legislator could mandate by law that technological measures must allow a certain number of copies for private or educational purposes without any additional permission by the content provider. Worldwide, the legislators only rarely take this approach. In Europe, article 3 (a) of the revised Television Directive of 1997 [20] requires that certain "events of major importance for society" (e.g. sports events such as the Olympic Games) be available not only on technologically protected pay TV channels. Whereas this statutory limitation of technological protection measures is not based on copyright considerations, it uses the same regulatory approach as described in this subsection.

7.3.2 Limiting the Anti-circumvention Protection

The second regulatory option to solve the tension between technological protection measures and necessary limitations to this protection is to restrict the legal protection of technological protection measures. The legislator could deny the protection by anti-circumvention provisions in certain cases. Without legal protection, there is no reason why the user should not be allowed to circumvent the technological protection. Basically, this approach gives the user a "right to hack" technological protection measures in certain cases specified by law.

This approach has been taken by the U.S. "Digital Millennium Copyright Act" (DMCA) of 1998. The very broad protection of technological access and usage control measures in 17 U.S.C. § 1201 (a) and (b) is limited by several very specific exceptions in § 1201 (d)-(j) (protecting libraries, law enforcement, reverse engineering, encryption research, privacy and security testing). Nevertheless, the DMCA has produced lots of legitimate criticism (see [21]). Firstly, several of the exceptions to the anti-circumvention provisions do not authorize the creation of tools necessary for benefiting from the exception. Essentially, this makes the exceptions meaningless. Secondly, there is no exception to the anti-circumvention protection that is as broad as the fair use defense to copyright law. There are numerous uses that are lawful under traditional copyright law but not under DMCA's anti-circumvention provisions. It is difficult to see a good reason for this differentiation. Finally, the relationship between the anti-circumvention provisions and the protection of free speech under the First Amendment to the U.S. Constitution remains a complex and unresolved problem. Basically, these are the issues that lie beneath many of the current legal quarrels concerning the DMCA, especially the DeCSS, Felten, Ferguson and Sklyarov cases.

7.3.3 "Key Escrow" Approach

A third regulatory option tries to evade some of the disadvantages of the approaches aforementioned. Under this approach, a consumer who benefits from a limitation to DRM protection would not be allowed to develop or distribute circumvention devices as it is the case under the precedingly described approach. Rather, he would be entitled to obtain appropriate means (circumvention devices, decryption keys etc.) from some instance in order to circumvent the technological protection (see [22, at 99-104], [19]). This approach resembles the "key escrow" approach taken in the crypto debate

as in both cases encrypted communications can be decrypted with appropriate tools that are legally available under certain circumstances from a specified authority.[14]

In the DRM context, this authority could be placed in the hands of either the content providers themselves or a trusted third party. As was shown above, copyright limitations serve public interests that are very often not congruent with the content providers' interests. Therefore, it would be a much better idea to charge an independent trusted third party with the administration of such a key escrow system. Otherwise, the content providers could unjustifiably refuse access to circumvention tools when the circumvention ran contrary to their own interests.

In the European Union, the Copyright Directive of 2001 [2] basically employs a modified "key escrow" approach. According to the lengthy and hardly understandable article 6 (4) of the directive, under certain circumstances content providers can be required by law to make circumvention devices or services available to consumers who benefit from some copyright limitation.[15] However, the provision itself severely restricts the scope of this "key escrow" approach in several ways. The most important restriction is that the possibility for the legislator to establish a key escrow system depends on the business model the content provider chooses: If the content provider offers his DRM-protected content over the Internet and if he conditions the access to the content on the prior formation of a contract (e.g. by using click-wrap contracts), the legislator is not allowed to establish any "key escrow" system at all (see article 6 (4) (4) of the directive). By choosing a specific business model, content providers can dispose of all copyright limitations – a highly questionable development.

Moreover, the "key escrow" approach has some general flaws as well (see [19, at 16-17]). Before benefiting from a limitation, a consumer would have to contact a "key escrow agency" in order to obtain the appropriate circumvention devices. Due to considerable transaction costs, this could have chilling effects significantly diminishing the total number of fair uses made in a society. The "key escrow" approach could lead to a centralization of copyright limitations where only a few actors determine who benefits from such limitations for what purposes.

Ultimately, one will have to get used to the fact that no silver-bullet solution exists for reconciling technological protection measures with necessary limitations to this protection. Each approach has some drawbacks. The current regulations in the U.S. and the European Union each are overly complex and inconsistent. Unfortunately, we are far away from a coherent solution of the tension between technology and public interests in the DRM field.

8 Conclusion

Within DRM systems, content providers protect their interests by the combination of technology, contracts, anti-circumvention regulations and technology license agree-

[14] The idea of the "key escrow" or "key recovery" approach was to establish trusted third parties that keep copies of the users' private decryption keys (or at least of parts thereof). Thereby, the prosecution authorities and intelligence services would have the ability to intercept encrypted communications and decrypt them properly.

[15] However, this does not seem to be the only approach allowed under article 6 (4).

ments. The protection by traditional copyright law plays only a minor role as a safety net. Rather, the intertwining of the different means of protection mentioned could supplant copyright protection to a large extent. Legislators support this development by enacting anti-circumvention regulations that protect the content provider only indirectly and by treating shrink-wrap licenses as enforceable contracts. There are some dangers to this development, however. Firstly, it is far from clear that content providers really need the combination of five different means of protection (technology, contracts, technology licenses, anti-circumvention regulations and copyright law) instead of one (copyright law). Unfortunately, the assumption that such a "hyperprotection" is necessary is rarely challenged. Secondly, in DRM systems the control over the design of informational rights is shifted into the hands of private parties, who may or may not honor the interests of third persons or the society at large. It is the law that has to react to this "overprivatization" and limit the different means of protection in a DRM system.

These features of DRM regulation – an increasing protection by technology and contracts, an increasing privatization of protection, the statutory limitation of this privatization to preserve public values as well as the retreat of the legislators to mere indirect regulations – are common to many areas of Internet law. For instance, in the privacy field, discussions are going on as to whether consumers can protect their privacy interests by contractual licenses or privacy-enhancing technologies (*protection by contract or technology*). Concerning the tension between domain names and trademarks, the "Internet Corporation for Assigned Names and Numbers" (ICANN) has established a dispute resolution mechanism (Uniform Dispute Resolution Policy, UDRP). It enables trademark holders to challenge the registrant of a domain name and potentially gain control over the name. By a pyramid of contracts, ICANN – which is a private entity – obliges every domain name registrant to participate in such dispute resolutions. Some commentators have criticized this as the creation of a new body of international, but private trademark law (*privatization of protection*). Statistical analyses of the cases decided so far under the UDRP also suggest that public values (e.g. the use of domain names for criticism or parody purposes) might not be adequately preserved in this system (*tension between private ordering and public values*). Concerning the protection of minors on the Internet, private companies have developed filtering software that deny minors access to harmful content (*protection by technology*). It is no longer the state that provides this protection, but rather private software companies (*privatization of protection*). Many commentators have criticized such filtering software as means of "private censorship" (*tension between private ordering and public values*).

In such a context, it is no longer the role of the law alone to solve the regulatory problems at stake. Rather, the law has to provide a framework in which other regulators (e.g. technology or market forces) can evolve securely and effectively. The role of the law diminishes to a structural and backup responsibility. Questions of how to regulate self-regulation become vitally important.

Confronted with the myriad of problems in the DRM context, the solutions offered by the different disciplines appear disillusioning. The *technological* development of DRM systems is not yet complete. Large problems remain in the area of system security, interoperability and system integration. The *economic* analysis of DRM systems, e-commerce and the information society in general still poses numerous unresolved

problems. From a *business* perspective, it is an open question which business model for distributing digital content will prevail and what level of security measures and usability restrictions the consumers will be willing to accept in a DRM system. In the *legal* area, the situation is no better by any means. Difficult legal questions remain unresolved. Legislators enact overly complex statutes the implications of which nobody can really foresee.

This article did not try to solve these problems. Instead, it tried to give an overview of some of them and to show that they can be grasped much better when one looks at them from a multidisciplinary perspective. Furthermore, this article did not cover all aspects of DRM. While it viewed DRM systems mainly as tools to prevent consumers from unauthorized copying and to control the use of digital content, DRM systems can be also viewed as instruments to enable digital distribution platforms where innovative business models can be implemented. A comprehensive analysis of DRM systems would need to take such business aspects as well as social implications into account and interweave the results with other parts of the analysis of Digital Rights Management.

References

1. Bechtold, Stefan: Vom Urheber- zum Informationsrecht – Implikationen des Digital Rights Management, Munich 2002
2. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society. Official Journal of the European Communities L 167, June 22, 2001, pp. 10-19
3. Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access. Official Journal of the European Communities L 320, November 28, 1998, pp. 54-57
4. Universal Music Group/InterTrust Technologies Corporation: *Bluematter End User License Agreement*, http://offers.bluematter.com/sniffer/terms.htm (visited Dec. 11, 2001)
5. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447-1455 (7th Cir. 1996)
6. UCITA online, http://www.ucitaonline.com (visited Dec. 11, 2001)
7. Federal Communications Commission: *In re Implementation of Section 304 of Telecommunications Act of 1996*, 15 F.C.C.R. 18,199 (Sep. 18, 2000)
8. OpenCable Initiative, http://www.opencable.com (visited Dec. 11, 2001)
9. Landes, William M./Posner, Richard A.: *An Economic Analysis of Copyright Law*, 18 Journal of Legal Studies 325-363 (1989)
10. Pindyck, Robert S./Rubinfeld, Daniel L.: *Microeconomics*, 5th edition, Upper Saddle River 2001
11. Posner, Richard A.: *Economic Analysis of Law*, 5th edition, New York 1998
12. Fisher, William W.: *Property and Contract on the Internet*, 73 Chicago-Kent Law Review 1203-1256 (1998)

13. Boyle, James: Cruel, Mean, or Lavish? Economic Analysis, Price Discrimination and Digital Intellectual Property, 53 Vanderbilt Law Review 2007-2039 (2000)
14. Gordon, Wendy J.: Intellectual Property as Price Discrimination: Implications for Contract, 73 Chicago-Kent Law Review 1367-1390 (1998)
15. Netanel, Neil Weinstock: *Copyright and a Democratic Civil Society*, 106 Yale Law Journal 283-387 (1996)
16. Merges, Robert P.: The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce, 12 Berkeley Technology Law Journal 115-136 (1997)
17. Lemley, Mark A.: *The Economics of Improvement in Intellectual Property Law*, 75 Texas Law Review 989-1084 (1997)
18. Lessig, Lawrence: *Code and Other Laws of Cyberspace*, New York 1999
19. Burk, Dan L./Cohen, Julie E.: *Fair Use Infrastructure for Copyright Management Systems*, 2000, http://papers.ssrn.com/abstract_id=239731 (visited Dec. 11, 2001)
20. Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities. Official Journal of the European Communities L 202, July 30, 1997, pp. 60-71
21. Samuelson, Pamela: Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised, 14 Berkeley Technology Law Journal 504-566 (1999)
22. Stefik, Mark: The Internet Edge. Social, Legal, and Technological Challenges for a Networked World, Cambridge 1999