Abstract

Over the last ten years, legislators and courts worldwide have created a comprehensive legal framework surrounding Digital Rights Management (DRM). Starting from a description of the technologies underlying DRM, the article analyzes the implications of this legal framework in the U.S. and the European Union. Compared to other contributions in the field, the article stresses that the real innovation of DRM systems is not the protection of content by technology or some other means of protection alone. Rather, it is the intertwining of different means of protection (technology, contracts, technology licenses, anti-circumvention regulations and traditional copyright protection) that lead to the unique problems of DRM. Furthermore, the article analyzes several patent and know how license agreements that deal with DRM technologies in detail.

The article demonstrates that, both in the U.S. and the European Union, this intertwining of different means of protection may lead to a new "property right" making copyright protection obsolete. It also highlights that there is a danger of over-protection: questions of fair use and droit d'auteur 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 doubtful at least – it is the law that must provide a solution. The article analyzes and compares the different solutions the U.S., the European Union and Germany have adopted concerning the relationship between copyright limitations and the protection by technology, contracts, and technology licenses. In particular, the article compares the solutions provided in § 1201 of the U.S. Digital Millennium Copyright Act of 1998 and Art. 6 (4) of the European Copyright Directive of 2001.
Table of Contents

I. Introduction ................................................................. 323
II. Different Means of Protection in a DRM System ...................... 325
   A. Protection by Technology ........................................... 326
      1. Overview ......................................................... 326
      2. Supporting Protection by Anti-Circumvention Regulations ... 331
   B. Protection by Usage Contracts ...................................... 339
      1. Overview ......................................................... 339
         a) Examples of DRM Usage Contracts ...................... 339
         b) Enforceability of DRM Usage Contracts .............. 341
      2. Supporting Protection by Technology ......................... 344
      3. Supporting Protection by Anti-Circumvention Regulations ... 346
   C. Protection by Technology Licenses .................................. 347
III. Paradigm Shift in Protection ......................................... 352
   A. Intertwining Means of Protection .................................. 352
   B. Creation of a Privatized "Property Right" ......................... 355
IV. Necessity of Copyright Law ........................................... 359
   A. Copyright Law as a Safety Net .................................... 359
   B. Overextension of DRM Protection .................................. 359
V. Law as a Limitation of the DRM Protection .......................... 364
   A. Limitation of the Protection by Contracts ....................... 365
   B. Limitation of the Protection by Technology Licenses .......... 367
   C. Limitation of the Protection by Technology ..................... 368
      1. Direct Influence on the Design of Technological Protection Measures ... 369
         a) In Theory ..................................................... 369
         b) In Practice .................................................. 370
      2. Indirect Regulation by Establishing a "Right to Hack" .......... 371
         a) In Theory ..................................................... 371
         b) In Practice .................................................. 372
      3. Indirect Regulation by Creating a "Key Escrow" System ........ 374
         a) In Theory ..................................................... 374
         b) In Practice .................................................. 376
      4. Removing Market Failures ........................................ 379
         a) In Theory ..................................................... 379
         b) In Practice .................................................. 380
      5. Combination of Different Regulatory Approaches ............... 381
VI. Conclusion ............................................................... 381

STEFAN BECHTOLD
Digital Rights Management in the United States and Europe

I. INTRODUCTION

Throughout its history, copyright law has always evolved in response to disruptive technological changes. In recent years, the Internet and other digital communication technologies have once again begun to challenge the scope and justification of copyright law. Unlike earlier challenges, however, the implications of this challenge are Janus-faced. On the one hand, it is extremely difficult to take legal action against copyright infringers in communication networks. The advent of music file sharing networks such as the former Napster system, Gnutella, KaZaA, and Morpheus has brought the world's musical heritage to everyone's computer at a negligible cost. Accordingly, the recording industry has accused such networks of enabling mass-scale piracy and severely hampering revenue opportunities for content industries.

On the other hand, digital technologies provide many tools through which digital content may be securely distributed under the auspices of its respective rights holders. Indeed, as a now popular slogan aptly states, the answer to the machine may lie in the machine. Digital Rights Management (DRM) promises to offer a secure
framework for distributing digital content, be it music, video, works in writing or even raw data. DRM ensures that content providers—in particular copyright owners—receive adequate remuneration for the creation of the content that is distributed over the DRM system. Compared to traditional copyright law, DRM promises an unprecedented degree of control over the entire distribution chain and the usage of digital content.

While DRM is en vogue these days, no generally accepted definition for the term “Digital Rights Management” exists. In their weakest form, DRM systems prevent or impede consumers from copying digital content. In their strongest form, they enable complex business models in which consumers have to pay for the individual use of digital content (“pay-per-use”). Today, DRM components may be found in DVD players and discs which use up to ten different technological protection measures. Pay TV decoders, which decrypt pay TV programs and enable pay-per-use models, are also examples of today’s DRM systems. Furthermore, new online music services such as Apple’s iTunes service use extensive DRM systems to control whether consumers can copy music or burn it onto CDs. Finally, DRM solutions are being integrated into standard audio and video software players, ebook reading software, operating systems and mobile devices.

While DRM uses various technologies to secure digital content, it is not only a technological phenomenon. From an organizational pers-

tem, see Peter Biddle et al., The Darknet and the Future of Content Distribution, in Digital Rights Management—Technological, Economic, Legal and Political Aspects 344 (Eberhard Becker et al. eds., 2003); Stuart Haber et al., If Piracy is the Problem, is DRM the Answer?, in Digital Rights Management—Technological, Economic, Legal and Political Aspects 224 (Eberhard Becker et al. eds., 2003).


6. In fact, DRM is not even a generally accepted term for the technologies it intends to describe. Some commentators use the terms “Electronic Copyright Management System” (ECMS), “Copyright Management System” (CMS), “Automated Rights Management” (ARM), “Electronic Rights Management System” (ERMS), “trusted systems”, and “Intellectual Property Rights Management” (IPRM). As used in this article, the term “Digital Rights Management” has a broader scope. DRM architectures range from simple copy-prevention technologies to comprehensive secure distribution systems. Furthermore, the term “Digital Rights Management” is not only used to cover a great number of different technologies by which digital content can be secured. It also covers the protection of digital content by various legal instruments as well as business and economic aspects of DRM.

7. http://www.apple.com/itunes (last visited Sept. 1, 2004).pective, DRM interoperability and standardization remain open problems to a large extent. From a business perspective, it is intriguing to examine the new business models which DRM systems could enable. From an economic perspective, DRM could challenge—jointly with other technologies associated with 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.

As it is impossible to cover all these issues in several dozen pages, the goal of this article is threefold. First, the article intends to provide an overview of what a DRM system actually is. Secondly, it analyzes what role copyright protection could still play in a DRM-suffused information environment. Thirdly, it describes the legal framework surrounding DRM systems and compares the regulatory approaches which the legislators in the United States and in the European Union have taken over the last few years.

The article proceeds as follows. Section two provides an overview of the various means by which a DRM system protects digital content. In section three, the article analyzes how the combination of these means challenges the justification of copyright law as we know it. Section four points out that copyright law will nevertheless remain important in DRM systems. In particular, statutory limitations to the different means of DRM protection seem necessary. Section five describes the regulatory options available to legislators. In addition, it analyzes the regulatory options adopted by the U.S. and European legislators over the last few years, and compares the efficiency of these regulatory instruments. Section six concludes the article.

II. DIFFERENT MEANS OF PROTECTION IN A DRM SYSTEM

As this section will describe, DRM systems use various technological protection measures to prevent digital content from being distributed without the rights holder’s consent. However, DRM protection is not synonymous with technological protection. DRM systems also employ usage contracts and technology license agreements to protect digital content. In addition, anti-circumvention regulations, which have been adopted over the last several years both in the U.S. and Europe, defend technological protection measures against hacking and circumvention.

8. Although the following description of DRM technology may be a tough read for lawyers who lack any technical background, the author deems such description necessary in order to provide a sound foundation for the subsequent analysis.
A. Protection by Technology

1. Overview

In order to ensure that consumers pay for using digital content and that content providers are adequately remunerated, DRM systems use various technologies to control access to and use of digital content. Encryption technologies are of particular importance. "Digital containers" enable the durable encryption of distributed content, even if it is stored on a local computer or passed on to friends.


11. In a DRM system based on digital containers, content is wrapped up in a cryptographic envelope. This "digital container" then gets transmitted to consumers. In consumers' devices, the content is stored in the encrypted form and is not available when a consumer wants to access the content in an authorized way. Many current DRM systems are based on this concept. See Paul B. Schneck, Persistent Access Control...
2. usage rules under which content may be accessed and used;\textsuperscript{16} and of
3. users of protected content.\textsuperscript{17}

Such metadata may be stored in the special headers of a digital content format. It may also be embedded directly into the content with so-called “digital watermarking” technologies.\textsuperscript{18} With metadata, DRM systems are not only able to control access (who, for what purpose and at what time), they can also control the geographical distribution of protected content. The “regional code playback control” used in the DVD standard, for instance, prevents European consumers from playing U.S. DVDs on their domestic DVD players.\textsuperscript{19}


16. See infra text accompanying notes 103-110.

17. DRM systems employ numbering systems that identify either the device of a particular user, the content the user accesses, or the decryption keys used by the user. User devices may be identified, e.g., by unique “IP addresses” of computers connected to the Internet or by unique identification numbers of hardware components; see Jonathan Zittrain, Copyright-Based ID: Rights Managed and Trusted Systems, 52 STAN. L. REV. 1251, 1263-1268 (2000); Michael A. Fromkin, The Death of Privacy?, 52 STAN. L. REV. 1461, 1490-1491 (2000). Digital content may be identified by “digital fingerprints,” a variation of digital watermarking techniques (see infra note 18). Decryption keys can be identified by “traitor tracing” and other technologies, see Benny Pinkas & Matt Franklin, An Efficient Public Key Traitor Tracing Scheme, in ADVANCES IN CRYPTOLOGY – CRYPTO 1998, 502 (1999); Benny Pinkas, Vicky. S. Y. Yun, Threshold Traitor Tracing, in ADVANCES IN CRYPTOLOGY – CRYPTO 1999, 338 (Michael J. Wiener ed., 1999).

18. With an ideal digital watermarking technology, content is altered only to a degree that is imperceptible to the human eye or ear. Yet, the metadata that is embedded in such a digital watermark becomes inextricably interwoven with the content so that the deletion of the metadata either materially degrades the quality of the content useless. Currently, intent and content useless, is of technical and empirical level whether real-world watermarking technologies can ever provide such security and robustness. For more information on digital watermarks, see STEFAN C. KATZENBEISER & FABIAN A. PETITCOLAS, INFORMATION HIDING TECHNIQUES FOR STEGANOGRAPHY AND DIGITAL WATERMARKING (2000); INGRID C. COX ET AL., DIGITAL WATERMARKING (2001); NEIL F. JOHNSON ET AL., INFORMATION HIDING: STEGA-NOGRAHY AND WATERMARKING (2001); Fabian A. P. Petitcolas et al., Information Hiding – A Survey, 87 PROCEEDINGS OF THE IEEE 1062 (1999); Frank Hartung & Martin Kutter, Multimedia Watermarking Techniques, 87 PROCEEDINGS OF THE IEEE 1079 (1999); Cumard et al., supra note 15, at 29-32; http://www.watemarkingworld.org (last visited Sept. 1, 2004); http://www.petitcolas.net/fabien/watermarking (last modified June 22, 2004).

19. The DVD regional code playback control divides the world into six regions (North America; Western Europe, South Africa, Middle East and Japan; Southeast Asia; Australia, New Zealand and South America; Africa and Russia; China). DVDs distributed in each of these regions can only be played on a player purchased in the same region; see Taylor, supra note 13, at 187-190; STEFAN BECHTOL, VOM URHEBER-ZUM INFORMATIONSRECHT – IMPLIKATIONEN DES DIGITAL RIGHTS MANAGEMENT (2004). In order to provide a uniformly high level of security, various technologies are used to ensure the integrity and authenticity of digital content, its accompanying metadata as well as the hardware and software components of a DRM system.\textsuperscript{20} In addition, tamper-resistant hardware and software makes it more difficult for hackers to crack the security of a DRM system.\textsuperscript{21} Some DRM systems use specialized search engines and related technologies to discover unauthorized content on the Internet.\textsuperscript{22} Analog protection systems and digital watermarks intend to render even the analog copying of protected content more difficult.\textsuperscript{23}

DRM systems do not only provide passive protection mechanisms. Rather, they also employ various means that prevent or respond actively to security breaches. Specialized filters\textsuperscript{24} may block access to pirated content. “Fair-exchange protocols” use technology to ensure that the consumer receives access to protected content only if he complies with the terms of the license. For more information, see Jeffrey Reisman, ‘Providing Strong Digital Rights Management’, in PROCEEDINGS OF THE 11TH ANNUAL DIGITAL RIGHTS MANAGEMENT CONFERENCE, 381 (2004).

20. Possible technologies include digital signatures, hash functions, challenge-response protocols, and digital watermarks. For more information, see KOEGER & COX, supra note 17, at 106-108; see also ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO COUNTERMEASURES (2004).

21. At least in the commercial context, tamper-resistant hard- and software is far from available to offer 100% protection against unauthorized use. For an overview of tamper-resistant smartcard architectures, see ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO COUNTERMEASURES (2004).

22. For such a specialized search engine, see Hector Garcia-Molina et al., Safeguarding and Charging for Information on the Internet, in PROCEEDINGS OF THE 14TH INTERNATIONAL CONFERENCE ON DATA ENGINEERING 182 (1998).

23. In the videocassette sector, the two analog copy-protection technologies developed by Macrovision Corp. (“automatic gain control” and “ColorStripe”) are widely used, see Taylor, supra note 13, at 196.

after having paid the corresponding fees. Furthermore, DRM systems have the ability to 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. In the whole distribution chain, from the creation of content to its consumption by individual users, it must be assured that no single device or component can transmit the content in an unencrypted form, as this would compromise the security of the DRM system. DRM standards can achieve this goal by ensuring that different devices interoperate in a proper and secure way. Standardizing DRM systems is a complex task as the opposing interests of various affected parties—rights holders as well as the entertainment, computer, broadcasting, and telecommunications industries—have to be taken into account. Various working and standardization groups attempt to coordinate the development process of DRM technologies. Important DRM standards include the “Content Scramble System” (CSS) which is used in video DVDs, the aforementioned CGMS, the “Content Protection for Recordable and Prerecorded Media” (CPRM/CPFM), and the “Digital Transmission Content Protection” (DTCP), the “High-bandwidth Digital Content Protection” (HDCP), and the “Trusted Computing Group” (TCG).

In summary, DRM is a general term for a set of intertwining technologies that may be used to establish a secure distribution chain for digital content.

2. Supporting Protection by Anti-Circumvention Regulations

Although DRM systems promise to provide a high level of technological security, no commercially-viable system will be technologically 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, special legal regulations have been created over the last few years that outlaw the circumvention of technological protection measures and the production and distribution of devices which may be used to circumvent such measures (so-called “preparatory activities”).

On the international level, such provisions may be found in two treaties adopted in 1996, under the aegis of the World Intellectual Property Organization (WIPO). Article 11 of the WIPO Copyright Treaty (WCT), which went into force on March 6, 2002, outlaws the circumvention of effective technological measures used by copyright holders in order to protect their rights, and Article 12 of the WIPO Performances and Phonograms Treaty (WPPT), which came into force in 2001, outlaws the circumvention of effective technological measures used by producers of phonograms in order to protect their rights, and the protection of performance.

33. DTCP protects the transmission of digital content between different hardware components, e.g., between a computer and a digital video recorder. See http://www.dtcp.com (last visited Sept. 1, 2004); Marks & Turnbull, supra note 10, at 208; Block note 5, supra note 13, at 1270-1271.

34. HDCP protects the transmission of digital content between a computer system and a connected monitor. See http://www.digital-cp.com (last visited Sept. 1, 2004); Taylor, supra note 13, at 199-200, 490.

35. TCG is a computer industry working group aimed at developing a standard for a trusted hardware computing platform; see http://www.trustedcomputinggroup.org (last visited Sept. 1, 2004); TRUSTED COMPUTING PLATFORMS—TCPA TECHNOLOGY IN CONTEXT (Siany Pearson ed., 2003); Bechtold, supra note 12, at 633-650; Stefan Bechtold, Trusted Computing Blog, at http://cyberlaw.stanford.edu/blogs/bechtold/ (last modified May 7, 2004).


37. The idea of anti-circumvention regulations is not totally novel. In 1984, a provision was introduced into U.S. communications law that outlawed the unauthorized interception of encrypted satellite TV transmissions by private individuals 47 U.S.C. § 605 (2004); see Steven DeBraun, The Piracy of Subscription TV—a Marketplace Solution? An Unauthorized Reauthorization of Copyrights, 34 UCLA L. REV. 445 (1986); Robert D. Hayden, Who Owns The Air? Unraveling the Satellite Viewing Rights Dilemma, 20 LOY. L.A. L. REV. 145, 161-166 (1986). 17 U.S.C. § 1002 (c) (2004), which was introduced into U.S. copyright law by the Audio Home Recording Act of 1992, prohibits devices that circumvent the “Serial Copy Management System” (SCMS); for more information on SCMS, see supra note 14. Article 1707 of the North American Free Trade Agreement (NAFTA), which went into force in 1994, requires that each NAFTA country provide adequate protection of encrypted satellite TV transmissions against unauthorized circumvention devices. Furthermore, §§ 296-299 of the Betamax Copyright, Designs, and Patents Act of 1988 provided a comprehensive set of anti-circumvention regulations. Despite all these scattered provisions, it was only in the last few years that comprehensive anti-circumvention regulations were passed by legislators worldwide.
owners to protect their works. A similar provision protecting performers and producers of phonograms may be found in Article 18 of the WIPO Performances and Phonograms Treaty (WPPT), which went into force on May 20, 2002. Furthermore, Articles 2, 3 and 6 of the Convention on Cybercrime of 2001, which was negotiated by the Council of Europe and to which many European countries as well as the U.S., Canada and Japan are signatory countries, may ban the circumvention of DRM security measures and related preparatory activities as well. Finally, over the last two years, the United States has concluded several bilateral trade agreements with countries such as Singapore and Australia, that include detailed provisions regarding the circumvention of technological protection measures.

In the United States, the U.S. Congress enacted complex anticircumvention regulations as part of the Digital Millennium Copyright Act (DMCA) of 1998. The DMCA arranges its anti-circumvention provisions along two dimensions. First, it distinguishes between technological protection measures that “control access to a work” (“access control”) and measures that “protect rights of the copyright owner” (so-called “usage control”). Secondly, it distinguishes between the actual circumvention of technological protection measures and preparatory activities, in particular the production and distribution of tools that can be used to circumvent such measures. Whereas the DMCA prohibits the actual circumvention and preparatory activities in regard to access control technologies, it only targets preparatory activities in regard to usage control technologies.

Over the last few years, courts have applied the anti-circumvention provisions of the DMCA in several cases. In 1999, a federal district court issued a preliminary injunction barring a software company from offering a computer program that circumvented a regional code management system in Sony’s “Playstation” game console. In 2000, another district court granted a preliminary injunction against a company offering software that circumvented a copy protection technology in the widely-used RealNetworks audio and video player software. In August 2001, a Russian software company was indited for marketing a software program that circumvented a DRM protection in Adobe’s ebook reader software. In November 2001, the U.S. Court of Appeals for the Second Circuit upheld an earlier decision barring a magazine from publishing (or even linking to) the source code of a software program (called “DeCSS”) that could be used to circumvent the “Content Scramble System”

Law, 18 BERKELEY TECH. L.J. 619 (2003); see also infra text accompanying note 73. For an important decision that analyzes the relationship between an alleged "access right" under the DMCA and the traditional rights as granted by the Copyright Act, see Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004) (stating on pp. 1200-1201 that "the broad policy implications of considering 'access' in a vacuum devoid of 'protection' i.e., the protection granted by traditional copyright law are both absurd and disastrous"). The term "usage control" is imprecise, as the mere use of a work is not covered by copyright law; for the situation in the U.S., see Niva Elkin-Koren, Copyright Policy and the Limits of Freedom of Contract, 12 BERKELEY TECH. L.J. 93, 106 (1997); Mark A. Lemley, The Economics of Improvement in Intellectual Property Law, 75 TEM. L. REV. 988, 1014 (1997); for the situation in Germany, see BUCHHOLD, supra note 19, at 220 note 112.

17 U.S.C. § 1201(b)(1) (2004). One reason for the omission of an anti-circumvention regulation concerning the actual circumvention of usage controls is that in such cases, traditional copyright law applies; see U.S.S. Rep. No. 105-190, at 12 (1998); Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1185 (Fed. Cir. 2004) (see also Nimmer, 2 supra note 42, at 431. Another reason is allegedly that through this omission, copyright limitations such as the fair use defense may be preserved; see Library of Congress, Copyright Office, supra note 43, at 64557.

For more information on regional code management systems, see supra text accompanying note 45.

47. See supra note 48; see also supra note 49.

48. See supra note 49; see also supra note 48.

49. See supra note 49; see also supra note 48.
employed in DVDs. In February 2004, a federal judge in California ruled that a software program which allowed customers to make backup copies of DVDs violated the anti-circumvention provisions of the DMCA.

In October 2004, the U.S. Court of Appeals for the Sixth Circuit vacated an earlier DMCA-related injunction which a manufacturer of laser printers had sought against a manufacturer of toner cartridges that competed with the printer manufacturer’s own cartridges. In August 2004, the U.S. Court of Appeals for the Federal Circuit upheld a summary judgment preventing a manufacturer of garage door opener systems from using the DMCA to hinder competitors in the downstream market of hand-held portable transmitters from offering transmitters that interoperate with the manufacturer’s garage door opener system. These cases are examples of a trend where companies attempt to use anti-circumvention regulations in circumstances for which they were clearly not intended: controlling downstream markets by a combination of technology and law and channeling innovation in these markets.

Besides 17 U.S.C. § 1201 (a) and (b), other anti-circumvention provisions may be found for video recorders in 17 U.S.C. § 1002 (1) (B), for DAT players in 17 U.S.C. § 1002 (c) and for satellite TV in 47 U.S.C. § 605. Furthermore, technological protection measures may be protected as trade secrets. In rare cases, traditional copyright law could apply as well, as the production and distribution of circumvention devices might, under very narrow conditions, constitute contributory copyright infringement. Finally, over the last few years, several U.S. states have been modernizing their communications security statutes. These modernized statutes, which are accompanied by lobbying efforts from the motion picture and cable service industries, include anti-circumvention regulations that, in some cases, go well beyond the scope of the regulations in the federal DMCA.

In the European Union, anti-circumvention provisions have been enacted in various Directives related to copyright law over the last few years. Article 7 (1) (c) of the Software Directive of 1991 prohibits the circulation and “possession for commercial purposes” of any tools which are solely intended to circumvent technical measures protecting a computer program. The most important European anticircumvention regulation, however, may be found in the Copyright Directive of 2001, which had to be implemented by the member states of the European Union by December 22, 2002. Article 6 (1) of this Directive prohibits the actual circumvention of any “effective” measures.

50. See supra note 30.
53. Lemmark Intern., Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004). For more information on this case that has significant impact on the whole remanufacturing industry, see Bechtold, supra note 12, at 623-626; see also Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1198-1199, 1201 (Fed. Cir., Aug. 31, 2004) (stating on p. 1201 that any understanding of the DMCA has to avoid “allow virtually any company to attempt to leverage its sales into aftermarket monopolies – a practice that both the antitrust laws... and the doctrine of copyrig... prohibit”).
54. Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004) (highlighting the differences between this case and the Lemmark case on pp. 1198-1199 and stating on p. 1201 that Chamberlain’s rejection of construction of the DMCA “would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial encryption scheme, and thereby gain the right to restrict consumers’ rights to use its products in conjunction with competing products.”)
55. For more information on this development in general, see Bechtold, supra note 12, at 619-629.
56. For some information on the latter two provisions, see supra note 37.
59. On this development, see Cunard et al., supra note 15, at 58-59. For an overview of these state laws, see Public Knowledge, 2005 State DMCA Table, at http://www.publicknowledge.org/content/reference/super-dmca-table (last visit Sept. 1, 2004).
63. However, nearly all member states, including Germany, have not met this deadline; see infra note 69.
64. The Directive provides a nearly tautological definition of an “effective” technological measure in Article 6 (3) No technological measure seems “ineffective” under this standard; see Bechtold, supra note 19, at 204; see also Thomas Hoeren, Entwurf
technological measure that is used by the rights holders of any copyright or neighboring right to protect their works. Article 6 (2) prohibits a wide range of preparatory activities, including the production, distribution, promotion, or “possession for commercial purposes” of devices that “have only a limited commercially significant purpose or use other than to circumvent”65 or are at least “primarily designed . . . [to enable] the circumvention” of technological protection measures. In general, the anti-circumvention regulations of Article 6 (1) and (2) provide a very broad protection of DRM systems.66

Article 4 of the Conditional Access Directive of 199867 prohibits the production, distribution, and promotion of illicit devices that circumvent technological protection measures. Although the Directive stems from the pay TV and broadcasting sector, it may apply to a wide variety of Internet-based DRM systems as well.68 Whereas the Computer Program and the Conditional Access Directives have been implemented into the national laws of most of the member states of the European Union, the European Copyright Directive has only re-

einer EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft, MULTIMEDIA UND RECHT 2000, 515, 529 (distinguishing between an inter action ex post (dele-
asis); Séverine Dusollier, Tipping the Scale in Favor of the Right Holders: The Anti-
Circumvention Provisions, in DIGITAL RIGHTS MANAGEMENT – TECHNOLOGICAL, ECO-
NOMIC, LEGAL AND POLITICAL ASPECTS 466-467 (Eberhard Becker et al. eds., 2003).

65. This provision attempts to exempt tools from the prohibition that may also be used for legitimate purposes (“dual use tools”), see WAND, supra note 38, at 111; but see Thomas Dreier, Die Umsetzung der Urheberrechtsrichtlinie 2001/29/EG in deut-
schisches Recht, ZEITSCHRIFT FÜR URHEBER- UND MEDIENRECHT 2002, 28, 38-39, and
Spindler, supra note 62, at 116 (both pointing out that nearly all circumvention tools
may be used for both legitimate and illegitimate purposes).

66. See also Vinje, supra note 62, at 555; Hart, supra note 62, at 62. For an anal-
ysis of the limitations to this protection by Article 6 (4) of the Copyright Directive, see infra text accompanying notes 258-274.

ber 20, 1998, on the Legal Protection of Services Based on, or Consisting of, Con-
ditional Access, Official Journal of the European Communities L 320 (Nov. 28, 1998), 54. See also BECHTOLD, supra note 19.

68. According to Article 2 (a), the Directive protects telecommunications and radio broadcast-
ings services as well as “information society services”. The term “information soci-
ey services” is defined in the Transparency Directive as “any service normally
provided for remuneration, at a distance, by electronic means and at the individual
definition is very broad and covers many transmissions over the Internet; see Dusol-
lier, supra note 51, at 290; Heide, supra note 67, at 1062-1004; WAND, supra note 98,
at 82-84; BECHTOLD, supra note 19, at 215-216; see also Justin Harrington, INFORMATION
SOCIETY SERVICES: What Are They and How Relevant Is the Definition, JOURNAL OF BUSI-
NESS LAW 190 (March 2001).

69. In Germany, Article 7 (1) (c) of the Computer Program Directive has been
implemented as § 69 f (2) of the Urheberrechtsgesetz (Copyright Act). The Conditional
Access Directive has been implemented as the Gesetz über den Schutz von zugangs-
kontrollierten Diensten und von Zugangskontrolldiensten (Zugangskontrolldienstes-
1090. The Copyright Directive has been implemented by the Gesetz zur Regelung des
Urheberrechts im Bereich der Informationsgesellschaft v. 12. 9. 2003, Bundesgesetzblatt I of
September 12, 2003, at 1777. For these implementations, see Steen Bechtold, SCHUTZ UND IDENTIFIZIERUNG DURCH TECHNISCHE SCHUTZMAßNACHEN, IN
HANDBUCH MULTIMEDIA-RECHT, Teil 7.11, Rdnr. 39-186 (Thomas Hoeren & Ulrich
Sieber eds., 2004). For an overview of the implementation of the Copyright Directive in
the United Kingdom, see Michael Hart, Implementation of the Copyright Directive
in the United Kingdom, in Maximilian Haedich, Die Umgung technischer Schutzmä-
ßnarchen durch Dritte als mittelbare Urheberrechtsverletzer, in URHEBER-
RECHT GESCHN – HEUTE – MORGEN: FESTSCHRIFT FÜR ADOLF DIETZ ZUM 65. GEBURT-
STAG 349 (Peter Ganea et al. eds., 2001).

70. For an overview of the applicable provisions in Germany, see Bechtold, supra
note 69. For an application of traditional copyright law under the doctrine of contribu-
tors see Maximilian Haedich, Umgung technischer Schutzmaßnahmen durch Dritte als
mittelbare Urheberrechtsverletzer, in URHEBERRECHT GESCHN – HEUTE – MORGEN:
FESTSCHRIFT FÜR ADOLF DIETZ ZUM 65. GEBURSTAG 349 (Peter Ganea et al. eds., 2001).

71. See Hart, supra note 62, at 62; see also Till Jaeger, Auswirkungen der EU-
Urheberrechtsreform auf die Regelungen des Urheberrechtsgesetzes für Software,
COMPUTER UND RECHT 2002, 309. This tension becomes particularly problematic if the
once clear-cut distinction between computer programs and other works protected
by copyright law blurs, see BECHTOLD, supra note 19, at 215 note 1087.
However, while the Copyright Directive should protect works, the Conditional Access Directive is targeted at protecting services.

Yet, it is at least questionable whether these theoretical distinctions will work in practice. First, it is a hard question as to whether and to what extent a “right to control access” may be distinguished from existing rights under copyright law.72 Furthermore, as most uses of a work are preceded by the access to the work, controlling access also empowers the content provider to control those uses.74 Finally, most conditional access services will include at least some copyrighted works, rendering the distinction between protecting works and services hollow as well.75

In general, the last few years have seen a spreading of anti-circumvention regulations worldwide. From a copyright law perspective, this is remarkable because, in the past, copyright merely reacted to significant changes in technology, rather than anticipating such changes.76 When the World Intellectual Property Organization adopted anti-circumvention regulations in 1996, it did so without any noteworthy practical experience in the individual countries as to what the implications of such regulations are, and without having any secure forecasts as to what the importance of technological protection measures will be in the future. The adoption of these regula-

72. Explanatory Memorandum to the Proposal for a European Parliament and Council Directive on Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, C(97) 628 final (Dec. 10, 1997), comments to Article 6 (4), at 42; but see European Commission, supra note 67, at 22-23. This distinction is similar to the distinction between access controls and usage controls in the U.S. DMCA; see supra text accompanying note 43.


74. See Bechtold, supra note 15, at 220; see also Heide, supra note 67, at 997; Ginsburg, supra note 42, at 143; Wandra, supra note 38, at 108.75. Koelman & Helberger, supra note 38, at 219. For a more detailed analysis, see Heide, supra note 67, at 1018-1019; Bechtold, supra note 19, at 219-221.

76. See supra note 1.

77. For a criticism of such rushed procedure, see Stefan Bechtold, Das Urheberrecht und die Informationsgesellschaft, in INTERESSENAUSGLEICH IM URHEBERRECHT 67 (Reto Hilty & Alexander Peukert eds., 2004).


80. The German DRM trial service “Musikdownload24” by BMG Entertainment, which ceased operation in August 2001, used very similar license agreements as well.


82. § 8(b) of the Terms of Service reads in part: “You understand that the Service, and products purchased through the Service, such as sound recordings and related artwork (‘Products’), include a security framework using technology that protects digital information and limits your usage of Products to certain usage rules established...
to burn protected content onto CD-ROMs for personal use and to use the content on three computers authorized by Apple, at any time. 

Furthermore, many DRM usage contracts expressly forbid the consumer to copy, distribute, transmit, broadcast or modify protected content or to alter or delete attached metadata and usage rules. Other common contractual terms include restrictions against downloading content on to anything other than DRM-secured devices; the limitation of, or prohibition against, burning content to CD-ROMs or DVD-ROMs; and the prohibition against copying, pasting and printing of images or text.

Yet, DRM usage contracts are not only used to protect digital content, but also to protect the security of the DRM system itself. The former Pressplay “End User License Agreement” required the consumer to consent to automatic updates of the client software, which were deemed necessary for security purposes. The consumer was also required to consent to automatic revocation of the software, or face remote shut-down if the DRM system detected a security breach. Furthermore, the consumer is regularly forbidden from policies apply. You agree to abide by the rules and policies established from time to time by pressplay. Such rules and policies will be applied generally in a nondiscriminatory manner to users of the Software, and may include, for example, required or automated updates, modifications, and/or reinstallations of the Software to address security, interoperability, and/or performance issues. These updates, modifications and the like may occur on a periodic or as needed basis without notice to you. In addition, you understand that the Software is capable of monitoring itself for security-related and tamper-detection purposes and communicating information about security incidents. Your copy of the Software and your access to certain applications that communicate with it are subject to restriction and/or revocation (such as being shut down) for security purposes or according to consistently applied Content-protection policies. You understand and agree that this would likely result in Content that was previously available for use being unavailable thereafter. A similar provision could be found in § 6(c) of the aforementioned RealNetworks End User License Agreement. (see supra note 84). “AutoUpdate: The RealOne Player, using AutoUpdate, automatically communicates with [RealNetworks]’ servers on the Internet to check for updates to [RealNetworks] and [its] partner’s software, such as bug fixes, patches, enhanced functions, missing plug-ins and new versions. . . . certain updates to RealOne Player functionality will happen automatically and without advance notification.” (8 a) added: “You agree that communications enabled by the DRM, including automatic updating of the DRM without further notice . . . .” See also Elizabeth G. Thornburg, Going Private: Technology, Due Process, and Internet Dispute Resolution, 34 U.C. Davis L. Rev. 151, 175-176 (2000). The Supplemental End User License Agreement for Microsoft Windows Media Player 9 which the user has to agree to during installation states: “If the DRM Software’s security/revocation system is compromised, owners of Secure Content . . . may request that Microsoft revoke the DRM Software’s right to copy, display and/or play Secure Content. Revocation does not alter the DRM Software’s ability to provide unprotected content. A list of revoked DRM Software is sent to your computer whenever you download a license for Secure Content from the Internet. You agree that the Microsoft revocation list is for your computer on behalf of Secure Content Owners . . . Secure Content Owners may also require you to upgrade some of the DRM components in the OS Components . . . before accessing their content.”
DRM usage contracts are legally enforceable. This is questionable as DRM usage contracts resemble "shrink-wrap licenses" for computer software.\(^{89}\)

In both the United States and Europe, the enforceability of shrink-wrap licenses was formerly unclear. For a long time, U.S. courts refused to enforce shrink-wrap licenses.\(^{90}\) In 1997, however, Judge Easterbrook of the Seventh Circuit Court of Appeals issued a landmark opinion that found a shrink-wrap license to be a valid contract.\(^{91}\) Since then, the Seventh Circuit and other courts have enforced shrink-wrap licenses as well.\(^{92}\) Furthermore, the controversial, now largely defunct "Uniform Computer Information Transactions Act" (UCITA) accepted shrink-wrap licenses as enforceable contracts to a large extent.\(^{93}\)

Remainder of the Public Domain, 26 Brooklyn J. Int'l L. 77, 79-80 (2000); The attempt to use a net of contracts in a mass market is not a new phenomenon. In the beginning of the 20th century, book publishers and record companies used similar techniques, see RCA Co. v. Whitman, 114 F.2d 86, 87 (2d Cir. 1940); Bobbs-Merrill Co. v. Straus, 210 U.S. 339 (1908); see also David Nimmer et al., The Metamorphosis of Contract into Expand, 87 Cal. L. Rev. 17, 44-45 (1999); Jessica Litman, The Tales that Article 2B Tells, 13 Berkeley Tech. L.J. 931, 939 (1998).

88. A "shrink-wrap license" is a license that is added to a retail software package and covered in a plastic or celluloid "shrink-wrap". According to some software vendors, the licenses become effective as soon as the customer tears the wrapping from the package, see ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996); Margaret J. Radin, Humans, Computers, and Binding Commitment, 75 Ind. L.J. 1125, 1134 (2000).


92. See UCITA § 209 (a) (2002); Radin, supra note 88, at 1114-1142. For more information on the UCITA in general, see Patrik A. Shah, The Uniform Computer Information Transactions Act, 15 Berkeley Tech. L.J. 85 (2000). In 2003, the National Conference of Commissioners on Uniform State Laws (NCCUSL), facing mounting opposition, decided to cease efforts to get the Uniform Computer Information Transactions Act (UCITA) of 1999 enacted in all states of the U.S. UCITA has only been enacted in Maryland and Virginia.

93. A "click-wrap license" appears on the users' computer screen and requires him or her to agree to the license terms before being able to use the software or service.

94. Clearly, the click-wrap licenses ("Schutzdumpenverträge") are enforceable contracts has been addressed by courts only rarely, but the majority of commentators deny its enforceability.\(^{95}\) Similarly, German commentators generally disapprove of the enforceability of many click-wrap licenses (often called "Enter-Verträge").\(^{96}\) However, the enforceability of both kinds of licenses under German law depends on how the licenses are designed. As long as the consumer acquires the purchased good from the same party as with whom the shrink- or click-wrap license agreement was entered into,\(^{100}\) and as long as the consumer unequivocally
manifests assent to this agreement, DRM usage contracts may be enforced under German contract law. The enforceability of click-wrap licenses is confirmed by Article 9 (1) of the European E-Commerce Directive which requires EU member states to allow “contracts to be concluded by electronic means”.

It is impossible to make broad statements about the enforceability of all shrink-wrap and click-wrap licenses in general. Whether particular terms of such licenses are enforceable depends on, for example, whether and when the consumer had sufficient opportunity to review the license terms, who the parties to the contract are, whether the license terms violate a fundamental public policy, and which laws are applicable. Yet, no fundamental obstacle exists for content providers to contractually protect their content in a DRM system. It is possible to design a DRM system and its business model in a way that such contracts are legally enforceable. Despite the criticism of U.S. court decisions that enforce shrink-wrap licenses and despite the failure of UCITA, the trend to enforce such licenses in the U.S. cannot be denied. A similar trend is evident in Europe, at least with regard to click-wrap licenses. As long as a DRM system takes the legal concerns into account and designs its usage contracts accordingly, DRM usage contracts can be enforceable. Therefore, in a DRM system, it is possible to protect content not only by technology, but also by contract.

2. Support Protection by Technology

As was described above, DRM usage contracts include usage rules that define the ways in which consumers are authorized to use and access content. These usage rules are not only expressed in legal documents, i.e. contracts, but also in machine-readable metadata. So-called “rights expression languages” (RELS) enable the content provider to express a rich set of usage rules in machine-readable metadata that may be attached to the content. 

consumer (i.e. one contract between the content provider and the consumer), then a major obstacle to the enforceability of DRM usage contracts under German law is removed; see BECHTOLD, supra note 19, at 164-165.

101. See Schuhmacher, supra note 98, at 643-644; HOREN, supra note 98, at § 432; MARBY, supra note 98, at § 389.


103. For the concept of metadata, see supra text accompanying notes 15-17.

104. Regularly, an REL only defines the way in which usage rules may be expressed in a machine-readable way. So-called “rights data dictionaries” (RDDs) are then used to define which particular conditions can be expressed in an REL, see Susanne Guth, Rights Expression Languages, in DIGITAL RIGHTS MANAGEMENT – TECH-
the contractual terms are encoded. This demonstrates that, in a DRM system, the contractual protection is supported by a technological protection. Technology makes it more difficult or even impossible to disobey contractual obligations.110

3. Supporting Protection by Anti-Circumvention Regulations

However, this technological protection of DRM usage contracts is not failsafe. Once in a while, hackers will succeed in altering or deleting usage metadata. If such attacks are successful, the content may be used without paying the appropriate fee. In order to prevent such attacks, the law provides regulations which specifically prohibit the manipulation or deletion of metadata.111

On the international level, the removal or alteration of usage metadata is forbidden by Article 12 of the WIPO Copyright Treaty (WCT) and Article 19 of the WIPO Performances and Phonograms Treaty (WPPT).112 These are very detailed provisions which served as a model for many national metadata regulations.113 A very similar provision may be found, for example, in Article 7 of the European Copyright Directive of 2001114 and in § 95c of the German Copyright Act.115 In the United States, the WCT and WPPT provisions have been implemented as § 1202 of the Digital Millennium Copyright Act.116

Although these metadata regulations differ in detail, they all follow the same path.117 In general, only metadata that identifies content, rights holders and usage rules is protected by the anti-circumvention regulations. Metadata systems that identify consumers do not benefit from this protection due to privacy concerns.118 Furthermore, metadata anti-circumvention regulations only outlaw the actual removal or alteration of metadata. Preparatory activities, such as the production of devices that may be used to remove metadata, are usually not covered by the prohibitions.119 Finally, most anti-circumvention regulations only prohibit the removal or alteration of metadata, but not the provision or distribution of false metadata.120

The supporting protection of metadata by anti-circumvention regulations highlights one of the most important features of DRM: the intertwining means of protection in a DRM system. Content providers may protect their content by contracts, which may themselves be protected by various technological protection measures, which are in turn legally protected against circumvention.

C. Protection by Technology Licenses

DRM usage contracts are not the only contractual protection used in DRM systems. Rather, technology license agreements are employed as well. Many DRM technologies are protected by patents or kept as trade secrets. If computer or consumer electronics manufacturers want to enable their devices to process content that is protected by this DRM technology, they must enter into a technology license agreement with the developer 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. Licensors of DRM technologies are either the companies which have developed the DRM technology or specialized licensing authorities that administer the licensing process on behalf of these companies.121

119. See Betchold, supra note 19, 239.

120. The exception to this rule is the United States, where provides in 17 U.S.C. § 1202 (a) (2) (2004) that no person shall "distribute or import for distribution copyright management information that is false"; see Nimmer & Nimmer, supra note 78, § 12A.10(A), at 12A-128 – 12A-132. A similar provision that applies to DAT recorders may be found in 17 U.S.C. § 1002 (d) (1) (2004).

In the scholarly debates about DRM, a fact that has been constantly overlooked is that DRM technology license agreements are used to protect the interests of content providers, although they typically are not the licensors of the DRM technology. In protracted negotiations between the content, computer and consumer electronics industry, the content industry 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. In particular, the movie industry wanted to make sure that consumers would only be able to play its movies on players that would prevent consumers from making illegal copies. The content industry therefore had a strong interest in ensuring that sufficient DRM security would be built into all consumer equipment available on the market.

As the content industry is not in the business of producing consumer equipment, it came up with a strategy to force the producers of such equipment to integrate sufficient DRM security into their devices. The content industry stated that it would release its content in a digital format only after the content has been encrypted, using an encryption technology developed by a third-party DRM technology provider. For such content to be playable on consumer devices, the manufacturers of these devices therefore have to license appropriate decoding technology from either the DRM technology provider or an affiliated licensing authority.

As no DRM technology could be successful on the market without an appropriate amount of content accessible within this system, every developer of a DRM technology component has vital commercial interests that their technology be implemented in consumer devices in the most secure way. Therefore, DRM developers license their technology on the condition that the interests of content providers are preserved when the technology is implemented in consumer devices. Due to this complex interweaving of interests, the license agreements indirectly serve the interests of content providers, even though the content providers are usually not a party to the DRM technology license agreements – they are made between DRM technology providers and consumer device manufacturers.

Although the various DRM technology licenses differ in detail, all of them exhibit striking similarities. In general, it is crucial for the commercial success of a DRM system that content be protected at every stage within the system. However, a DRM system is not a single, monolithic technology, but consists of a large number of different components. Therefore, numerous protection measures have to be combined to provide a continuous level of high security. To achieve this goal, technology licenses tie several DRM technologies together by requiring that the licensor of one specific DRM technology also use another DRM technology in its implementation. For instance, the CSS License Agreement requires that the manufacturer of standalone DVD players also incorporate regional code management technology into its players. Furthermore, the players are only allowed to transmit analog video data in a format protected by particular analog copy protection systems 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. If a DVD player, for example, transmits a CSS-protected digital video stream to another device such as a digital video recorder, the CSS license requires that this transmission be protected.


125. For a more detailed description, see Bechthold, supra note 19, at 186-189. For the following analysis, most of the publicly available DRM technology licenses were evaluated. Other technology licenses are only available subject to non-disclosure agreements. The evaluated licenses are the CSS, CPRM/CPPM, DTCP and HDCP licenses. For an overview of the underlying DRM technologies, see supra notes 30, 32-34. In addition, the Pod-Host Interface License Agreement was evaluated. This license deals with a decryption technology (“Dynamic Feedback Arrange Scrambling Technique”, DFAST) that is used in U.S. pay TV decoders. For more information, see Weinberg, supra note 122, at 287-288; Bechthold, supra note 19, at 184; Cable TV NPT 2000, supra note 124. DFAST is also licensed under other licensing terms; see Consensus Cable MSO – Consumer Electronics Industry Agreement on “Plug & Play” Cable Compatibility and Related Issues (Dec. 19, 2002), at http://www.nte.org/pdf_files/CE-NCTAAgreement.pdf; see also In re Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, Compatibility between Cable Systems and Consumer Electronics Equipment, 18 F.C.C. Red. 20,885, ¶ 75 (2003) (hereinafter: Cable TV Order 2003).

126. For an overview of the “Content Scramble System” (CSS), see supra note 30. 127. See supra note 19.


---

122. So far, the relationship between DRM technology licenses and copyright policy has only been analyzed thoroughly by Jonathan Weinberg, Digital TV, Copy Control and Public Policy, 20 CARDozo Arts & Ent. L.J. 277 (2002), for a specific license in the pay TV context. Pod-Host Interface License Agreement and by Bechthold, supra note 19, at 178-196, 405-406, for such licenses in general; see also Marks & Turner, supra note 10, at 206. For an extensive overview of current problems of DRM technology licenses that have been certified by the U.S. Federal Communications Commission to comply with its 2003 Broadcast Flag Order, see Order in the Matter of Digital Output Protection Technology and Recording Method Certifications, 19 F.C.C. Red. 15876 79-103 (Aug. 4, 2004).

123. See also Weinberg, supra note 122, at 285-286.

124. See Bechthold, supra note 19, at 180; Weinberg, supra note 122, at 286; In re Implementation of Section 304 of the Telecommunications Act of 1996, Commercial
by DTCP or HDCP. If the digital video recorder then transmits the video stream to another device, the DTCP license requires that this transmission be protected by DTCP as well. By tying together different DRM technologies, technology license agreements attempt to ensure a high system security across the whole DRM system.

DRM technology licenses also attempt directly to prevent unauthorized copying. Various licenses restrict the quality or speed by which content is transmitted, thereby making piracy less attractive as it either takes too long or leads to inferior copies. DRM technology licenses also require that DRM-enabled devices obey the usage rules of digital content that are determined by the content provider. If, for example, the content provider has embedded a digital watermark into its content prescribing that the content may only be copied once, all consumer devices that use the licensed DRM component ensure technologically that the user may indeed make only one copy.

Furthermore, DRM technology licenses include provisions to ensure that consumer device manufacturers implement the DRM technology in a robust and secure way. For this reason, manufacturers are required to use security technologies such as encryption, self-checking, and tamper-resistant hardware and software in their DRM implementations. Technology licenses further require that it at least be difficult to defeat the DRM protection through the use of professional tools such as logic analyzers, chip disassembly systems or in-circuit emulators.

If the security mechanisms implemented in the consumer devices or the underlying DRM security architecture are nevertheless defeated, the license is required to redesign or replace its affected products within clearly defined time frames. Often, the licensor also reserves the right for himself and for content providers (such as movie studios) to prevent compromised consumer devices from further accessing DRM-protected content. Finally, technology licenses prohibit manufacturers of DRM-enabled consumer equipment from producing devices or software that may be used to circumvent the DRM protection.

In summary, DRM technology licenses are used to establish a comprehensive DRM security architecture that enables secure transmissions from the content provider to each consumer. They include numerous terms that indirectly serve the copyright- and security-related interests of content providers. DRM technology license agreements complement the list of possible means by which digital content may be protected in a DRM system.

This particular means of protection would fail, however, if DRM technology licenses would be fully or partially unenforceable. Although specific statutory regulations concerning DRM technology licenses are extremely rare, such licenses could theoretically come into conflict with antitrust laws. As was described above, many DRM technology licenses require, for example, that the licensor not only integrate the licensed technology in its devices, but also additional technologies that the licensor must acquire from third parties. It is impossible to draw any general conclusions about the antitrust-related problems of DRM technology licenses. However, upon closer look, most DRM technology licenses are unlikely to raise antitrust concerns, either because they do not restrain competition in any meaningful way, or because various exemptions for technology licenses apply.

136. See § 4.2.2 CSS License Agreement, Version 1.2, at http://www.dvdeca.org/css (last visited Aug. 25, 2004); §§ 6.2.4.3, 6.2.5.5, 6.2.6 CSS Procedural Specifications, supra note 128; § 3.5 and § 3.7, Exhibit C, of the DTCP License Agreement, supra note 129; § 5.2.3, Exhibit D, of the HDCP License Agreement, supra note 129; §§ 3.4.3-6 and § 3 (f), Exhibit B, of the POD-Host Interface License Agreement, supra note 129.

137. See § 9, CPRM/CPM License Agreement, supra note 129; § 4, DTCP License Agreement, supra note 128; § 7, HDCP License Agreement, supra note 129. For the underlying technologies, see supra note 26.

138. See §§ 6.2.12 CSS Procedural Specifications, supra note 128; § 2.6, CPRM/CPM License Agreement, supra note 129; § 5.6 and § 5, Exhibit B, Part 1, of the DTCP License Agreement, supra note 129; § 2.6, and § 1.1, Exhibit B, HDCP License Agreement, supra note 129.

139. See infra text accompanying notes 207-213.

140. See supra text accompanying notes 126-131.

141. For a comprehensive antitrust analysis, the specific wording of a particular license agreement, the surrounding contractual framework, the structure of the particular market and of the licensor, as well as other factors would have to be assessed.

142. See supra notes 19, 193-196.

III. 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).

![Diagram showing different means of protection in a DRM system]

**Figure 1: Different Means of Protection in a DRM System**

From a legal perspective, this architecture has two implications that will be analyzed in this section.

A. 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 innovation and potential of DRM systems. The following three examples should clarify this proposition:

1. In order to prevent large-scale piracy, content providers have strong interests in hindering consumers from making unlimited copies of digital content. A fully-developed DRM system provides numerous ways to realize these interests: encryption and other technologies may be employed to control the uses a consumer can make of a digital content (protection by technology). If a hacker is able to circumvent these technologies, he or she may violate legal circumvention prohibitions (legal protection of the technological protection). The weaker the technological protection is, the more important the legal circumvention prohibitions become. Furthermore, consumers may be required by usage contracts 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. Thereby, it is ensured through technology that users obey the terms of their usage contracts. Metadata may be embedded in the content by using robust digital watermarks. Different technologies exist to ensure the authenticity and integrity of metadata. Ideally, with these technologies, usage terms can be inseparably intertwined with the content itself (in each case a technological protection of the contractual protection). If a hacker still 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 technologically possible, yet still commercially viable. From a technical viewpoint, this involves tamper-resistant hardware and software, technologies to check the integrity and authenticity of DRM components, and systems 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 to circumvent 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).

3. In a DRM system, usage rights may be granted and restricted along a chain of contracts that originates from the copyright owner and extends to the consumer.

---

In the U.S., see Antitrust Guidelines for the Licensing of Intellectual Property, 4 Trade Reg. Rep. ¶ 13132 (Apr. 4, 1995).

144. For an overview of the importance of intermediaries in electronic commerce as well as the opposing trends of disintermediation and reintermediation, see Michael D.
such a system, contractual commitments run with the digital content. If an intermediary conveys to a consumer the right to reproduce content under some conditions, this entitles the consumer to reproduce the content only if the intermediary possessed this right and was able to impose such conditions. As in real property law, intellectual property law has to deal with the tension between two competing principles. On the one hand, in general, an individual may not sell something he does not own, or transfer a title more complete than his own. On the other hand, a purchaser should not suffer from circumstances and title restrictions he was unaware of at the time of purchase. In general, intellectual property law does not recognize the bona fide acquisition of rights. While the law has developed rather complex mechanisms to balance the interests of the parties involved, DRM systems may also use technical solutions that ensure the integrity of a contractual distribution chain.

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 may be circumvented, statutory prohibitions may be disobeyed, contracts may be breached. However, one of the most interesting features of DRM systems is that these means of protection do not operate independently. If one of the means fails, another steps in to sustain 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.

B. Creation of a Privatized “Property Right”

The intertwining protection of DRM technology, anti-circumvention regulations, usage contracts, and technology license agreements raises the question of what the implications for traditional copyright protection are. It is of particular interest to analyze whether this intertwining protection could serve as a substitute for traditional copyright protection.

In principle, a DRM usage contract 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 content, all consumers are in privity with the content provider. The combination of all DRM usage contracts could amount to a level of protection that is similar to an existing property right: copyright law.

In the United States, Judge Easterbrook of the Seventh Circuit Court of Appeals rejected this reasoning in ProCD, Inc. v. Zeidenberg: “A copyright is a right against the world. Contracts, by contrast, generally affect only the parties; strangers may do as they please, so contracts do not create ‘exclusive rights’”. The overwhelming majority of commentators, however, have criticized this reasoning. Shrink-wrap licenses and DRM usage contracts are standardized contracts that are imposed on a mass market. Individual consumers do not have any influence on the specific contractual terms: DRM usage contracts are offered on a take-it-or-leave-it basis. Due to their uniformity and immutability, Professor Robert Merges


145. Following the notion of viral marketing, Professor Margaret Radin has named such contracts “viral contracts”, see Radin, supra note 88, at 1132; Margaret J. Radin, Online Standardization and the Integration of Text and Machine, 70 FORDHAM L. REV. 115, 115-116 (2002).


148. See BECHTOLD, supra note 19, at 263-269.
has described such contracts as “private legislation”. From this perspective, the sum of all usage contracts in a DRM system leads to a level of protection that is similar to copyright protection. Every consumer in an entire 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, as it underestimates the intertwining means of protection in a DRM system. If a content provider were to only rely on a myriad of contracts to protect his digital content, 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 usage contract at all. In an idealized DRM system, however, 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. RELs enable the DRM system to enforce the contractual provisions technologically (in both cases protection by technology). If the consumer circumvents this procedure, he or she may violate anti-circumvention provisions (legal protection of technology). Furthermore, the system may be secured by appropriate technology license agreements. Through this combination of technological and legal protection, a DRM system tries to ensure that digital content may never be accessed or used without having the appropriate usage contract in place. The intertwining means of protection try to inextricably knit content and usage terms together.

Therefore, the real innovation of DRM systems is not the protection of content by unilateral contracts which bind every consumer. Rather, it is the combination of this protection with other supporting means that creates a level of protection that may be commonly found only with traditional property rights. As with the protection by a property right, all consumers of DRM-protected content are subject to the DRM protection. Therefore, regarding the conglomerate of contractual and supporting technological and statutory protection in a DRM system, the terms “privatized property right” and “private legislation” seem appropriate indeed. This line of reasoning cannot


154. See also Elkin-Koren, supra note 43, at 103-104. For some caveats on this statement, see infra text accompanying notes 163-165.


only be applied in the U.S. context, but also in Europe and Germany. In a DRM system, content becomes inseparable from its technological and contractual protection. Overall, a trend from protection by copyright law to protection by the intertwining means of technology, contracts, anti-circumvention regulations and technology licenses is evident. In their combina-

in the Library of the Future, 42 REPRESENTATIONS 53, 63 (1993); Elkin-Koren, supra note 43, at 104-105; Heide, supra note 67, at 1012; P. Bernt Hugenholtz, Code as Code, Or the End of Intellectual Property as We Know It, 6 MAASSTRAIGHT JOURNAL OF EUROPEAN AND COMPARATIVE LAW 308, 309 (1999); Mark A. Lemley, Beyond Preemptiveness: The Law and Policy of Intellectual Property Licensing, 87 Cal. L. Rev. 111, 148 (1999); Merges, supra note 153, at 1613; O’Rourke, supra note 90, at 80; D. Nimner et al., supra note 87, at 60-61; J. Thomas Warlick, A Wolf in Sheep’s Clothing? Information Licensing and De Facto Copyright legislation in UCC §2B, 45 J. COPYRIGHT Soc’y U.S.A. 158, 170 (1997); Charles R. McManis, The Privatization (or “Shrink-Wrapping”) of American Copyright Law, 87 Cal. L. Rev. 173, 183 (1999); Thornburg, supra note 85, at 176. However, most of these commentators only take the proliferation of the contractual protection into account and underestimate the importance of the intertwining with other modes of protection, as is described in this article. For this reason, no contradiction between the point of view adopted by this article and the recent decision of the U.S. Court of Appeals for the Federal Circuit in Chamberlin Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004), exists. The Court aptly emphasizes that the anti-circumvention provisions of the DMCA do not create a new property right, see id. 1192-1194. However, the combination of anti-circumvention provisions with the other means of protection in a DRM system creates a de facto property right, as described in this article.

156. In general, German law strictly distinguishes between rights that are effective against all the world (“absolute Rechte”) and rights that are only effective against a specific party (“relative Rechte”). The combination of contractual, technological and statutory protection in a DRM system means, however, that the sum of DRM usage contracts (“relative Rechte”) and the contractual terms (“relative Rechte”) are now effective against all parties. This development resembles other areas where “relative Rechte” are assimilated to “absolute Rechte” (so-called “Verdinglichung obligatorischer Rechte”). For a more detailed analysis under German law, see BECHTOLD, supra note 19, at 268-277.

157. This article’s strong emphasis on the close intertwining of content with technological, statutory, and contractual protection is reminiscent of Professor Margaret Radin’s emphasis on the contract-as-product model. In a contract-as-product model, the contractual terms are part of the product rather than separate conditions agreed upon between the parties by mutual agreement. Terms and product merge into a single package. See Radin, supra note 98, at 1126, 1131; Radin, supra note 145, at 114-116; Golmukhiewicz, supra note 152, at 891; “The license is the product”; Maureen A. O’Rourke, Progressing Towards a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity?, 14 BERKELEY TECH. L.J. 635, 648 (1999); Raymond T. Nimmer, Images and Contract Law – What Law Applies to Transactions in Copyright, 40 Hof. L.J. 1, 4 (1998); Niva Elkin-Koren, Copyright the Formation of Information Contracts, 36 HOUS. L. REV. 195, 215, 217 (1999); Julie E. Cohen, Copyright and the Jurisprudence of Self-Help, 13 BERKELEY TECH. L.J. 1089, 1115 (1998).

tion, these means provide a level of protection very similar or even superior to the protection by traditional copyright law. This new conglomerate has the potential to supplant copyright law as the primary means of protection in the digital environment. Although a law and economics analysis of DRM systems is beyond the scope of this article, it is interesting to note that such analysis leads to similar results: DRM protection is a substitute for copyright protection.

DRM systems are essentially a privatized copyright law cast in silicon, the scope, design and extent of which may be determined by the providers of content and DRM technology. As Professor Charles McManis has described in a slightly different context: "We face, in a word, is the imminent privatization, or 'shrink-wrapping', of [...] copyright law."

IV. 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, two of which will be depicted in this section.

159. Elkin-Koren, supra note 153, at 1158; Hugenholtz, supra note 155, at 312.
160. Goldstein, supra note 158, at 151; Gimbel, supra note 153, at 1672.
161. As any information, digital content is (to some extent) a public good characterized by its non-rivalry and non-exclusivity. Because it is impossible to exclude non-paying consumers from the consumption of the content, no consumer will pay for using the content. By hiding his real preferences, every consumer would hope that another consumer would buy the content and that he could 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. To eliminate this market failure, the law grants the content provider 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 like copyright law, the DRM protection eliminates the non-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. From a law and economics perspective, the protection by DRM systems could replace the protection by copyright law to a certain extent. For a much more in-depth treatment that also addresses legitimate objections to the outlined analysis, see Bectold, supra note 19, at 282-315.


A. Copyright Law as a Safety Net

Unfortunately, it is an oversimplification to say that content providers may effectively protect themselves 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 may be void or unenforceable. Technological protection may be defeated; the supporting circumvention prohibitions do not cover every attack and every person involved in an attack. As such, copyright law could fill protection gaps left open by the DRM protection. Although copyright law would no longer serve as the primary means of protection for content providers, it would step in as a safety net when all other means of protection in a DRM system fail (see infra figure 2).

163. The probability of such defects increases with the length of the chain of usage contracts used in a DRM system, see Merges, supra note 147, at 119-120.
164. See id. 119-121; see also Bectold, supra note 19, at 371-372; Gimbel, supra note 153, at 1683.
165. See Bectold, supra note 19, at 373.
166. See European Copyright Directive, supra note 62, at 10.
167. Although it is a fair question whether such a lengthy copyright term is a limitation in any practical sense; see Eldred v. Ashcroft, 123 S.Ct. 769, 807-812 (2003) (Breyer, J., dissenting).
169. See Guibault, supra note 96, at 29-47.
170. See id. 47-56.
171. See id. 56-68.

B. Overextension of DRM Protection

More importantly, copyright protection has never been unlimited. In the United States, one of the most important copyright limitations is the fair use defense, a highly flexible common law doctrine that is applied in contexts as different as parody, home videotaping and other non-commercial uses. In European droit d’auteur countries, a more detailed set of copyright limitations exists. Article 5 of the European Copyright Directive of 2001 includes a list of over 20 different copyright limitations. Besides limitations in scope, copyright law also limits the protection in duration: copyright protection ends 70 years post mortem authoris.

While the objectives of particular copyright limitations vary from case to case and from country to country, they may be classified into various categories. Some copyright limitations protect constitutional rights such as the freedom of expression and the right to privacy. Others intend to preserve well-functioning competition.
to further the dissemination of knowledge, to and to overcome market failures such as prohibitively high transaction costs. Finally, others are designed to promote the dissemination of new works and to ensure the preservation of a vigorous public domain.

While limitations are inherent components of any copyright regime, the protection by DRM systems is potentially unlimited. Theoretically, DRM enables content providers to protect their interests without paying adequate attention to interests of third parties or the society at large. In particular, DRM systems may undermine copyright limitations. They may protect digital content that is not copyrightable. They may prevent consumers from copying content for private purposes even if a copyright limitation allows them to do so without the rights holder’s permission. DRM systems may also extend their protection to areas that lie outside of the reach of copyright protection. They may, for example, control how often a consumer listens to a song, at what time and at what location a text may be read, or even the viewing quality in which the consumer will be able to watch a movie. This runs counter to traditional notions of copyright law in that a DRM system is able to control the mere use or consumption of a work.

While it is a complex question as to what extent particular copyright limitations should apply to the different means of protection in

172. See id. 69-77.


176. For actual examples, see Bechtold, supra note 19, at 375-378; see also Guibault, supra note 96, at 169; Vinje, supra note 162, at 436; Robert C. Denicola, Mostly Dead? Copyright Law in the New Millennium, 47 J. Copyright Soc’y U.S.A. 193, 196 (2000); Lessig, supra note 158, at 529; Burk & Cohen, supra note 158, at 50-51; Koelman & Helberger, supra note 38, at 191; Vinje, supra note 62, at 555; Thomas Hoeren, Urheberrecht 2000 – Thesen für eine Reform des Urheberrechts, Multimedia und Recht 2000, 3, 4; Detlef Kröger, Die Urheberrechtlerinheit für die Informationsgesellschaft – Bestandsaufnahme und kritische Bewertung, Computer und Recht 2001, 316, 321.

177. For the situation in Germany, see Bundesgerichtshof, Gewerblicher Rechtsschutz und Urheberrecht 1991, 449, 453 – Betriebssystem; Bundesgerichtshof, Computer und Recht 1994, 257, 276 – Holzhandelsprogramm. For the situation in Europe, see Lessig, supra note 158, at 436; Guibault, Contracts and Copyright Exemptions, in Copyright and Electronic Commerce 129, 132 (P. Bernt Hugenholtz ed., 2000). For the situation in the U.S., see Elkin-Koren, supra note 43, at 106; Lemley, supra note 43, at 1014; see also Bechtold, supra note 73, at 26.

178. This problem is tied up with the fact that it is a complex economic question as to what role limitations play in traditional copyright law and how their role changes with the introduction of DRM systems. If one views copyright limitations primarily as a tool to reduce transaction costs, their importance could decrease considerably in DRM systems. At least theoretically, DRM systems have great potential to lower transaction costs, therefore rendering limitations to the DRM protection unnecessary. However, it is highly questionable whether an analysis of copyright limitations that is restricted to transaction costs economics adequately grasps the importance and scope of such limitations; for a detailed analysis, see Bechtold, supra note 19, at 312-317, 324-328; see also supra note 174. Determining the importance of limitations to DRM protection from an economic perspective also depends on the underlying economic analysis of copyright law. One way of explaining copyright law is to view it as a sort of monopoly (which is a severe oversimplification, however). According to monopoly law, the copyright owner – like any monopolist – has the ability to raise the price for his work above marginal costs. Thereby, compared to a perfectly competitive market, fewer consumers buy the work. This may lead to a social welfare loss due to the underutilization of the work; see, e.g., Bechtold, supra note 19, at 298-299. From this perspective, it is the goal of copyright law and its limitations to reconcile the welfare loss due to the undervaluation of content (leading to copyright protection) and the welfare loss due to the underutilization of the produced content (leading to copyright limitations). This analysis may 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 may lead to a socially wasteful underuse of the protected content as well. From this perspective, the protection by DRM systems should be limited just as copyright protection should be limited; see id. 299. By contrast, 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 DRM technology and contractual protection in a DRM system offers numerous means to engage in price discrimination. However, it is a highly contentious issue whether such price discrimination would really render limitations to the DRM protection unnecessary; see id. 300-311, 321-324. Another way to look at copyright law – which in the last 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-value-added 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 aid in creating a price for resource allocation; cf., e.g., Nei W. Netanel, Copyright and a Democratic Civil Society, 106 Yale L.J. 283, 309-310 (1996). For this line of thought, copyright limitations are far less important, as the allocation of rights is left to the market to the largest extent possible. If one applied this theory to the protection by DRM systems, limitations could play a much less important role.


agreements may potentially undermine copyright limitations as well. Therefore, an effective limitation to DRM protection has to limit all the different means of protection in a DRM system (see infra figure 2).

While the intertwining means of protection in a DRM system may have the potential to supplant copyright protection, there is still a need for something more. While the content provider is able to protect himself by the means of protection in a DRM system, the protection of 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 statute that protects interest of consumers and the society at large. Or, as Professor Lawrence Lessig has put 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”. 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 as to which institution should determine what those limits are. In principle, this could be accomplished either by market forces or by the legislature. According to one view, DRM systems, which are biased too strongly in favor of content providers and do not take appropriate limitations into account, will not be successful on the market 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 competition among vendors protects consumers in a market economy.

However, this view assumes that well-functioning competition between different DRM systems or producers of DRM-protected content exists. At a minimum, this assumption is questionable. Within DRM systems, information asymmetries, indirect network effects, high switching costs and lock-ins may occur, leading to market failures and thereby preventing well-functioning competition.

On both sides of the Atlantic, it is often argued that the alleged tension between DRM systems and copyright limitations is not an actual problem, as works published in a DRM-protected format will almost always be available in unencrypted form as well. One reason may be that a market for the work in an unencrypted form will continue to exist (such as in the area of newspapers and magazines). Another reason may be that DRMs systems will never be able to cordon off content completely. File-sharing networks will continue to exist, movies and photos can be captured from a computer screen, and music can be re-recorded from a loudspeaker.

However, such copying, capturing and re-recording will not be feasible in many cases. Furthermore, it is problematic to refer a beneficiary of copyright limitations to versions of copyrighted works which are technologically inferior. Why should the rights holders benefit from the new opportunities of DRM systems in order to protect their legitimate interests, while the beneficiaries of a copyright limitation have to fall back on an inferior and sometimes outdated version of the work in order to carry out their legitimate interests? It may be true that, from a strictly legal perspective, U.S. copyright law does not guarantee beneficiaries of copyright exceptions that they may copy works by the optimum method or in the identical format of the original. However, from a policy perspective, it is highly unsatisfactory in an information society to restrict the fair use defense and other copyright limitations to technologically inferior versions of copyrighted works. For an emerging information society, the goal should not be a DRM environment which protects the legitimate interests of rights holders only, but a symmetric DRM environment which protects the legitimate interests of both rights holders and users.

For these reasons, 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.

182. See also Elkin-Koren, supra note 154, at 105-106, 113; Lemley, supra note 155, at 114-115, 171-172; Koedl & Helberger, supra note 174, at 200-201; Bechtold, supra note 19, at 382-383.

186. A detailed economic analysis of these aspects is beyond the scope of this article. For such analysis, see Bechtold, supra note 19, at 338-364; see also Elkin-Koren, supra note 153, at 1182-1185.


188. See Bechtold, supra note 19, at 381-382.


190. For more reflection on such a symmetric DRM system, see Bechtold, supra note 12, at 607-609. To some extent, this relates to the argument that digital technologies have changed the social conditions of speech and that, therefore, a copyright theory in an information society should be based on a symmetric democratic culture of free expression; see Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U. L. REV. 1 (2004).
V. Law as a Limitation to the DRM Protection

If one adopts the viewpoint that some limitation to the protection by DRM systems is necessary, it is important to realize that all of the different means of protection that are used in DRM systems have to be limited. Not only is each of these means capable of undermining the limitations to traditional copyright law, they are also so closely intertwined that only a comprehensive regulatory approach would put effective limits on DRM protection in its totality. Therefore, the law has to limit the extent to which content providers may use technology, contracts, and statutory provisions to protect their interests in DRM systems (see figure 2).

![Diagram](image)

**Figure 2: Limiting DRM Protection by Law**

In the remainder of this section, the article will describe the theoretical options available to legislators to limit DRM, and the actual options exercised by legislators in the U.S. and Europe.

A. Limitation of the Protection by Contracts

In a DRM system, content providers could override copyright limitations by employing a contractual protection scheme. In the software sector, contractual terms forbidding the reverse engineering of software have been around for years. This raises the question of whether the balance between the interests of copyright owners and the public as determined by copyright law may be altered by contractual arrangements.

In the United States, the tension between federal copyright law and state contract law has attracted a significant amount of attention among legal scholars. The preemption doctrine, which is codified in 17 U.S.C. § 301, specifically addresses the relationship between federal copyright law and state legislation. However, various courts and commentators differ to a great extent on how to interpret and apply this provision in the area of contract law. The current preemption doctrine does not provide easy guidelines to determine whether certain kinds of DRM usage contract terms are permissible or not. Indeed, there is good reason to believe that the preemption doctrine is fundamentally ill-suited to solve the tension between copyright and contract.

During the drafting process of the “Uniform Computer Information Transactions Act” (UCITA), the relationship between copyright and contract was one of the most contentious issues of the entire project. In the final version of the model law, § 105 (b) UCITA provides that courts may refuse to enforce contractual provisions that violate a “fundamental public policy”. Such public policies include “innovation, competition, fair comment and fair use”. The UCITA

---

191. 17 U.S.C. § 301 (2004) does not preempt particular contracts as such, but the enforcement of particular contracts by the states; see Lemley, supra note 155, at 137 note 108.


193. Indeed, Lemley, supra note 155, at 115, writes: "...the law of preemption is a mess". For an overview of the debate, see id. 111; Michael J. Madison, Legal-Ware: Contract and Copyright in the Digital Age, 67 FORDHAM L. REV. 1025, 1128-1132 (1998); Mercer, supra note 152, at 1333-1337. For an overview of case law dealing with the application of 17 U.S.C. § 301 (2004) to the intersection of copyright and contract, see Ballis v. Tedesco, 41 F.Supp.2d 531, 536 note 14 (D.N.J. 1999).

194. See Lemley, supra note 155, at 144-150; Reichman & Franklin, supra note 175, at 920-922; Madison, supra note 193, at 1131-1132.

195. See Reichman & Franklin, supra note 175, at 875; Warlick, supra note 155; McManis, supra note 155, at 176; Lemley, supra note 155; Brennan, supra note 87.

196. Official Comment 3, UCITA § 105 (2002). For a detailed analysis, see Brennan, supra note 87.
has only been enacted in two states and, in 2003, it was decided to cease efforts to get the UCITA enacted in additional states.\textsuperscript{197} Therefore, whether this approach suffices to preserve public values and copyright limitations in the context of DRM usage contracts will probably remain an open question. Other approaches to reconcile copyright limitations with contract law include the application of the copyright misuse doctrine and the contract doctrine of unconscionability.\textsuperscript{198}

In spite of the remarkable efforts of U.S. courts, legislators, and commentators to shed light on the relationship between copyright and contract over the last years, it remains a thicket that lacks clear-cut rules. While DRM usage contracts may be limited by the preemption, public policy, misuse and unconscionability doctrines, the exact scope of permissible DRM usage contract terms is unclear under U.S. law and will probably remain so, at least for the near future.

In Europe, astonishingly, the tension between copyright limitations and contractual arrangements has not been discussed a great deal.\textsuperscript{199} The European Union Directives in the copyright area contain only a few isolated provisions that prohibit the overriding of copyright limitations by contract.\textsuperscript{200} The recently adopted Copyright Directive states explicitly that copyright limitations as defined in Article 5 of the Directive should not prevent “contractual relations designed to ensure fair compensation for the rights holders”.\textsuperscript{201} In general, in European Union copyright law, the relationship between copyright exemptions and usage contracts is unclear.\textsuperscript{202}

On the level of the individual member states, the relationship is generally not much clearer. The German Copyright Act, for instance, only rarely provides that particular copyright limitations cannot be waived by contract.\textsuperscript{203} A general theory of how copyright limitations and contract may be reconciled does not exist.\textsuperscript{204} Yet, German courts have to deal with the intersection of copyright and contract on a regular basis. According to § 32 of the German Copyright Act, both non-exclusive and exclusive grants of usage rights may be made subject to limitations with regard to place, time, or content. Courts have consistently ruled that this freedom to impose restrictions is limited by generally accepted business practice standards. While the exact scope and depth of this doctrine is still in flux, it has severely limited the ability of software manufacturers to restrict their software licenses to specific processors, networks, computers, or distribution channels.\textsuperscript{205} This case law might be applied in the context of DRM usage contracts. However, it also does not provide clear-cut guidelines regarding which kinds of DRM usage contract terms are permissible.\textsuperscript{206}

\section{B. Limitation of the Protection by Technology Licenses}

As was described above,\textsuperscript{207} DRM technology licenses enable content providers to make sure that all consumer devices adhere to usage rules as set by the content providers. Although DRM technology licenses do not directly supersede copyright limitations, they may render it unlawful for device manufacturers to produce devices that enable consumers to benefit from copyright limitations\textsuperscript{208} – which, in the end, leads to the same result: hampering copyright limitations. If, for example, a content provider wants to distribute its content only in a DRM-protected form that allows no private copying, DRM technology licenses can ensure that no consumer device is available on the market which does not adhere to this rule. Therefore, DRM technology license agreements can \textit{de facto} override limitations to copyright law.

\begin{footnotesize}
\textsuperscript{197} See supra note 92.
\textsuperscript{199} The only exceptions are Guibault, supra note 177, and Guirault, supra note 96.
\textsuperscript{200} According to Article 9 (1) of the Software Directive (see supra note 60), copyright owners are forbidden to use contracts as a means to override the decompilation exemption in Art. 6. A similar provision against the contractual overriding of specific copyright exemptions can be found in Art. 15 of the Database Directive; see Directive 96/9/EC of the European Parliament and of the Council of March 11, 1996, on the legal protection of databases, \textit{Official Journal of the European Communities} L 77 (Mar. 27, 1996), 20.
\textsuperscript{201} Recital 45 of the European Copyright Directive, supra note 62. What the implications of this Recital are is unclear to some extent. For severe criticism that is based on the understanding that the Recital could ultimately allow rights holders to override any copyright limitation by contract, see Hugenholz, supra note 62, at 501; Betchtold, supra note 19, at 391; for a somewhat milder criticism, see Europäisches Urheberrecht – Kommentar, Info-RL, IV. Kap., § 98 (Michael M. Walter ed., 2001) (based on an interpretation of the German version of the Directive which cannot be applied to the English language version; see Betchtold, supra note 19, at 391 note 1993; see also Guibault, supra note 96, at 219-220.
\textsuperscript{202} See Guibault, supra note 177, at 155; Vinje, supra note 73, at 195-196.
\textsuperscript{203} See §§ 69 g (2), 55 a (3) and 87 e UrhG. In addition, these explicit provisions about the relationship between copyright limitations and contract were only introduced into German copyright law because Germany was required to do so by the aforementioned EU Directives.
\textsuperscript{206} See supra text accompanying notes 121-143.
\textsuperscript{207} See supra note 122, at 292.
\end{footnotesize}
The potential tension between DRM technology license agreements and copyright limitations has been very rarely addressed by legislators or the administration. So far, this has not been the case at all in Europe. In the U.S., in its assessment of a DRM technology license in the pay TV sector, the Federal Communications Commission rejected the claim that the license would preclude reasonable home recording of DRM-protected content. Although the FCC did not take action against the particular DRM technology license, this instance shows a possible method for reconciling technology licenses with the balance of interests struck by copyright law, limiting the range of terms licensors may write into a DRM technology license.

C. Limitation of the Protection by Technology

As was shown above, technological protection measures may be used by content providers to undermine copyright limitations. Several regulatory options exist that may reconcile technological protection measures with copyright limitations. The remainder of this subsection will describe what these theoretical options are and which of these options the U.S. and European legislators have adopted.

1. Direct Influence on the Design of Technological Protection Measures

a) In Theory

The first regulatory option for the legislature to reconcile technological protection measures with copyright limitations is to enact provisions that directly affect the design of technological protection measures. The legislature could, for example, prohibit the use of any technological protection measure that ignores copyright limitations. It could also mandate by law that technological protection measures must allow a certain number of copies for private or educational purposes without any permission by the rights holder. The legislature, in other words, would use the law to directly shape technology in accordance with certain policy goals.

Unfortunately, this approach suffers from severe limitations. Most importantly, from a technical point of view, it seems impossible to design a DRM system that respects all copyright limitations on a technical level; the complexity of the law in this area seems to defy any clear technical definition that could be used in a real-world DRM system. This applies in particular to the United States where the

---

209. Even scholarly literature about DRM technology license agreements is extremely scarce both in Europe and the U.S. The only exceptions are BECHTOLD, supra note 19, at 405-406, and Weinberg, supra note 122.

210. However, the possible tension between DRM technology licenses and other areas of public policy, in particular antitrust concerns, have long been recognized in Europe; see only Annex I, Part I, lit. (c) to Article 6 (1) of the Directive 2002/29/EC of the European Parliament and of the Council of March 7, 2002, on Access to, and Interconnection of, Electronic Communications Networks and Associated Services (hereinafter: Access Directive), Official Journal of the European Communities L 108 (Apr. 24, 2002) 7 (prescribing DRM technology providers to use technology licenses to prevent the inclusion of competing DRM systems in a single pay TV set top box, as such license terms could thwart competition between different DRM technology providers). This provision supercedes the similar Article 4 (d) of the Directive 95/47/EC of the European Parliament and of the Council of October 24, 1995, on the Use of Standards for the Transmission of Television Signals, Official Journal of the European Communities L 281 (Nov. 23, 1995) 51.

211. See also for the “POD-Host Interface License Agreement,” see supra note 125.

212. In re Implementation of Section 304 of Telecommunications Act of 1996, supra note 124, at § 28-29. That the FCC recognized the possible tension between DRM technology licenses and copyright limitations becomes evident in the separate statement of Commissioner Gloria Tristani: “... our ruling in no way authorizes any attempt by providers of services to utilize this ruling to combine technology with copyright protection in a manner that interferes with, or unreasonably restricts, a consumer’s fair use of copyrighted material... Today’s declaration ensures the financial rewards of copy protection to content owners while protecting citizens from the dispossession of their right to fair use. Based on the record before us and controlling Supreme Court precedent, I believe we have struck the appropriate balance,” id. at 18220. See also Weinberg, supra note 124, at 289-292 (criticizing the FCC’s failure to recognize the underlying public policy concerns).

213. BECHTOLD, supra note 19, at 405-406. This is not a totally novel approach, as the limitations on DRM technology licenses due to antitrust concerns demonstrate, see supra note 210.

214. See supra text accompanying notes 175-186.

215. Regulatory options that turn away from technological protection measures and build upon alternative compensation systems instead are beyond the scope of this article. Over the last two years, scholars and policymakers on both sides of the Atlantic have proposed to condemn DRM systems and expand so-called levy systems instead. For the discussion in the U.S., see WILLIAM FISHER, PROMISES TO KEEP - TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT (2004); NETANIEL, IMPROSE A NONCOMMERCIAL USE LEVY TO ALLOW FREE P2P FILE SHARING, 17 HARV. J.L. & TECH. 1 (2003); LAWRENCE LESSIG, THE FUTURE OF IDEAS 254-255 (2001). For the relationship between DRM systems and levy systems from a European perspective, see P. BERNT HUGENHOLTZ ET AL., THE FUTURE OF LEVIES IN A DIGITAL ENVIRONMENT (2003), http://www.ivir.nl/publications/other/DRM%20Levies%20Final%20Report.pdf. For the discussion in general, see BECHTOLD, supra note 12, at 614-617.

216. In the following, only provisions that have actually been limited by the legislature will be discussed. Some anti-circumvention regulations, such as the European Conditional Access Directive, are not limited at all; see BECHTOLD, supra note 19, at 428; HEIDE, supra note 61, at 1026-1044; see also GINSBURG, supra note 73. Furthermore, in the context of the European Computer Program Directive, it is disputed whether the limitations of Articles 5 and 6 restrict the anti-circumvention protection of Article 7 (1) (c) of the Directive; see WALTER (ed.), supra note 201, Art. 7 Software-RL § 15; WANG, supra note 58, at 72-73, 126-133; THOMAS HEIDE, COPYRIGHT, CONTRACT AND THE LEGAL PROTECTION OF TECHNOLOGICAL MEASURES, 50 J. COPYRIGHT soc. U.S.A. 315, 334-336 (2003); see also BECHTOLD, supra note 19, at 430. Finally, the protection of 47 U.S.C. § 605 (2004) is not limited either.

217. See Burk & Cohen, supra note 158, at 55-58.

218. See Koelman & Helberger, supra note 38, at 198; KOELMAN, supra note 73, at 279; FISHER, supra note 158, at 1254.

219. See Burk & Cohen, supra note 158, at 55-57, 70; SANDER, supra note 12, at 74; EDWARD FELTEN, A SKEPTICAL VIEW OF DRM AND FAIR USE, 46 (4) COMMUNICATIONS OF
scope and applicability of the fair use defense is often unclear.\textsuperscript{220} If a legislature adopted this regulatory approach, it seems inevitable that the DRM system would, in some cases, deny access to protected content although a copyright limitation applies. Nevertheless, this regulatory approach may still prove helpful, particularly in combination with other regulatory approaches.\textsuperscript{221}

b) In Practice

Worldwide, the legislative bodies have only rarely decided to directly influence the technological design of DRM systems. In Europe, Article 3 (a) of the revised Television Directive of 1997\textsuperscript{222} requires that certain “events of major importance for society” (for example sports events such as the Olympic Games) be available from other sources than just 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 above.\textsuperscript{223} In the United States, the Digital Millennium Copyright Act introduced a somewhat similar provision regarding analog protection systems that are used in video recorders.\textsuperscript{224} Furthermore, the Audio Home Recording Act of 1992 requires that any consumer DAT player sold in the U.S. be equipped with the “Serial Copy Management System” (SCMS).\textsuperscript{225} On the one hand, SCMS prevents digital copies of the second generation from being made.\textsuperscript{226} On the other hand, SCMS allows consumers to make first generation digital copies of any audio recording. Therefore, the Audio Home Recording Act implicitly ensures that no DAT player is sold in the U.S. that prevents consumers from making one digital copy for personal purposes.\textsuperscript{227} Whether this system is a wise policy choice is a question that this article does not address.\textsuperscript{228} It merely wants to show that the statutory mandate to integrate SCMS into DAT players is an example of how the U.S. legislature directly influenced the design of technological protection measures.\textsuperscript{229} However, as all these examples show, the legislatures decide to influence the particular design of a technological protection measure only in rare and narrow circumstances.

2. Indirect Regulation by Establishing a “Right to Hack”

a) In Theory

The legislature does not have to directly influence the design of technological protection measures in order to reconcile them with copyright limitations. A second regulatory option is to restrict the legal protection of technological protection measures. The legislature could deny the protection by anti-circumvention provisions in cases where the combined protection by technology and anti-circumvention provisions is overbroad. Without legal protection, there is no reason why the user should not be allowed to circumvent the technological protection measure. Basically, this approach gives the user a “right to
hack.²³⁰ Technological protection measures in certain cases specified by law.²³¹

In many cases, however, granting consumers a mere "right to hack" will not be sufficient. Most consumers will not have the necessary know-how to circumvent technological protection measures on their own. Rather, they depend on the availability of tools and services that enable an easy circumvention of the technological protection measure. Therefore, if the legislature decides to adopt this regulatory approach, it has to allow to some extent the distribution of circumvention tools and the provision of circumvention services ("preparatory activities").²³² Unfortunately, in most cases, circumvention tools and services are "neutral" in the sense that they may be used to circumvent technological protection measures for both legitimate and illegitimate purposes.²³³ It is extremely difficult to draw a clear line between tools that should be allowed, because they enable consumers to benefit from copyright limitations, and other tools that should be prohibited, because they enable mass-scale piracy. If the legislature enacted too broad a prohibition on circumvention tools and services, the "right to hack" would essentially become futile. If, on the other hand, the legislature enacted too narrow a prohibition on circumvention tools and services, DRM systems would fail in providing adequate protection to content providers as nearly every consumer could circumvent the DRM protection in all cases.²³⁴ Any regulatory system that implements a "right to hack" has to deal with this inherent tradeoff in one way or the other.

b) In Practice

In the United States, Congress adopted this approach to establish a "right to hack" in the Digital Millennium Copyright Act of 1998.²³⁵ The very broad protection of technological access and usage control measures in 17 U.S.C. § 1201 (a) and (b) is limited by several

²³⁰. This use of this term does not mean to imply that the beneficiary of copyright or anti-circumvention regulations has indeed a "right" in a legal sense. For an analysis of the complex question whether copyright limitations are "rights" or mere privileges or defenses, see Guibault, supra note 96, at 90-110; see also Bechthold, supra note 19, at 383 note 1967; Schack, supra note 204, at 504-555; Udo von Diemar, Kein Recht auf Privathöfen – Zur Rechtsnatur der gesetzlichen Lizenz zu Gunsten der Privatwurzel-oldie, Gewerblicher Rechtsschutz und Urheberrecht 2002, 557.

²³¹. This regulatory option is sometimes called the "Cohen theorem", see Lessig, supra note 2, at 139.

²³². See Koelman, supra note 73, at 274; see also Samuelson, supra note 42, at 458; Wand, supra note 38, at 41, 56-57.

²³³. Due to these characteristics, they are sometimes also described as "dual use tools".

²³⁴. On this tradeoff, see Koelman, supra note 73, at 274.

²³⁵. In addition, in a rule making procedure under 17 U.S.C. § 1201 (a) (1) (C) and (D) (2004), the U.S. Copyright Office exempted four classes of works from the anti-circumvention provisions of 17 U.S.C. § 1201 (a) (1) (2004): works that are protected by malfunctioning protection measures, lists of websites that are protected by filtering software applications, computer programs and video games distributed in formats that have become obsolete, and ebooks that prevent the blind from accessing the work; see 37 C.F.R. § 201.40 (2004), and Library of Congress, Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62011 (2003).


²³⁷. For an overview, see Ginsburg, supra note 42, at 148-152.

²³⁸. See supra text accompanying note 43.

²³⁹. Such as 17 U.S.C. § 1201 (d) (g), (i), and (j) (2004).

²⁴⁰. Such as 17 U.S.C. § 1201 (e) and (f) (2004).

²⁴¹. See supra text accompanying notes 44-53.

²⁴². Such as 17 U.S.C. § 1201 (d) and (i) (2004).
activity activities as well. In addition, whereas some of the limitations that exempt preparatory activities only exempt activities which are targeted at access control measures, others cover activities which are targeted at usage control measures as well. In most cases, no good reasons exist for making all these distinctions. The limitations to the DMCA’s anti-circumvention provisions are overly complex and demonstrate a severe lack of a clear regulatory concept. Many examples exist in which uses that should be deemed as “fair” are not covered by these limitations.

3. Indirect Regulation by Creating a “Key Escrow” System
   a) In Theory

A third regulatory option to reconcile technological protection measures with copyright limitations tries to evade some of the disadvantages of the aforementioned approaches. Under this regulatory option, a consumer who benefits from a limitation to DRM protection would not be allowed to develop, distribute or obtain circumvention devices from the market. Rather, the consumer would be entitled to obtain appropriate means, such as circumvention devices or decryption keys, from a particular institution. Equipped with these means, the consumer would be allowed to circumvent the technological protection. This beneficiary of a copyright limitation would be forbidden from passing on these means to other consumers. Rather, these other consumers could obtain the same means from the institution if, and only if, they would be beneficiaries of a copyright limitation as well. This regulatory approach tries to prevent circumvention tools and services, which may be used to circumvent the DRM protection for illegitimate purposes, from being freely available on the market.

From a technical perspective, this approach resembles so-called “key escrow” architectures in encryption systems. In both cases, encrypted communications may be decrypted with appropriate tools that are legally available under certain circumstances from a particular institution.

Although this approach seems promising at first sight, it is fraught with problems as well. First, in a DRM “key escrow” system, one must decide who operates the institution from which consumers may obtain the appropriate means to circumvent technological protection measures. If this “key escrow” agency were operated by content providers, there would be a danger that content providers would use the control over this agency strategically. As was described above, copyright limitations serve public interests that are very often not congruent with the content providers’ interests. If, through a key escrow agency, content providers could control which consumer could obtain circumvention tools and thereby benefit from copyright limitations, content providers would likely deny access to circumvention tools when the circumvention ran contrary to their own interests. In such an institutional arrangement, copyright limitations would probably not be appropriately protected. As a result, it would be a much better idea to charge an independent trusted third party with the administration of a DRM key escrow agency.

Secondly, in a key escrow system, before a consumer could benefit from a copyright limitation, he would have to contact the escrow agency in order to obtain the appropriate circumvention devices. Due to considerable transaction costs, this could have chilling effects that would significantly diminish the total number of fair uses made in a society. In particular, spontaneous fair uses could be chilled. Finally, key escrow agencies could collect personal information on which user circumvents technological protection measures and for what purpose. Therefore, a key escrow system raises privacy concerns, but is firmly opposed to by civil liberty organizations, were heavily discussed in the context of the so-called “Clipper Chip”, see A. Michael Froomkin, It Came From Planet Clipper: The Battle Over Cryptographic Key Escrows, 1996 U. CHI. L.C. 15. For a more detailed comparison, see BECHTOLD, supra note 19, at 413. See Burk & Cohen, supra note 158, at 59-65. Such a system was first proposed by MARC STEFIR, THE INFORMATION EDGE 99-102 (1996) under the name “Digital Property Trust”. See Burk & Cohen, supra note 158, at 59-60, 63. However, Burk and Cohen also aptly point out that a key escrow system might be easier to be implemented in European countries which limit their copyright protection not by a very broad and often fuzzy fair use doctrine, but by an enumerative list of discrete copyright limitations; see id. at 70. And, indeed, article 6(4) of the European Copyright Directive attempts to avoid the problem mentioned above by focusing on agreements between associations of rights holders and users rather than on individual users exercising their rights. By enabling user associations to bring an action against rights holders on behalf of individual users who might want to avoid the hassle of suing rights holders, and by altering the burden of proof under certain circumstances, the German Copyright Act implements article 6(4) of the European Copyright Directive in an even more sophisticated way; see BECHTOLD, supra note 69, Rdnr. 68-60.
cerns. In general, the “key escrow” approach could lead to a centralization of copyright limitations where only a few actors determine who benefits from such limitations, and for what purposes.

b) In Practice

During the drafting of the EU Copyright Directive of 2001, which has sometimes been called the “most lobbied Directive in European history”, one of the most contentious issues was how technological protection measures should be reconciled with copyright limitations. In its final version, the Directive basically employs a modified “key escrow” approach. As opposed to the U.S. DMCA, the European Copyright Directive does not benefit beneficiaries of copyright limitations to circumvent technological protection measures and distribute tools needed for such circumvention on their own. Rather, according to the lengthy and hardly understandable Article 6 (4) of the Directive, under certain circumstances, content providers may be required to make circumvention devices or services available to consumers who benefit from some copyright limitations. However, Article 6 (4) severely restricts the scope of this “key escrow approach” in three ways:

1. Article 6 (4) (1) states that “voluntary measures taken by rights holders, including agreements between rights holders and other parties concerned” have priority over any legislative action. If, for example, content providers reach an agreement with library associations that enable libraries to benefit from relevant copyright limitations in spite of technological protection measures, the member countries of the European Union cannot enact any laws prescribing a “key escrow” system.

2. The authorization of member states to prescribe a key escrow system is further limited by the fact that it only exists in regard to certain copyright limitations. Article 5 of the Copyright Directive provides a list of 22 limitations to copyright law which the member states may enact in their national copyright laws. In regard to certain limitations – such as copying privileges for libraries, researchers, museums, hospitals, and disabled persons – member states are obliged to enact a key escrow system, see Article 6 (4) (1). In regard to another copyright limitation – the privilege to make copies for private purposes – member states are not obliged, but are entitled to take such action, see Article 6 (4) (2). In regard to a third set of copyright limitations – including the privilege to quote existing works for purposes of criticism or review or to use them for parody purposes – member states are not even entitled to take such action. Even the limitation concerning temporary copies in Article 5 (1) falls in this cate-

256. See Burk & Cohen, supra note 158, at 60-61, 63-65.

257. See Bechtold, supra note 19, at 414.

258. See also Hugenholtz, supra note 62, at 581; Shah, supra note 62, at 110-115; see also Reinothe, supra note 62, at 500 (criticizing the legal uncertainty created by Article 6 (4)). The implementation of Article 6 (4) of the Directive in the various member states of the European Union differs to a large extent, see Marie-Therése Hupertz, The Peculiar Role of Digital Rights Management Systems in the Digital World, COMPUTER UND RECHT INTERNATIONAL 2002, 105, 109-111; Karin Retzer, On the Technical Protection of Copyright, COMPUTER UND RECHT INTERNATIONAL 2002, 134; for the implementation in Germany, see Bechtold, supra note 69, Rdnr. 68-97; for the implementation in the United Kingdom, see Hart, supra note 69.

259. Whether the Directive requires that such an obligation be enacted as a statutory provision or merely as a matter of good practice in order to be avoided in court or should be left to (automatic) dispute resolution mechanisms is unresolved questions; see Reinothe, supra note 62, at 50-51; Dreier, supra note 65, at 39.

260. However, this is not the only possible understanding of the provision. Article 6 (4) (1) of the Copyright Directive provides: “... Member States shall take appropriate measure to make available to rights holders the means of benefiting from that exception or limitation... the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.” What such “appropriate measures” would be in practice, is neither defined nor discussed in the Directive or its Recitals. Besides the key escrow solution described herein, another option for the legislator could be to oblige content providers to adapt their DRM system so that it observes copyright limitations from the beginning; see Hart, supra note 62, at 62; Dusollier, supra note 64. For such direct influence of the legislature on the design of technological protection measures, see supra text accompanying notes 217-227. Another solution would be the mere statutory codification that rights holders have an obligation to cooperate with beneficiaries of copyright limitations; see Reinothe, supra note 62, at 742; Dreier, supra note 65, at 39; see also Vinge, supra note 62.
3. The most important restriction, however, which was introduced very late in the legislative process, is that the possibility for the legislature to establish a key escrow system depends on the business model the content provider chooses. If the content provider offers DRM-protected content downloadable over the Internet, and if access is conditioned on formation of a contract (e.g., by using click-wrap contracts), the member states are not allowed to establish any "key escrow" system at all (see Article 6(4)(4)). This hidden provision de facto eradicates the limitation allowing copies to be made for private purposes. In addition, by choosing a specific business model, content providers may dispose of all copyright limitations—a highly questionable development.

4. Removing Market Failures

a) In Theory

As was mentioned above, the legislature is not only institution that could alleviate the tension between technological protection measures and copyright limitations. Rather, a well-functioning competition between different DRM technology and content providers could reduce the tension as well. Unfortunately, in the DRM field, such competition is often impeded by market failures that stem from information asymmetries, indirect network effects, high switching costs, and lock-ins. Instead of attempting to cure the symptoms of these market failures, the legislature can address the underlying market failures themselves. If competition is impeded by network ef-

---

264. This means that if a DRM system prevents the making of temporary copies, which are ubiquitous on the Internet, by a technological protection measure, the member states cannot do anything about it, even though copyright limitation concerning temporary copies is the only limitation which all member states are required to implement into their national laws, see Article 5. See also Spindler, supra note 62, at 117.

265. Bechtold, supra note 19, at 425; see also Dusollier, supra note 64; Dreier, supra note 65, at 37; Spindler, supra note 62, at 117.

266. Reinboth, supra note 62, at 742.

267. The specific wording in Article 6(4)(4) “… that members of the public may access [the content] from a place and at a time individually chosen by them” means the “right of making available to the public”, see Article 3(2) of the Directive. This right covers all transmissions over the Internet, as long as the user is able to choose and initialize that transmission. See Hart, supra note 62, at 58; Bechtold, supra note 19, at 426. Non-interactive Internet transmissions do not fall under this provision, see Recital 53 to the European Copyright Directive, supra note 62. What constitutes a “non-interactive” transmission is unclear. While Reinboth, supra note 62, at 742, cites “pay per view” and “webcasting” as examples for non-interactive online services, Dreier, supra note 65, at 30, note 20, doubts this categorization; see also Spindler, supra note 62, at 108, 119. On the general problems of distinguishing between interactive and non-interactive services in copyright law, see Bechtold, supra note 75, at 25-26; Bechtold, supra note 19, at 426 note 2173.

268. Article 6(4)(4) provides: “The provisions [enabling member states to limit technological protection measures] shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.” It has been stated by some European Commission officials that Article 6(4)(4) is only intended to deal with video-on-demand and similar services. However, this is not what the wording of Article 6(4)(4) says; see Bechtold, supra note 19, at 426 note 2173; Hart, supra note 62, at 63; see also Dreier, supra note 65, at 37.

269. Spindler, supra note 62, at 119.

270. See also Vinje, supra note 62, at 557; Dusollier, supra note 64.

271. See also Vinje, supra note 62, at 555-558; Hugenholtz, supra note 62, at 501; Reinboth, supra note 62, at 742; Severine Dusollier, Exceptions and Technological Measures in the European Copyright Directive of 2001 - An Empty Promise, 34 International Review of Industrial Property and Copyright Law 62 (2003). For a similar attitude of the Copyright Directive concerning the possible tension between usage contracts and copyright limitations, see supra note 201.

272. See Bechtold, supra note 19, at 427.

273. See also Hart, supra note 62, at 63. A few years will still pass until sufficient experience with the various implementations of the Directive in the member states of the European Union will have been gained.

274. Bechtold, supra note 19, at 427-428; See also Vinje, supra note 62, at 555-558.

275. See supra text accompanying note 186.

276. See supra note 186.
fests and lock-in situations, for example, interoperability and inter-connection mandates between different DRM systems could reduce the negative implications of these effects.\textsuperscript{277}

b) In Practice

Legislatures have only started to experiment with this approach. One of the market failures that recur in DRM systems is an information asymmetry between DRM providers and consumers. Very often, before consumers install a particular DRM system or acquire DRM-protected content, they are not fully aware of the specific uses the DRM system allows and prevents. Due to information asymmetries, it is fully rational for the DRM provider not to reveal such information and for the consumer not to look for it, as the related transaction costs would be prohibitively high.\textsuperscript{278} Information asymmetries prevent competition between DRM systems that differ in the kinds and numbers of uses they allow.\textsuperscript{279}

To remove this market failure, the German legislator has recently included a provision into the German Copyright Act according to which content providers have to fully disclose the scope and characteristics of the DRM protection they use for their content. Thereby, consumers could make an informed decision about whether they want to buy the protected content or not.\textsuperscript{280} However, provisions that intend to enable well-functioning competition between DRM systems are still extremely rare.\textsuperscript{281}

\textsuperscript{277} See BECHTOLD, supra note 19, 407-408. For an abstract analysis of the relationship between network effects and interoperability/interconnection requirements, see Stefan Bechtold, Governance in Namespaces, 36 LOYOLA L.A. L. REV. 1239, 1273-1281 (2003); see also Mark A. Lemley & David McGowan, Legal Implications of Network Economic Effects, 86 CAL. L. REV. 479, 516, 599-600; CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES 186 (1999).

\textsuperscript{278} For a detailed analysis that builds upon Akerlof’s model of the market for lemons, see BECHTOLD, supra note 19, at 339-348. For an analysis that includes behavioral law and economics, see Russell Korobkin, Bounded Rationality and Uncensorship: A Behavioral Theory of Policing Form Contracts, 70 U. CHI. L. REV. 1209 (2003).

\textsuperscript{279} Or, in other words, they prevent competition between “fair-use-friendly” and “fair-use-hostile” DRM systems.

\textsuperscript{280} § 35d (1) of the German Copyright Act states: “Works and other protected subject matter, that are protected by technological measures, shall be labeled clearly with information about the characteristics of the technological measures used”. For a detailed analysis of this provision, see Bechtold, supra note 69, Rdnr. 166-185. In the United States, a similar bill was introduced into the Senate in March 2003, but, until now, has not been adopted by the Congress, see U.S. Senate, 108th Congress, S. 692, Digital Consumer Right to Know Act of 2003. The legislator is not the only institution that is able to alleviate market failures that result from information asymmetries. For the announcement of the International Federation of the Phonographic Industry (IFPI) to introduce a new logo for copy-protected CDs that could also decrease information asymmetries, see IFPI announces new optional copy control symbol for CDs, at http://www.ifpi.org/888/content/press/20020917.html (Sept. 17, 2002).

\textsuperscript{281} Whereas the German provision mentioned deals with information asymmetries, one European pay TV provision exists that deals with network effects, switching costs, and lock-in situations. Various standards developed by the “Digital Video Broadcasting Project” (DVB) allow several competing DRM systems (so-called “conditional access systems”, CAS) to be included in a single Pay TV set top box; for more information, see BECHTOLD, supra note 19, at 105 note 822; Carole Llorens-Malauqer, European Responses to Bottlenecks in Digital Pay-TV: Impacts on Plurality and Competition Policy, 16 COLUM. ARTS & ENT. L.J. 557, 560-563 (1998); European Commission, The development of the market for digital television in the European Union – Report in the Context of Directive 95/47/EC of the European Parliament and of the Council of 24th October 1995 on the Use of Standards For the Transmission of Television Signals, COM (1999) 540. This architecture and related approaches enable competition to occur between different providers of DRM systems in the pay TV market. In order to protect this competition, the European Access Directive prohibits DRM technology providers from using technology license agreements to thwart this competition, either by preventing interoperability between different DRM systems or by preventing the inclusion of a competing DRM system in the same set top box; see Annex I, Part 1, lit. (c) to Article 6 (1) of the Access Directive, supra note 210. This prevents DRM technology providers from using license agreements to impede competition between different DRM systems.

282 Dan Burk and Julie Cohen, for example, have proposed to combine the direct shaping of technological protection measures in certain areas with a key escrow system in other areas; see Burk & Cohen, supra note 158, at 65-70.

VI. CONCLUSION

With DRM systems, content providers may protect their interests by the combination of technology, usage contracts, anti-circumvention regulations, and technology license agreements. The intertwining of these different means of protection could supplant copyright protection to a large extent. Both in the United States and in Europe, legislatures support this trend towards a privatization of content protection by enacting broad anti-circumvention regulations and by increasingly accepting click-wrap licenses as valid contracts.

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 society at large. Legislators are required to react to this “overprivatization” and limit the different means of protection in a DRM system. Numerous theoretical approaches exist to reconcile DRM protection with copyright limitations. On both sides of the Atlantic, legislators have chosen to follow different paths. Unfortunately, in both the U.S. and Europe, the legal framework surrounding DRM systems is complex and does not offer any clear and consistent vision of how the tension between DRM protection and copyright limitations should be resolved.\textsuperscript{283}

Confronted with the myriad of problems in the context of digital rights management, 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, to some extent, still 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. The relationship between technological protection measures, usage contracts, and copyright limitations is only one, albeit important, example. The implications of DRM on competition and innovation in upstream and downstream markets are still a \textit{terra incognita} to a large extent.\textsuperscript{284} Legislators enact overly complex statutes, the implications of which nobody can really foresee. After copyright law has proactively shaped digital rights management over the last eight years,\textsuperscript{285} it seems that, before copyright law can return to its traditional role of reacting to the next disruptive technological change,\textsuperscript{286} it should first clear up the mess it has created.

\textsuperscript{283} For some general thoughts on how to proceed in order to develop a theory of copyright law in the information society, see Bechtold, supra note 77.

\textsuperscript{284} See Bechtold, supra note 12, at 619-630.

\textsuperscript{285} See supra text accompanying note 77.

\textsuperscript{286} See supra note 1.