Private Copyright: Digital Rights Management Systems and the Consumer

By V. Nick Knipe
vnk@law.georgetown.edu

Introduction

Before the Internet, transactions for copyrighted works were not treated much differently from transactions for other forms of property.[1] Any limitations upon the use of a copyrighted work were generally known to consumers and in place via copyright law.[2] Initial attempts by content holders to extend control of their work beyond the scope of copyright law were struck down by courts.[3]

The emergence of the digital age has radically changed the nature of consumer transactions for copyrighted goods. Copyrighted works in digital form (digital content) can be replicated and distributed on an enormous scale through use of personal computers and the Internet.[4] With potentially millions of infringers, traditional copyright law has

[1] See Llewellyn Joseph Gibbons, Stop Mucking Up Copyright Law: A Proposal for a Federal Common Law of Contract, *35 Rutgers L. J. 959, 959-960.*

[2] Consumers recognized themselves as the owner of the physical embodiment of the copyrighted work, but knew that Copyright law limited their ownership in various ways. See Id.

[3] The earliest and most famous of these attempts concerned the first sale doctrine. See *Bobbs-Merrill Co. v. Straus*, *210 U.S. 339 (1908)* (U.S. Supreme Court ruling that Copyright law did not permit a content owner to control second-hand sales of a copyrighted work); see also *Quality King Distributors Inc., v. L'anza Research International Inc*., *523 U.S. 135 (1998)* (where the Court found that a content holder could not prevent the distribution of "grey market" goods through Copyright law). The first-sale doctrine is now codified in U.S. law at 17 U.S.C. § 109. Commonplace business enterprises such as video rental stores have used §109 to flourish by not being required to gain the content-holder's permission for their activities.

[4] See Hisanari Harry Tanaka, Post-Napster: Peer-to-Peer File Sharing Systems: Current and Future Issues on Secondary Liability Under Copyright Laws in the United States and Japan, *22 Loy. L.A. Ent. L.*

been ill-equipped to enforce a content holder's rights.[5] Content holders[6] – with the support of Congress – have responded by employing Digital Rights Management (DRM) systems to protect digital content. This entails the use of a license agreement to which the consumer must consent, technological protections designed to stop or curb infringement of the digital work, and the support of legislation that makes it illegal to circumvent these technological protections.[7] DRM has had the effect of what many commentators have termed the "privatization of copyright."[8]

The result has been a market paradigm plush with legal issues regarding contracts, antitrust, privacy, free speech, and copyright fair use. This article does not pretend that it can cover each of these issues in detail. Rather, it seeks to examine these issues with respect to how this market paradigm affects the consumer and what changes can be made to bring about a more sensible digital content market in the United States.

This article is presented in four parts. Part I outlines the relevant provisions of the Copyright Act of 1976 and provides background information on DRM systems. Part II discusses how the use of DRM systems has impacted consumer digital content

Rev. 37, 38 (2001); see also Raymond Shih Ray Ku, The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology, *69 U. Chi. L. Rev. 263* (2002).

[5] See Assaf Hamdani, Who's Liable for Cyberwrongs?, *87 Cornell L. Rev. 901, 910 (2002).*

[6] Throughout this paper I use the term "content holder" to refer to any person or entity that holds legal copyright title to music, video, software, or anything else capable of being protected by Digital Rights Management systems.

[7] See generally Stefan Bechtold, Digital Rights Management in the United States and Europe, *52 Am. J. Comp. L. 323.*

[8] See id. at note 161; Charles R. McManis, The Privatization (or "Shrink-Wrapping") of American Copyright Law, *87 Cal. L. Rev. 173*; Robert P. Merges, Intellectual Property and the Costs of Commercial Exchange, *93 Mich. L. Rev. 1570, 1613 (1995);* Niva Elkin-Koren, Copyrights in Cyberspace – Rights Without Laws?, *73 Chi.-Kent L. Rev. 1155, 1164-1165 (1998).*

transactions. Part III proposes steps that can be taken to make aspects of this market more fair and transparent. Concluding thoughts are discussed in Part IV.

I. BACKGROUND OF THE DIGITAL CONTENT MARKETPLACE

A transaction for DRM-protected digital content involves several parties – the consumer, the content holder, and consumer device manufacturers – and possibly conflicting legal frameworks – federal copyright law and the contract law of the state in which the transaction took place. This section will provide an overview of how these different entities and legal areas interact to shape the digital content marketplace.

A. The Copyright Act

Copyright law is a balancing act between providing incentives for authors to create original works and the "general benefits derived by the public from the labors of authors."[9] The Copyright Act of 1976[10] (the Copyright Act) enumerates the rights of copyright holders and codifies defenses to copyright infringement. It has been amended several times since its enactment. The most significant of these was the Digital Millennium Copyright Act[11] (DMCA) of 1998, but its provisions will be omitted here so it can be introduced in a better context.

[9] *United States v. Paramount Pictures, Inc., 334 U.S. 131, 158 (1948)*, quoting *Fox Film Corp. v. Doyal et. al., 286 U.S. 123, 127 (1932).*

[10] *17 U.S.C. 101-810.*

[11] *Pub. L. 105-304.*

1. The Bundle of Rights Granted to the Content Holder

To provide incentives to authors to generate original works, the Copyright Act grants exclusive rights to "original works of authorship fixed in any tangible medium of expression…. which can be reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[12] As this provision implies, digital content is protected by the Copyright Act because it is read with the aid of a device. In the case of computer programs, copyright protection extends to both the source code and the object code.[13]

The Copyright Act gives the content holder many exclusive rights, the most important of which is the right to exclusively reproduce copies of the work. Other important rights are the right to create derivative works and the right to alienate any of the exclusive rights granted by copyright. Alienation permits the content holder to license the work or derivative works as they see fit.

2. Basic Copyright Exemptions for the Public

[12] *17 U.S.C. 102.*

[13] The source code of a computer program is the human-readable text that the program is written in. While source code can still be arcane to a layman, it is understandable by a person versed in the computer language. Object code is source code that has been compiled into commands that the computer hardware can understand. It consists of strings of 1's and 0's and is void of any cognizable human element. For an analysis of the copyrightability of source code and object code, see *Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3rd Cir. 1983).*

The Copyright Act also seeks to ensure that the public can benefit from the creation of original works by limiting the monopoly that copyright grants to the author of an original work. Three of these limitations are relevant to the discussion in this article: the first sale doctrine, the exceptions for computer programs, and fair use.[14]

i. The First Sale Doctrine

The first sale doctrine allows the "owner" of a copy of a copyrighted work to sell that copy without the permission of the copyright holder.[15] This severs a content holder's distribution rights of a particular copy of a copyrighted work once that copy is sold downstream. The seminal case in the first sale doctrine occurred before its codification as § 109 of the Copyright Act. The Supreme Court ruled in *Bobbs-Merrill*[16] that resale of a book could not be prohibited by the copyright holder because there was no privity of contract between the copyright holder and the consumer.[17] Copyright law by itself did not grant the copyright holder any such right to control second sales of the work.[18]

[14] Qualifying these limitations as "rights" is somewhat of a misnomer. The first sale doctrine and the computer program exceptions only apply to the "owner" of a copy of a copyrighted work, not necessarily to the general public (e.g., a licensee or non-party). See *17 U.S.C §§ 109, 117*. Despite the undisputed importance of fair use and the characterization of it as a "right" by many commentators, it is properly understood as a defense to copyright infringement. See *Eldred v. Ashcroft, 537 U.S. 186, 210* (the U.S. Supreme Court characterizes fair use as a defense).

[15] *17 U.S.C. 109*.

[16] Supra, note 3.

[17] A printed notice in the book that stated second sale restrictions was insufficient to establish privity of contract. Id. at 342.

[18] *Id.* at 350.

The first sale doctrine becomes complicated when applied to digital works because many digital works involve a license and not a traditional transfer of ownership[19]. There has been legal confusion as to whether a licensee qualifies as an owner for purposes of the first sale doctrine. The courts that have construed such licenses to constitute ownership in this respect have either cited a disdain for "shrink-wrap" licenses,[20] suggested the terms of the contract are substantially similar to the rights of an owner under federal copyright law,[21] or have otherwise hinted that such licenses are preempted by federal law.[22] Some courts have held otherwise, finding that the first sale doctrine is inapplicable in a licensing agreement.[23]

ii. Computer Program Exceptions

[19] This is mostly the case in computer software and content downloaded from the Internet. See *Adobe Systems, Inc. v. One-Stop Micro, Inc., 84 F. Supp. 2d 1086, 1091-1092 (N.D.C.A 2000)* (citing evidence that almost all software manufacturers use a license agreement).

[20] See *Novell, Inc. v. Network Trade Ctr., 25 F.Supp.2d 1218, 1229-1231 (C.D. Utah 1997)* (where the court determined that consumer purchases of plaintiff's product from the defendant qualified as sales under the U.C.C., and cited disdain for the shrink-wrap license of the plaintiff's product that "modify the original purchase agreement with the retailer.").

[21] See *Step-Saver Data Systems, Inc. v. Wyse Technology and the Software Link, Inc., 939 F.2d 91, 100 (3rd Cir. 1991)* (stating that the terms of the license agreement are almost identical so as if the transaction were "characterized as a sale of a copy.").

[22] See id., note 7 (where the court suggests that purpose of computer program license agreements are to "avoid the federal copyright law first sale doctrine," raising questions of federal preemption.); but see id., note 27 (stating that the court does not intend to "resolve the sale-license question.").

[23] See *Adobe at 1089-1092* (holding that a license agreement is sufficient to find the first sale doctrine inapplicable); *Davidson & Associates, Inc. v. Internet Gateway, 334 F.Supp.2d. 1164, 1178 (E.D. Mo. 2004).*

Congress recognized computer software as somewhat unique to the rest of copyright because of its functionality. [24] Accordingly, the Copyright Act limits the exclusive rights granted to the content holder of a computer program in § 117 by permitting the "owner" of a copy of that software to create copies as "an essential step in the utilization of the computer program"[25] or for "archival purposes."[26]

Similar to the provisions of the first sale doctrine, the computer program exceptions grant these exceptions to the "owner" of the copy of the work, leaving it unclear as to the rights of software licensees. Raymond Nimmer dissects this dilemma best in stating that "[e]ither a licensee can never be the owner of a copy for purposes of § 117 or ownership of the licensed copy depends on the terms of the license agreement."[27] Some courts have drawn on the former interpretation and denied ownership rights to those without formal title.[28] Other courts have found formal title not to be dispositive of §

[24] Computer software has both expressible elements (protected by copyright law) and functional elements (protected by patent law). In order to use the functional elements of a computer program, a computer must "copy" the computer code from its storage on a hard drive (where the program can only be read at a comparatively slow pace) to the computer's random access memory (better known as RAM, where the computer can access and run the program at a faster pace). Thus copyright law would punish those who merely run a computer program without being licensed to do so (e.g., a computer repair technician who was not licensed to "copy" the software by the copyright holder). For the seminal case in this dilemma, see *MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993)*; see also Final Report of the National Commission on New Technological Uses of Copyrighted Works (July 31, 1978) (CONTU Report) at 31.

[25] *17 U.S.C. 117*(1). This is to avoid the undesirable result where using the software would constitute copyright infringement because the computer must copy the program from storage into its RAM memory in order to utilize the program. See generally *MAI*, supra note 14.

[26] *17 U.S.C. 117*(2).

[27] Raymond T. Nimmer, Law of Computer Technology: Rights Licenses Liabilities, *§ 7:69* (3d ed. 2003).

[28] See *MAI*, supra note 14, at note 5 (shortly stating that defendant is a licensee and thus cannot qualify as an "owner" for purposes under § 117); *Advanced Computer Computer Servs. of Mich., Inc. v. MAI Sys. Corp.*, *845 F. Supp. 356, 367 (E.D. Va. 1994)* (same); *CMAX/Cleveland, Inc. v. UCR, Inc.*, *804 F.Supp. 337 (M.D. Ga. 1992)* (stating that leasing and having possession of software does not qualify one as an "owner" under § 117).

117 ownership and analyze the license agreement to determine whether the contract "exercises sufficient incidents of ownership over [the copy of the program]" where the licensee could "be sensibly considered the owner of the copy."[29]

iii. Fair Use

Fair use – codified in § 107 of the Copyright Act – is a doctrine that provides a defense to copyright infringement so as to seek a balance between the competing goals of providing incentives for creative innovation and giving the general public use of these innovations.[30] § 107 provides for a four-factor balancing test that a court should consider when analyzing a fair use defense: (i) purpose and character of the use; (ii) the amount and substantiality of the portion used; (iii) the nature of the copyrighted work; and (iv) the effect of the alleged infringement upon work's potential market or value.[31] The availability of fair use has been heavily debated with respect to DRM and copyright restrictions. However, this article addresses fair use only in the context that it directly restrains consumer use of the work: time shifting and space shifting.[32]

[29] *Krause v. Titleserv, Inc., 402 F.3d 119, 124 (2nd Cir. 2005)* (finding § 117 ownership where the licensee had a permanent ownership and the software was created specifically for the licensee's purposes); see *Telecomm Technical Services Inc. v. Siemens Rolm Communications, Inc.*, *66 F. Supp. 2d 1306, 1325 (N.D. Ga. 1998)* (finding ownership within the meaning of § 117 because the software license was granted forever in return for a single payment); see also 2 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 8.08[B][1][c]. But see *DSC Communs. Corp. v. Pulse Communs., Inc.*, *710 F.3d 1354, 1360-1362 (Fed. Cir. 1999)* (stating that not all licensees are "non-owners" for purposes of § 117, but that the restrictions in the license agreement there were indicative of finding no ownership).

[30] See *Sony Corp. of Am. v. Universal City Studios, Inc. (Sony Betamax)*, *464 U.S. 417, 479 (1984)*.

[31] *17 U.S.C. 107.*

[32] Other heavily-debated fair use issues such as commentary are better addressed in a free speech context than in a consumer protection context.

Time shifting entails the recording of television programming onto a device – such as a VCR or digital video recorder (DVR) – so as to be viewed at a more convenient time. Time shifting was sanctioned as fair use in the landmark Supreme Court case *Sony Betamax*, where the Court determined that Sony's Betamax video recorder was not liable for indirect infringement because it was capable of significant non-infringing uses.[33]

Space shifting is a fair use concept permitting the owner of a copy of a work, such as a digital music file (e.g., an mp3 file), to convert that copy to another format. It is argued as an analogy to time shifting, but has been met with mixed results. Some courts have found it to constitute fair use by qualifying it as "paradigmatic noncommercial personal use."[34] Others have rejected it, stating that "[c]opyright… is not designed to afford consumer protection or convenience but, rather, to protect the copyrightholders' property interests."[35]

Under the current legal framework time shifting has been determined as fair use, but space shifting as fair use has not been as well-established.

B. DRM Systems

[33] *Sony Betamax*, supra note 32.

[34] *Recording Indus. Ass'n. of Am. V. Diamond Multimedia Sys., Inc.*, *180 F.3d 1072, 1079 (9th Cir. 1999)*;

[35] *UMG Recordings, Inc. v. MP3.com, Inc.*, *92 F. Supp. 2d 349, 352 (S.D.N.Y. 2000)*; see *A&M Records, Inc. v. Napster, Inc.*, *239 F.3d 1004 (9th Cir. 2001)* (finding that space shifting could not be construed as fair use when the converted media would be widely available to piracy).

DRM systems are technological safeguards that provide a means for copyright holders to control the downstream consumption, access, and control of their digital content.[36] DRM systems can be simplistic – perhaps just prevent end-user copying – or they can facilitate intricate business models.[37] The potential regulatory ability of DRM is so profound that many commentators have suggested that DRM systems has enabled the "privatization" of copyright and the next generation of copyright legislation will aim to forge public access to DRM-protected works.[38]

This article introduces DRM systems through its four main features: (1) technological protections, (2) the DMCA, (3) end-user license agreements (EULAs), and (4) consumer technology licenses.

1. DRM Technological Protections

DRM systems will typically use several technologies to protect digital content. The intertwining of these technologies helps establish a secure platform for transmitting digital content.

The most important of the technologies used in DRM is probably the encryption technologies.[39] Encryption technologies effectively hinder the copying of digital content

[36] See Bechtold, supra note 6, at 52.

[37] Id.

[38] See Yochai Benkler, An Unhurried View of Private Ordering Information Transactions, *53 Vand. L. Rev. 2063, 2078 (2000)*; Lawrence Lessig, Code and Other Laws of Cyberspace 125, 130 (1999);

[39] See Dean S. Marks & Bruce H. Turnbull, Technical Protection Measures: The Intersection of Technology, Law, and Commercial Licenses, *22 Eur. Intell. Prop. Rev. 198, 204 (2000)*.

because any copies of that content can only be used if the decryption key is provided.[40] Without the decryption key, the digital content is gibberish. The decryption keys can be provided in many ways, but they must not be directly accessible by the user. If a user has access to the decryption key, the encryption technology is compromised because the content is then freely accessible by the user. The decryption keys are often embedded in hardware devices to make access to the keys very difficult. This helps ensure the security of the DRM system because hardware is more "tamper-proof" than software. But it is important to note that the use of hardware does not make the security of a DRM system infallible.[41]

DRM systems are not employed just to protect content but to manage content as well. "Meta-data" is information embedded as preamble to the digital content or in the content itself[42] that tells the DRM system who is entitled to use the content and with what rights or privileges. This allows the content holder to control in minute detail how the digital content is used.[43]

DRM systems can take assertive action to protect digital content. A DRM system can block access to digital content if it detects or suspects any irregularities. This could consist of the discovery of pirated content or devices that have been tampered with to

[40] See id.; Bechtold, supra note 6, 326.

[41] See, e.g., *Universal City Studios, Inc., v. Corley*, 273 *F.3d 429 (2d Cir. 2001)* (where at issue was the successful circumvention of CSS, the DVD DRM system that was embedded in DVD players).

[42] Embedding meta-data within the digital content is known as "digital watermarking." It is typically more difficult for hackers to circumvent because removing the watermark will degrade the content or possibly make the content useless. See Frank Hartung & Martin Kutter, Multimedia Watermarking Techniques, 87 Proceedings of the IEEE 1079 (1999).

[43] Bechtold, supra note 6, 326.

circumvent the DRM protections.[44] More complex DRM systems can monitor a user's activities or file system and communicate this information back to the content holder though the Internet.[45] It also can automatically update itself so as to keep the consumer equipped with the most robust protection system available.

The difficulty in implementing a DRM system is that the DRM protections must be standardized into consumer devices. Each device and component in the DRM system must be unable to transmit the content to the consumer in an unencrypted digital form.[46] As an example, the DRM protection system used in DVDs, CSS, must ensure that each device capable of decrypting CSS-encrypted content does not transmit that content to a consumer in unencrypted digital form. It is acceptable if the device transmit an unencrypted analog signal to a consumer.[47] However, the purpose of the DRM system would be frustrated if the device transmitted a digital signal to a digital television which in turn allowed the user access to the unprotected digital content. A robust DRM system must ensure that the digital television device does not allow the user access to digital content, and the most appropriate way to achieve this is to standardize the way devices

[44] Id. at 328. See also Dave Marsh, Output Content Protection and Windows Vista (April 27, 2005), available at http://www.microsoft.com/whdc/device/stream/output_protect.mspx (Jan. 10, 2007).

[45] Elizabeth G. Thornburg, Going Private: Technology, Due Process, and Internet Dispute Resolution, *34 U.C. Davis L. Rev. 151, 175 (2000).*

[46] See Marks & Turnbull, supra note 42, at 204. Various groups have come together to try and balance the needs between the device manufacturers and the content holders to develop standard DRM systems. See Bechtold, supra note 6, at 330.

[47] The emission of an analog signal presents a reduced danger of piracy since there is an inherent degradation of quality in analog signals.

implement the DRM system. Computing systems are being developed and tested today to ensure that digital content can never be transmitted in an unencrypted form.[48]

2. The DMCA's Anti-Circumvention Provisions

The private sector by itself is not sufficient to protect digital content. DRM systems are all vulnerable to being circumvented by hackers.[49] The widespread distribution of circumvention technologies can completely compromise a DRM system. To help curb this problem, Congress provided content holders with legal tools to reinforce DRM protection through the passing the DMCA in 1998.[50]

The DMCA has two provisions relevant to DRM. The first provision makes it illegal to personally circumvent or traffic in tools that allow the circumvention of technologies that control access to digital content (e.g., authentication measures).[51] The second provision makes it illegal only to traffic in tools that allow the circumvention of usage controls; that is, technologies that control how digital content can be used.[52] The personal circumvention of these usage controls is not controlled by the anti-

[48] Microsoft Corp.'s new operating system Windows Vista plans to facilitate complete lock-down on protected content, ensuring each device is compliant with a given DRM standard to ensure no content escapes in a useable unencrypted digital format. See Marsh, supra note 45.

[49] Bechtold, supra note 6, at 331. The secret keys to the DVD security system CSS was hacked by a 15-year-old Norwegian boy.

[50] *17 U.S.C. § 1201*(a), (b).

[51] *17 U.S.C. §1201*(a)(1), (2).

[52] *17 U.S.C. §1201*(b)(1).

circumvention provisions because traditional copyright law governs to what extent an individual may copy or use a copyrighted work.

U.S. courts have typically applied the letter of the law to anti-circumvention cases.[53] However, some court decisions have refused to grant relief when the anti-circumvention provisions are used to control access to down-stream markets and not actually copyrightable works.[54]

3. DRM Usage Contracts

DRM also protects the digital content by requiring consumers to enter into a contractual agreement, often called an "End-User License Agreement" (EULA), when they use DRM-enabled hardware, software, or content. EULAs are used to establish privity of contract with the copyright holder and the end-user.[55] They are typically in the form of "shrink-wrap" or "click-wrap" licenses.[56] The consumer must agree to the license and permit the DRM system to regulate her conduct accordingly; there is generally no possibility for bargaining.[57]

[53] See *Sony Computer Entertainment America, Inc. v. Gamemasters, Inc.*, *87 F. Supp. 2d 976 (N.D. Cal. 1999)*; *RealNetworks, Inc. v. Streambox, Inc.*, *2000 WL 127311 (W.D. Wash. 2000).*

[54] *See Lexmark Intern., Inc. v. Static Control Components, inc., 387 F.3d 522 (6th Cir. 2004)*; *Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir., Aug. 31, 2004).*

[55] See Bechtold, supra note 6, at 341. Establishing privity gets around the problem in *Bobbs-Merrill* where the U.S. Supreme Court established the first sale doctrine when there is no privity of contract between the copyright holder and the consumer. See *Bobbs-Merrill,* supra note 3.

[56] See Bechtold, supra note 6, at 342-343.

[57] Thornburg, supra note 48, at 175.

EULAs serve two purposes. First, they give the copyright holder substantially more control over the use of the work by restricting the scope that the consumer can use the digital content under traditional copyright law.[58] Second, EULAs help ensure that the DRM system remains secure. Many require that the user consent to automatic updates to ensure its client software be the most current.[59] Other provisions require that the consumer understands her use could be immediately terminated upon detection of illegitimate use. Furthermore, EULAs will typically require that the user not engage in reverse-engineering activities for any purpose.[60] These provisions aid in ensuring that the DRM system remains robust.

EULAs are generally enforceable in both the United States and Europe. U.S. courts initially greeted EULAs with skepticism,[61] but the trend recently has been strongly in favor of enforcement.[62] This is not to say that all EULAs are enforceable, but most companies have been successful in using EULAs to support their DRM system.[63]

[58] See id.

[59] See Bechtold, supra note 6, at 340.

[60] See id.; Thornburg, supra note 48, at 174-176.

[61] See *Step-Saver Data Systems*, supra note 25; see also Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, *68 S. Cal. L. Rev. 1239, 1248-1260 (1995).*

[62] See *ProCD, Inc. v. Zeidenberg, 86 F. 3d 1447, 1450-1453 (7th Cir. 1996);* see also *Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997); Brower v. Gateway 2000, Inc., 676 N.Y.S.2d 569, 572 (N.Y. App. Div. 1998); Davidson & Associates,* supra note 27, 1176-1178; *I. Lan Systems, Inc. v. Netscout Service Level Corp., 183 F. Supp. 2d 328, 338-339 (D. Mass. 2002); Steven J. Caspi, et. al. v. The Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); Groff v. America Online, Inc., 1998 WL 308001 (R.I. Super. Ct. 1998).* The EU has also confirmed the enforceability of these licenses by Article 9(1) of the European E-Commerce Directive. See Bechtold, supra note 6, at 344.

[63] See id. at 344. Some EULAs have been struck down by U.S. courts in recent years. See *Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332 (Kan. Dist. 2000)* (stating that silence is insufficient for acceptance of a contract to which terms were added); *Specht v. Netscape Communications Corp., F. Supp. 2d 585 (S.D.N.Y. 2001)* (where the court found there must be mutual consent, and merely providing a link to the EULA was insufficient; the EULA must be presented before the user can download).

4. Consumer Technology Licenses

To incorporate the use of hardware in DRM systems, content holders must ensure that their DRM specifications are built into all of the consumer electronics devices that read their content. DRM protection would be flawed if a commercially-available device provided a loophole to permit digital copies.[64] Naturally, manufacturers of consumer technology devices must produce products that can use available content. If the available content is encrypted using a patented DRM mechanism, the manufacturers must license that technology to make commercially-viable products. These licenses are not flexible. The manufacturer must agree to all the specifications made by the content holders, regardless whether or not those specifications relate to piracy protection.[65] Content holders use this licensing scheme to protect their content while providing consumers the means to play their content.

II. THE DIGITAL CONTENT MARKETPLACE AND THE CONSUMER

The use of DRM systems in the digital content marketplace places several burdens on consumers. While we expect certain burdens on consumers in various situations, many of

[64] An analog hole currently exists today in most DRM systems. However, analog holes are less worrisome because of the attrition of quality inherent in analog copies.

[65] For example, DVD players cannot skip through segments of content that is specifically marked not to be skipped by any particular DVD. This enables the content holder to force the consumer to view preamble warnings, coming attractions, or credits. Also, DVD players must incorporate a regional coding system so that a DVD player will only play content for the region it was licensed to play. This allows the content holders to control the sale of DVDs to different markets without having to worry about gray-market goods.

these burdens in the digital content marketplace fall in areas that run afoul of legitimate consumer expectations.

This section will analyze how the current digital content market burdens the consumer. It will address (1) EULAS; (2) consumer expectations of copyright limitations; (3) privacy; and (4) competition issues.

A. Usage Contracts and Market Policy

The use of shrink-wrap or click-wrap contract forms to impose a EULA is ubiquitous in the marketplace for digital works. Use of a digital work becomes conditional upon the consumer clicking the “I Accept” button and thereby agreeing to the terms presented on a scrollable window on the computer screen. The EULA contains pertinent information to the transaction. The majority of these EULAs term the transaction between the digital content holder and the consumer as a “license” to use the content, revocable by the content holder in certain circumstances. It attempts to define the scope of the consumer’s right to use the content, and often reserves the right to enforce these usage rules through DRM-enabled software.[66] Many provisions like these have become widely accepted

[66] See Bechtold, supra note 6, at 339.

while others are possibly unconscionable.[67] This paper will focus on the burdens posed by a EULA with otherwise conscionable terms.[68]

EULAs unfairly burden the consumer because consumers are ill-suited to comprehend the scope of such agreements. Do consumers ever actually read these license agreements? The answer is usually no.[69] But even if the EULA is read, did the consumer understand it? Again, the answer is probably no.

EULAs are often ignored because they are long, complicated and replete with technical terms, making for a demanding read.[70] User frustration is likely amplified in a computerized environment. The appeal of making purchases on the Internet or using computer software is its inherent efficiency. Digital content today can be made available in seconds. It is unreasonable to expect a consumer to bottle-neck the expediency of a transaction to read a lengthy contract when it can be circumvented with a mere click of "I Accept." Furthermore, consumers are inclined to ignore these contracts because many will feel that it would not be practical for the content holder to enforce the terms against them or because they assume it will not affect their use.[71] Also, the cost of the transaction

[67] See Annalee Newitz, Dangerous Terms: A User's Guide to EULAs, Electronic Frontier Foundation, available at http://www.eff.org/wp/eula.php (providing examples of ridiculous terms such as agreeing not to criticize the product publicly, not to use other vendor's products to remove bundled spyware, to implicitly accept any future changes the content holder might make to the EULA without notice, and revoke any implied warranty and liability to any damage caused by the software).

[68] Unconscionable terms would have good chance of being thrown out in court. Alternatively, an analysis of why otherwise conscionable terms in a EULA is inappropriate makes a stronger argument for a change in the marketplace.

[69] See "It Pays to Read License Agreements", available at http://www.pcpitstop.com/spycheck/eula.asp (where to prove a point, a software company provided a clause that offered monetary consideration to anyone who could show that they read a specific clause; thousands of people downloaded the software before someone meekly wrote in to receive $1,000).

[70] See Gibbons, supra note 1, 1001.

[71] See Newitz, supra note 69.

plays a role in whether the consumer will feel it worthwhile to subject herself to reading the terms. Many digital content transactions involve a relatively small amount of_money. Consider Apple's iTunes, where the client application software is free, but the purchase of a song is $0.99.[72] A consumer cannot be reasonably expected to read the lengthy iTunes EULA agreement when she only anticipates making a few dollars in purchases. However, when she has amassed a 200-song library, those terms become significantly important.

Consumer misunderstanding of EULA agreements is not limited to the confusing legal jargon found in many contracts.[73] Consumers are often faced with complicated, ever-changing usage rules.[74] In iTunes, the user is prevented from burning a specific music playlist over a specified number of times.[75] By itself that might be reasonable, but what is left unanswered is to what degree the playlist needs to be altered until it can again be burned to CD.[76] This kind of information might be critical because iTunes's usage rules could be strict enough to severely impact consumer purchase choices. How does iTunes go about describing its function for determining adequate playlist difference?

[72] See "Why 99 cents per song", available at http://www.marginalrevolution.com/marginalrevolution/2004/01/why_99_cents_pe.html

[73] See James Grimmelmann, Regulation by Software, *114 Yale L.J. 1719, 1728 (2005).*

[74] Consider Microsoft's new Zune music player, created to rival Apple's iPod. It has a function coined "squirting," whereby a Zune player can send a song to another Zune player within range. Microsoft had to compromise with the major record labels to only allow the "squirted" song to be deleted after three plays or three days, whichever first. See Steven Levy, Tune Into Zune?, Newsweek, Nov. 11, 2006, available at http://www.msnbc.msn.com/id/15669798/site/newsweek/ (Jan. 10, 2007).

[75] See Features Last in iTunes Upgrades, available at http://www.george.hotelling.net/90percent/digital_music/features_lost_in_itunes_upgrades.php.

[76] Grimmelmann, supra note 75, at 1754.

Such a function might involve complicated computations, something beyond the purview of average consumer understanding.

Even if we favor a policy reflecting a kind of *caveat emptor* for EULA contracts, there is still reason to sympathize with the consumer. At least one commentator has suggested that many companies purposely arrange EULAs in such a manner so as to ensure consumer vexation.[77] The goal in such cases is to provide the consumer with as much incentive as possible to click the "I Agree" button and bypass the EULA. The current enforceability of EULAs enable businesses to benefit from such practices.

The acceptance of EULAs as currently presented is inconsistent with a market policy that seeks mutual acceptance in contracting. Most often these contracts are not read or adequately understood by buyers. That does not mean that standard form contracts are unreasonable. The astounding amount of end-users simply would not permit a content holder to negotiate on a case-by-case basis. But the digital content market in its current form is not transparent to the consumer. While it may be convenient for the content holders to place the burden on the consumer, the reality of the situation is that the consumer is most likely to be unaware of the terms and restrictions of the content that she is purchasing.

B. DRM and Consumer Expectations of Copyright Limitations

[77] Gibbons, supra note 1, at 1001.

DRM systems have, without a doubt, imposed tighter restrictions on content use than the Copyright Act itself.[78] This privatization of copyright has sparked vigorous debate over the balance between authors' rights and public rights. Those copyright issues we address here – time shifting/space shifting, first sale doctrine, and the §117 computer program exceptions – are also qualitatively different from many other copyright defenses because they represent efficiency exceptions that the courts or Congress have carved out for consumers.[79]

1. DRM with Time Shifting and Space Shifting

Time shifting and space shifting represent two consumer fair use defenses that DRM will probably gain greater influence over. The budding use of trusted computing and similar technologies will help ensure that digital content remains under the purview of the content holders' control.[80] These technologies ensure that a "trusted" device will only interact with other "trusted" devices. Thus, a trusted device can be used to make certain that digital content is only handled by hardware that respects how the content

[78] See Bechtold, supra note 6.

[79] Concepts such as fair use parody and fair use commentary are beyond the scope of this article as they do not directly affect the consumer. Fair use parody involves the copying of a work so as to satirize the work. Fair use commentary permits one to use a work to comment on it, such as in a news program. Both forms are protected by fair use because often the content holder would be adverse to permitting such uses of the work. See, e.g., *Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994)*.

[80] See Trusted Computing: Promise and Risk, EFF, available at http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php.

holders want their content used. Content holders can impose such computing devices on consumers through DRM consumer device manufacturing licenses.[81]

However, the situation is not so dire so as to think DRM will spell the end of time shifting and space shifting. There is huge consumer demand for devices that facilitate this kind of use. It is irrational to assume the digital content market would be unable to find an agreeable solution in the face of such high demand. But the way in which these devices are used may change. For example, devices like DVRs that record TV shows for time shifting purposes have irked content holders because they allow viewers to skip commercials, reducing the value of advertising. DRM technology could prevent the viewer from skipping advertising or, concurrently, provide a service whereby the consumer pays a premium for the ability to fast forward commercials. Space shifting devices similarly have a high consumer demand where a market solution can be reached. We are already seeing enormous success with devices like Apple's iPod, which has balanced consumer usability with protection for content holders through its DRM system FairPlay.[82] High consumer demand can promote solutions where both the interests of consumers and content holders are accounted for.

2. DRM with the First Sale Doctrine and the Computer Program Exceptions

[81] See infra Part I.B.4.

[82] See iTunes Store: Terms of Service, available at http://www.apple.com/legal/itunes/us/service.html (Jan. 10, 2007).

The first sale doctrine and the § 117 computer program exceptions exist as defenses when one is the "owner" of a tangible copy.[83] The rampant use of EULAs in the digital content marketplace raises questions whether these consumer-licensees are entitled to the rights of an "owner."[84] The answer *should* be a cut-and-dry "no": it was recommended to Congress to adopt the term "possessor" to avoid this dilemma, but Congress instead chose to use the term "owner."[85] This would suggest that Congress intended for the courts to treat owners and licensees differently.

But in practice the answer has not been so clear because in the consumer's mind these transactions still resemble a purchase for ownership. Ownership is implied by the frequent use of life-time licensing terms.[86] As previously mentioned, the use of shrink-wrap agreements to convey these licenses has displeased some courts and many commentators. These licenses are so often skipped over or misunderstood that it is clear consumers place little gravity on the contract. It is no wonder that some courts have been reluctant to deny licensees ownership rights in this respect.[87]

DRM systems cripple the first sale doctrine and § 117's archival copy exception as they apply to consumers. DRM systems can regulate in these respects with or without the use of EULAs: the DMCA anti-circumvention provisions provide the requisite reinforcement to DRM measures that prevent archival copying or software tampering.

[83] See *17 U.S.C. 109, 117.*

[84] See infra Part I. B.3

[85] See *Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, note 11 (5th Cir. 1988).*

[86] See *Krause*, supra note 31, at 123-24.

[87] See *Vault*, supra note 84, at; *Step-Server Data Sys. V. Wyse Tech., 939 F.2d 91 (E.D. Penn.1991).*

DRM can also keep track of digital content to prevent a second sale. For example, Microsoft introduced "product activation" in its Service Pack 2 to Windows XP. By requiring users to activate their software with Microsoft servers, Microsoft is effectively able to tie each copy of Windows XP to work with only one computer. Windows XP makes a unique identification number of the computer it is installed on by compiling the computer's hardware specifications, and that copy of Windows is only usable on the computer with that unique identification number.[88] In order to make a second sale of the copy of Windows XP, it may not be enough for a consumer to uninstall it from her computer. She may have to sell the entire computer as well, and even that might not be permitted.[89] iTunes also hinders second sales by tying each song purchased from its online store to a user account which allows activation on up to five computers. Transferring individual songs to others is not included in the usage rules. [90]

Allowing second sales and archival copies may not be resolved by the market because the content holders lack the incentive to permit them. Enabling a DRM system to permit second sales would only be profitable if the consumer appeal of being able to make second sales increases revenue by more than the content holders would lose through the second sales themselves. The ability to resell digital content probably ranks well-below other consumer incentives to purchase.[91] Furthermore, current sales may be

[88] See Jennifer Granick, "Do Antipiracy Measures Rob Consumers?," available at http://news.com.com/2009-1001-251044.html?legacy=cnet (Jan. 10, 2007).

[89] Because Microsoft has tied the copy of Windows to the seller's computer, the buyer would be unable to activate the software on the buyer's computer.

[90] See iTunes Store: Terms of Service, supra note 82.

[91] See "New Report From the NPD Group Provides Insight Into What Drives Consumers to Purchase PC and Video Games", available at http://www.npd.com/press/releases/press_061026.html.

unaffected by any such demand because consumers may believe that they are entitled to a second sale having not read the EULA. Likewise, allowing archival copies for systems with product activation could mean the content holder loses sales for those who must purchase the product again in the case the consumer has lost the original copy. For digital content without product activation, allowing archival copies will facilitate illegal copying. Understandably, content holders would see it as a pointless service to allow.

Predicting the existence of these copyright exceptions in a DRM system requires analyzing whether the content holder benefits from the exceptions' efficiencies. Content holders probably stand to benefit from time and space shifting because of the consumer demand associated with it. The first sale doctrine and the archival copy computer exception do not share a like consumer demand and will probably not be widely available.

C. DRM and Privacy Concerns

DRM systems impact consumer privacy concerns because these systems have enormous potential for data collection and distribution.[92] Three questions must be asked of any DRM monitoring systems.

Who has access to the collected information? Controlling the flow of personal information is central to privacy. Consumers have a valid interest in whether the information is contained internally by the content holder or being sold to unknown third parties. Informing consumers about data access procedures lets the consumer know who

[92] See Julie Cohen, The Law and Technology of Digital Rights Management: DRM and Privacy, *18 Berkeley Tech. L.J. 575 (2003).*

to hold responsible if their information is made available. This information is easy for the content holder to provide to the consumer.[93]

What is the data being used for? This is important in the consumer's calculation concerning how much, if any, personal information she is prepared to share.[94] A consumer will be less inclined to offer information if it is used for marketing purposes as opposed to product research. Data can also be used for so called "self-help" purposes.[95] Self-help techniques detect unauthorized use and disable access to a work without the need to use the legal system.[96] Self-help measures can be self-contained – meaning that unauthorized access is detected solely by the monitoring software – or the monitoring system can be supplemented with external controls (e.g., an outside server maintained by the content holder) that determine when there is a violation and how to penalize it.[97]

What is the nature of the collected data? This is important because it determines the potential scope for which the data can be used. For example, anonymous information gives the data collector many less uses than does personalized information. Even when the data collector is a trusted entity, the nature of the data is crucial to maintain privacy.

[93] The European Community has been successful in proscribing regulations requiring data collectors to provide how their information is shared. See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data on the free movement of such data.

[94] See e.g., Privacy Online: A Report to Congress, FTC, available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[95] Cohen, supra note 94, at 586.

[96] Id.

[97] Id.

Collected data is subject to disclosure through security breaches or compelled production (i.e., subpoenas).[98]

DRM systems raise many of the same privacy concerns as other data collectors.[99] But DRM does differ significantly in the implementation of self-help mechanisms. If a user wants to use digital content protected by DRM self-help measures, she cannot opt-out of data collection since doing so frustrates content protection. Furthermore, many self-help mechanisms require particularized data about an individual and/or a computer.[100] The consumer should be made aware that identifying information is being mined. If this is only communicated in the EULA, as previously discussed, we can assume that the consumer is often oblivious.

D. Competition Issues

DRM is capable of certain market controls that can affect competition. Competition is crucial to consumer welfare in many instances.[101] DRM systems restrain access to the content within, so competition is affected when access to that content is crucial for competitors to make opposing products. This is most relevant in the context of software.

[98] Id. at 585.

[99] Data collectors such as websites also subject the consumer to a terms of service agreement to authorize data collection.

[100] This is more likely in scenarios where the DRM must keep track of the digital content, such as when content is available on a user’s hard drive.

[101] See Timothy J. Muris, The Interface of Competition and Consumer Protection (2002), available at http://www.ftc.gov/speeches/muris/021031fordham.pdf.

Also, the broad DRM licensing schemes imposed upon consumer device manufacturers can also harm competition. This section will examine both these issues.

1. Reverse Engineering

Reverse engineering is the seminal tool used to access functional content and allow a competitor to enter a market. The pre-DMCA/pre-DRM copyright version of this issue is the reverse engineering of a computer platform. This facilitates access to the computer platform so as to create working software or to create a transformative competitor of the platform itself.[102] Reverse engineering inherently involves unauthorized copying of underlying programs, which courts have termed "intermediate copying," to find the functional aspects of the computer platform.[103] Courts have characterized intermediate copying as fair use because the goal sought, the functional aspects, is unprotected by copyright. Not permitting intermediate copying would be a de facto protection of the functional aspects of the program, something left to patent law.

With the passing of the DMCA, many content holders thought they had new tools to combat reverse engineering. DRM technology can greatly hinder reverse engineering efforts by making such efforts even more time-consuming, but more burdensome still is the possible legal repercussions for circumventing the DRM technology.[104] However, some courts have continued the spirit of the pre-DMCA reverse engineering cases. In

[102] See, generally, *Sega Enterprises Ltd. v. Accolade Inc., 977 F.2d 1510 (9th Cir. 1992)*; *Sony Computer Entertainment Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000).*

[103] See id at 602-603.

[104] See *17 U.S.C. 1201*(a).

Chamberlain v. Skylink,[105] the Federal Circuit rejected the Chamberlain's claim that Skylink's garage-door transmitting device infringed the DMCA by being operational with the Chamberlain's automatic garage door. Chamberlain's garage door had been engineered with a "rolling code" that changed the code for the garage door on each use. This helped prevent potential intruders from intercepting the garage door code when used by the consumer.[106] Skylink had reverse engineered this system to create its own garage door remote, and by doing so Chamberlain claimed that it had violated the DMCA anti-circumvention provisions. The court made some insightful rulings into interpreting the DMCA, but most important for our purposes the court stated that the anti-circumventing provisions "did not create a new property right for copyright owners."[107] Thus content holders could not rely on the DMCA to enforce private protection measures for property rights not granted by the Copyright Act.[108] This reasoning is supportive of permitting new entrants into a technology market platform.

However, software protected by DRM is supplemented by a EULA which will typically require a repudiation of any right to reverse engineer. In *Davidson*,[109] the court upheld a EULA and held that defendants had agreed to give up any ambitions of reverse

[105] Supra note 54.

[106] Id. at 1183-84.

[107] Id.

[108] See also *Lexmark,* supra note 54. In *Lexmark,* plaintiff Lexmark used a mechanism in its printers that would perform a "handshake" with Lexmark's toner cartridges to ensure that only Lexmark toner cartridges were being used.[1] Defendant Static Control Components (SCC) developed toner cartridges that mimicked the handshake functions of the Lexmark toner cartridges and used, verbatim, a small sequence of copyrighted code. The court found that Lexmark's code was not copyrightable, and that Lexmark's "handshake" sequence did not qualify for § 1201 anti-circumvention protection. The "handshake" was not an adequate security device to qualify under § 1201.

[109] Supra, note 26.

engineering the plaintiff's game server. This ruling could chill competition because it suggests that no one would be permitted to reverse engineer any technology containing a EULA with an anti-reverse engineering clause. The content holder is unlikely to ever be interested in permitting reverse engineering in any available works because it would enable competition.

In sum, the language of the DMCA is not so draconian that courts apply a *per se* rule to circumvention of DRM technology. But the use of contract law to forbid reverse engineering is likely to encourage a competitive environment.

2. DRM Licensing Schemes

Many DRM systems incorporate the use of technology that is licensed to consumer device manufacturers. These licenses enable the manufacturers to create DRM-compatible devices under the auspices of specifications made or suggested by content-holding industry.[110] Device manufacturers are forced to enter into these agreements if they want content to be available for their product.[111] The technology is licensed by the developers of the protection technology or by a designated licensing authority that administers the licenses on behalf of a content industry.[112]

These licenses typically require a licensee for one DRM technology component to incorporate other DRM components. For example, a device manufacturer that wants to

[110] See Bechtold, supra note 6, at 367.

[111] Id.

[112] Id.

enable its product to use CSS[113] to play DVDs must also agree to use regional code management technology, only transmit analog video in a copy protected format, and disable digital transmissions to devices without copy protection technologies.[114] Antitrust claims relating to tying,[115] however, are probably premature or already failing. First, it is questionable whether the licenses curb horizontal competition among the manufacturers in a significant way.[116] Manufacturers are restrained in how they can compete in accessing protected content and how they can channel that content, but they are still free to compete over price, design, size, reliability, warranty, or other means.[117] Second, technology licenses have many antitrust exceptions that apply when efficiencies can be

[113] CSS stands for Content Scramble System. It provides a mechanism for encrypting/decrypting video on DVDs.

[114] See Bechtold, supra note 6, at 348. Reflecting upon the development of the DVD player device since the introduction of its DRM protection CSS in 1996 suggests that it has remained relatively unchanged. This is a large contrast with other non-DRM devices, such as the personal computer.

[115] Tying is the practice of making the sale of one product conditional upon the purchase of a different product. See *Eastman Kodak Co. v. Image Technical Services, Inc., 112 S. Ct. 2072 (1992); Northern Pacific Ry v. United States, 356 U.S. 1 (1958); International Salt Co. v. United States, 332 U.S. 392 (1947)* (ruling that it is illegal under the Sherman Act to tie a product that the seller has a legal monopoly with a product that the seller has no legal monopoly).

[116] Competition analysis for licensor-licensee agreements is conducted from a horizontal perspective. See Antitrust Guidelines for the Licensing of Intellectual Property (Antitrust Guidelines), *4 Trade Reg. Rep. P 13132*, § 4.1.1 (Apr. 4, 1995), available at http://www.usdoj.gov/atr/public/guidelines/0558.htm. It is also possible to critique the horizontal effects between the content holders (licensors). However, this may fail since the use of DRM provides a new competitive attribute to the market; content providers can now compete over whether their product is protected by DRM or not.

[117] The most interesting advance in DVD player technology was probably the introduction of filtering technology, created by a company called ClearPlay and made available on certain RCA players. ClearPlay’s movie critics went through hundreds of movies and noted scenes that might be deemed inappropriate. That information is embedded on the player’s firmware, and the player automatically filters out any portions of a movie that match its database. The Motion Picture Association of America filed suit against ClearPlay in 2004 for copyright and trademark infringement, but the case was considered moot after Congress passed the Family Entertainment and Copyright Act, which explicitly protected such filtering technology. See Ted Bridis, Congress OKs bill to strip DVD Movie Smut, Associated Press, April 20, 2005, available at http://www.usatoday.com/tech/news/techpolicy/2005-04-20-dvd-censor-bill-passes_x.htm?csp=34 (November 30, 2006).

found.[118] The Federal Trade Commission approaches technology licensing with a different understanding, recognizing that technology licensing generates efficiencies that may not be present in the licensing schemes of other industries.[119]

The current antitrust framework may not provide much in the way of recourse for technology licensing and tying. Historically, many technological innovations have involved the bundling of different technologies and the courts have deferred to innovators concerning the design of their product.[120]

E. Concluding Thoughts on the Digital Content Marketplace and the Consumer

The reality of the situation is that the content holders tend to have an unfair advantage over consumers and are not necessarily accountable for the frustrations imposed by their DRM systems. When a consumer activity is blocked or otherwise hindered, it is often unclear who is responsible.[121] Even if a consumer finds the DRM incorporated with content to be unacceptable, returning the content is often troublesome because some packaging seal has been breached, the license agreements states otherwise, or the

[118] See Antitrust Guidelines, supra note 115, at § 5.3.

[119] Id.

[120] See e.g., *United States v. Microsoft Corp., 346 U.S.App.D.C. 330 (Fed. Cir. 2001)* (recognizing that the tying of an Internet browser with an operating system was not an unlawful tie per se and that such design decisions could result in efficiencies for consumers)*; Transamerica Computer Co. v. IBM Corp., 698 F.2d 1377 (9th Cir. 1983)* (holding that IBM's design changes which made the plaintiff's devices incompatible were not unlawful)*; Digital Equip. Corp. v. Uniq Digital Techs., Inc., 73 F.3d 756, 761 (7th Cir. 1996)* (holding that the bundling of an operating system with an computer did not constitute unlawful tying) *Peripherals Leasing Corp. v. IBM Corp., 448 F. Supp. 228 (N.D. Cal. 1978)* (holding that the combining of disk and head/disk assembly was not unlawful per se)*, aff'd per curiam sub. nom. Memorex Corp. v. IBM Corp., 636 F.2d 1188 (9th Cir. 1980).*

[121] See Grimmelmann, supra note 73, at 1754.

consumer discovered the DRM restraint too late. Furthermore, the average consumer is going to be ignorant of the effect of anti-reverse engineering clauses, so by and large the consumer would be unlikely to consider it in her cost-analysis of the purchase even if the EULA was read.

III. REFINEMENTS TO THE CURRENT LEGAL FRAMEWORK

I propose addressing the digital content market deficiencies in two general ways: digital content transactions should be more transparent and the doctrine of copyright misuse should emerge to protect reverse engineering.

A. Making the Market More Transparent

Digital content holders do not usually communicate the nature of the transaction in such a way as to make it transparent that the consumer will be restricted by a DRM system. While the use of standard form contracts is probably essential when digital content is distributed via mass market mechanisms, a transparent transaction can help make up for the loss of consumer bargaining power that these contracts present. However, the nature of computerized transactions can make complete transparency difficult to achieve.[122] A prudent policy should take this into account to encourage consumer awareness of DRM restrictions.

[122] See infra Part II.A.

I propose that license agreements should walk, talk and act like license agreements. We know that digital content is almost universally licensed. Yet the operative word leading up to a transaction always suggests a sale of ownership. Apple's iTunes Music Store provides a button titled "Buy Now" next to each song. Software, in boxed form or available for download over the Internet, often entices the consumer to "buy" or "purchase."[123] Consumers will not equate "buy" with "buy a license agreement." The words "buy," "purchase," or "place order" are understood to confer a transfer of ownership in nearly every other context the consumer sees it.[124]

The overwhelming use of these operative words in conjunction with end-user licensing may be part of the reason that EULAs are so often overlooked. Were content holders required to entice buyers with a phrase like "License Now," the consumer may be better prepared and more willing to confront the EULA agreement responsibly.

Perhaps the greatest benefit lies in creating a market for digital goods to be sold for ownership. Consumers may be drawn to content holders that offer ownership in the place of licensing, allowing them to avoid the frustrations of DRM. Businesses are already considering these distribution models after considering the cost-effectiveness of using DRM.[125] Making license sales present themselves as actual licenses allows

[123] Purchases of digital content made in the "physical world" are little different from any other kind of purchase, except that a software box may have a small inscription stating that the purchase is subject to a license that is inside the box. See, e.g., *ProCD*, supra note 63, at 1450. Purchases for software in online stores make no mention of a license agreement, using instead a shopping cart model. At Amazon.com, consumers add items to a virtual shopping cart. When finished shopping, the consumer clicks the "Proceed to Checkout" button, and, after filling in credit card information, clicks a button titled "Place your Order."

[124] As a non-exhaustive list, leases for cars, living spaces, and furniture do ask the consumer to "buy."

[125] Sony BMG and Yahoo! are experimenting with DRM-free music. See US Yahoo Offer Copy-Free Music, BBC News, July 21, 2006, available at http://news.bbc.co.uk/2/hi/technology/5203146.stm (Jan 11, 2007). Steve Jobs of Apple has also stated his desire to move iTunes music to a less constrained

consumers to better distinguish the two, giving a boost to those companies selling DRM-free content.

Alternatively, the content holder would also be able to sell the content for ownership but still enable DRM. The sale of DVDs is an existing example of this, usually including a reservation of the content holder's rights.[126] This gets tricky when DRM-protected content is downloaded directly onto a personal computer. The consumer's ability to make a second sale becomes stunted.[127] The only way to sell the item may be to sell it along with the hard drive or circumvent the DRM and transfer it afterward.[128] This is not a favorable model, so ownership of DRM protected content may need a different approach.

B. Applying Copyright Misuse

DRM hinders the contribution reverse engineering gives to the technology marketplace. The Copyright Act permits technological circumventions for purposes of reverse engineering in § 1201(f). However, the license agreements in DRM systems typically

DRM-environment. See David DeJean, "Steve Jobs On DRM-Free Media: Right Idea, Whatever His Reasons," available at http://www.informationweek.com/blog/main/archives/2007/02/steve_jobs_on_d.html.

[126] General terms of these reservations include where the product is permitted to be sold and that it be used for private use only. "All other rights reserved."

[127] It would be unlawful for a content holder to restrict a consumer's second sale right without the use of a license agreement. See *17 U.S.C. 109*.

[128] Note that the consumer would be able to use circumvention tools because § 1201 does not apply to a consumer circumventing her own copy.

forbid this, and courts have upheld these provisions.[129] The fate of reverse engineering may be dependant on copyright misuse reaching full fruition.

The doctrine of copyright misuse has not been universally accepted. The United States Supreme Court has nominally recognized it,[130] and only a handful of lower court decisions exist that address it. Copyright misuse is an equitable doctrine that prevents a content holder from succeeding on a claim while she has “unclean hands.” Copyright misuse combines policy-based and market-based principles to coordinate copyright, patent, and antitrust law.[131]

There are some persuasive federal appeals cases that set the foundations for copyright misuse. In *Lasercomb Am., Inc. v. Reynolds*,[132] Lasercomb had licensed out its software that allowed the design and direction of manufacturing systems. The standard license agreement provided that the licensee could not create or sell software of this type.[133] A particular licensee copied the program for its own internal use and began selling a program that was nearly identical to Lasercomb’s. The Fourth Circuit found that “Lasercomb’s anticompetitive clauses in its standard licensing agreement constitute misuse of copyright.”[134] The Court clarified by stating there would be a finding of copyright misuse when a copyright holder uses a copyright “to control competition in an

[129] See *Davidson and Associates*, supra note 23.

[130] *Morton Salt Co. v. G.S. Suppiger, 314 U.S. 488 (1942), at 494.*

[131] See Frischmann & Moyan, The Evolving Common Law Doctrine of Copyright Misuse: A Unified Theory and Its Application to Software, *15 Berkeley Tech. L.J. 865 (2000),* 872-877.

[132] *911 F.2d 970 (4th Cir. 1990).*

[133] *Id.* at 973.

[134] *Id.* at 979.

area outside the copyright… regardless of whether such conduct amounts to an antitrust violation."[135] In *Alcatel USA, Inc. v. DGI Techs. Inc.*,[136] the Fifth Circuit found copyright misuse where a licensor (DSC) of copyrighted operating system software for switching equipment required that its licensees only use the software in "conjunction with DSC-manufactured equipment."[137] The defendant, DGI Technologies, Inc., (DGI) made a card that was interoperable with the plaintiff's operating system and was sued for copyright infringement.[138] A finding of copyright misuse was found with DSC was using its copyrighted operating system to gain control over switch components which were neither copyrighted nor patented.[139] Copyright misuse is typically applied when copyright license agreements tie in a different product. The key notion here is that while antitrust principles are applicable, the copyright holder's activity need not be unlawful.[140] It only need be improper.

Copyright misuse is an ideal judicial tool to ensure that copyright is not used to protect functional innovations. DRM reverse engineering issues are nearly identical to those raised in the above copyright misuse cases. In both situations, a content holder uses a license agreement as an instrument to protect the functional elements of the copyrighted work. This exacerbates the internal conflict of granting copyright protections to software

[135] *Id.*

[136] *166 F.3d 772 (5th Cir. 1999).*

[137] *Id. at 777.*

[138] DGI was also sued for trade secret violations, which the Fifth Circuit upheld. *Id.*

[139] *Id. at 793.*

[140] But see *Saturday Evening Post Co. v. Rumbleseat Press, Inc., 816 F.2d 1191, 1200 (7th Cir. 1987)* (where Judge Posner comments that copyright misuse should be analyzed under antitrust principles).

in the first place: using the copyright protections granted to software's expressive elements to protect the software's functional aspects.[141] It is important for the judiciary to ensure that functionality and expression are not jointly protected under copyright law.

However, copyright misuse is far from solidified. If one takes to giving greater weight to antitrust principles, a finding of misuse becomes more difficult because courts are less inclined to give content holders market power, a prerequisite for a finding of an antitrust violation.[142] For this reason I would advocate a less-strict adherence to antitrust principles when applying copyright misuse and a greater emphasis on the function-expression dichotomy.

IV. CONCLUSION

DRM systems enable content holders to create and maintain their own copyright regulations. As of today, DRM protections usually serve as an annoyance or frustration. Tomorrow it is possible that DRM will give content holders complete control over downstream consumption of their works. But this does not doom the consumer. We know that DRM burdens consumers in significant ways, but it is important to note that it also burdens content holders. Increased DRM protections will probably mean that the content holder must have greater infrastructure, more internal maintenance, and more technical support. And if the economic burdens on the content holder do not limit her use of DRM, there must surely be a limit to the extent of DRM-related hurdles that the consumer will

[141] See Grimmelmann, supra note 73, at 910-913.

[142] See Act of Nov. 19, 1988, Pub. L. No. 100-703, tit. II, 20, 102 Stat. 4676 (codified as amended at 35 U.S.C 271(d)(5)(1994)).

tolerate before interest in a product wanes. We will likely soon reach some kind of "DRM-threshold" for each kind of content medium.

The way to ensure that the DRM threshold is "fair" is to encourage competition between similar products with varying degrees of DRM protection. In places where high-consumer demand exists, such as time shifting and space shifting, we already see compromises being made to accommodate both content holders and consumers. Where there is no straightforward consumer demand, it is prudent policy to ensure that the market remains competitive and that other consumer and social interests, such as reverse engineering, remain intact.