REALNETWORKS, INC. V. STREAMBOX, INC. & UNIVERSAL CITY STUDIOS, INC. V. REIMERDES

By Eddan Elizafon Katz

The encoding of any type of expression in digital form preserves perfect quality in every subsequent copy, even when duplicated and distributed many times. When content is stored in digital form, technological barriers have to be imposed in order to create an artificial scarcity that would prevent the otherwise unobstructed propagation of information and art.[1] The copyright industries—music, film, television, and publishing—perceive the Internet and digital technology in general as a threat to their exclusive right to distribute and make copies of the copyrighted works they own. As a precondition for the release of their copyrighted works onto the Internet, these companies insist on a legal framework that supports the technological protection systems they have developed. Information technology companies, educational institutions, and consumer advocates are concerned that the implementation of these technological protection systems may result in an imbalance between the protections afforded to copyright owners and society's access to information. They argue for a flexible legal framework that encourages access to information implied by the open infrastructure of the Internet.

The Digital Millennium Copyright Act of 1998 ("DMCA")[2] sought to balance these interests. The anti-circumvention provisions in section 1201 of the DMCA prohibit the access and duplication of copyrighted works through circumvention of technological protections imposed by the copyright owner. *RealNetworks, Inc. v. Streambox, Inc.*[3] and *Universal City Studios, Inc. v. Reimerdes*[4] are the first cases to test these anti-circumvention provisions. Both raise urgent questions regarding legitimate uses of technology permitted to innovators, researchers, and the general public. The rulings in both district courts broadly interpreted the ban on circumvention and narrowly applied the various exemptions and limitations within the statute. The unfortunate result of these rulings may be the establishment of an asymmetrical copyright system that grants unchecked

[1] *See generally* John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, *available at* http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html.

[2] 17 U.S.C. § 1201 (Supp. IV 1998).

[3] No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

[4] 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

authority over the use of digital works to copyright owners. The cases demonstrate that such a strict understanding of the DMCA may lead to overprotection for copyright owners at the expense of public access to art and information.

I. BACKGROUND

A. DMCA Anti-circumvention Provisions

The DMCA contains three main provisions: (1) an act-of-circumvention ban;[5] (2) an access control circumvention device ban (sometimes called the "trafficking" ban);[6] and (3) a copyright protection circumvention device ban.[7] The first provision prohibits the *act* of circumventing technological protection systems, while the other two ban technological *devices* that facilitate the circumvention of access control or protection of the rights of the copyright owner. The three provisions are also distinguishable in that the first two provisions focus on technological protections that provide access control to the copyright owner, while the third provision prohibits circumvention of technological protections against unauthorized duplication and other copyright infringing activities.[8]

The act-of-circumvention behavior ban in section 1201(a)(1)(A) prohibits "circumvent[ing] a technological measure that effectively controls access to a work."[9] According to the statute, "to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[10] A technological protection that effectively controls access to a work is a measure which "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[11]

The second provision mandates that "[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" that is primarily used

[5] 17 U.S.C. § 1201(a)(1)(A) (Supp. IV 1998).

[6] *Id.* § 1201(a)(2).

[7] *Id.* § 1201(b).

[8] *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 690-91 (2000); *see also supra* notes 5-7.

[9] 17 U.S.C. § 1201(a)(1)(A) (Supp. IV 1998).

[10] *Id.* § 1201(a)(3)(A).

[11] *Id.* § 1201(a)(3)(B).

for circumvention.[12] Congress intended this provision to be analogous to existing laws prohibiting the manufacture or distribution of "black boxes" whose function is to descramble cable television and satellite cable services.[13] What constitutes "trafficking" is defined by three clauses prohibiting circumvention devices that (1) are "primarily designed . . . for the purpose of circumventing," (2) have "only limited commercially significant purpose or use other than to circumvent," or (3) are marketed for use in circumventing a technological measure."[14] As with the act-of-circumvention ban, this provision prohibits accessing a copyrighted work without authorization but does not regulate the activity of users once they have access.[15]

The third provision prohibits "circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner."[16] This provision regulates devices that enable copyright protection to be circumvented, whether or not gaining access was necessary or required authorization of the copyright owner. In contrast with the other provisions, the copyright protection circumvention device ban has no equivalent provision for circumvention activity in section 1201 of the DMCA. Rather, the provision serves as a buttress to the already prohibited uses of a work, extensively covered by traditional copyright law, once it is lawfully accessed.[17]

B. Exemptions and Limitations in Section 1201

In response to the warnings from information technology industry advocates that strict anti-circumvention controls would damage innovation and competition in the burgeoning digital economy, Congress included several explicit limitations to the three anti-circumvention provisions.[18]

One important limitation is the reverse engineering exemption,[19] which is most relevant to the development of software products. This exemption contains three significant subsections. The first subsection allows programmers to circumvent a technological measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer pro-

[12] *Id.* § 1201(a)(2).

[13] *See* H.R. REP. NO. 105-551, pt. 2, at 38 n.2 (1998).

[14] 17 U.S.C. §§ 1201(a)(2)(A)-(C) (Supp. IV 1998).

[15] Nimmer, *supra* note 8, at 686.

[16] 17 U.S.C. § 1201(b)(1)(A) (Supp. IV 1998).

[17] Nimmer, *supra* note 8, at 691.

[18] *See* H.R. REP. NO. 105-551, pt.2, at 25-26 (1998).

[19] 17 U.S.C. § 1201(f) (Supp. IV 1998).

gram."[20] The other two subsections allow the development of circumvention devices "for the purpose of enabling interoperability of an independently created computer program with other programs."[21] The third subsection takes into account the collaborative work involved in reverse engineering by exempting engineers from the "trafficking ban" if they permit the device to be made available to other persons for the purpose of interoperability, and not for gaining access to protected works for infringing purposes.[22]

The most controversial limitation attempts to preserve the defenses traditionally available under copyright law, including fair use.[23] It is unclear from the language of the provision whether or not fair use defenses can be applied to liability under the anti-circumvention provisions.[24]

Congress also recognized that the market behavior of copyright owners on the Internet, bolstered by a flat prohibition against circumvention of technological protection measures, could unduly hinder the public's access to information.[25] In order to alleviate these concerns, Congress established a two year delay for the act-of-circumvention ban after the enactment of the DMCA. This left open the possibility of incorporating any findings of the Copyright Office on the subject of noninfringing uses of circumvention.[26] After hearings, comments, and statements from diverse groups (including parties involved in *RealNetworks* and *Universal*),[27] the Copyright Office issued its Final Rule with two narrow exemptions, neither of which would have affected the outcome of either case.[28]

[20] *Id.* § 1201(f)(1).

[21] *Id.* § 1201(f)(2).

[22] *Id.* § 1201(f)(3).

[23] *Id.* § 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use.").

[24] *See infra* text accompanying notes 51, 105-07.

[25] H.R. REP. NO. 105-551, pt.2, at 36 (1998).

[26] *Id.*

[27] *See* U.S. Copyright Office, Statements from Anticircumvention Hearings, *at* http://www.loc.gov/copyright/1201/hearings/index.html (last visited Feb 7, 2001) (listing participants and providing links to testimony).

[28] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201). The first exemption is for compilations of lists of websites blocked by filtering software. The second exempts literary works protected by access control mechanisms that are broken.

II. CASE SUMMARIES

A. *RealNetworks, Inc. v. Streambox, Inc.*

The RealNetworks "RealPlayer" is a software application predominantly used to access "on demand" audio and video content over the Internet.[29] Through a "streaming" method of broadcast, the audiovisual information from originating servers can be viewed and listened to on an end-user's computer without transferring the file.[30] Once the content is encoded in the "RealMedia" format, it can be hosted on any web server and contains security measures that prevent the downloading of the file onto the end-user's computer.[31] This protection against copying is achieved by first using a "secret handshake" that authenticates the destination of the file as a RealPlayer, then activating a "copy switch" that prevents the download of the streamed content. If the content owner chooses to employ the copy switch with the streaming broadcast, the data will "evaporate" from the user's computer once it finishes playing.[32]

Streambox made a suite of software products that facilitated different uses of content transmitted from RealServers. The Streambox "VCR" allows end-users to download RealMedia files by mimicking the authentication procedure of the secret handshake and then ignoring the copy switch.[33] Rather than only accessing the streamed content while connected to a RealServer, the Streambox VCR allows end-users to download the RealMedia files and store them on their computers.[34] The Streambox "Ripper" allows files to be converted from the RealMedia format to other music or video file formats utilized by other software programs.[35] The Streambox "Ferret" is a plug-in application that allows the end-user to switch from the default search engine of RealMedia to a search engine operated by Streambox.[36]

RealNetworks brought suit against Streambox to enjoin Streambox's suite of products on the ground that they violated the trafficking provision in section 1201(b).[37] RealNetworks also alleged contributory copyright

[29] *See* RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889, at *5 (W.D. Wash. Jan. 18, 2000).

[30] *Id.* at *4-5.

[31] *Id.* at *5-6.

[32] *Id.* at *6.

[33] *Id.* at *10-11.

[34] *Id.* at *10-11.

[35] *Id.* at *14.

[36] *Id.* at *15.

[37] Complaint for Violation of The Digital Millenium Copyright Act, Contributory, Vicarious and Direct Copyright Infringement, Tortious Interference with Contract, and

infringement and interference with contract.[38] RealNetworks claimed that the Streambox VCR circumvented both security features of the RealPlayer upon which content owners rely for protection against the unauthorized duplication and distribution of their copyrighted works,[39] thereby violating both the access control and copyright protection circumvention device provisions of the DMCA. RealNetworks also claimed that the Streambox Ripper facilitated copyright infringement by creating "unauthorized derivatives" of copyrighted works in formats other than RealMedia files.[40] Finally, RealNetworks claimed that the Ferret's addition of the Streambox search engine threatened the exclusive licensing relationship between RealNetworks and Snap, the provider of RealNetworks' search engine.[41]

The District Court for the Western District of Washington issued a preliminary injunction against the Streambox VCR and Ferret and denied injunctive relief against the Streambox Ripper.[42] The court held that the Streambox VCR (1) circumvents an access control measure by mimicking the secret handshake to gain access to the RealMedia files and (2) circumvents a copy protection measure by ignoring the copy switch.[43] The Streambox Ferret was enjoined on a theory of contributory copyright infringement due to its altering of the user interface of the RealPlayer.[44] Finally, the court found that the Streambox Ripper did not violate the DMCA because the conversion feature was distinct from copying and, in fact, potentially served beneficial uses for the copyright owner.[45]

RealNetworks emphasized two concerns. First, content owners would lose significant advertising revenue from decreased website traffic as a result of users viewing their downloaded copies rather than streaming the content from the copyright owner's website each time they wanted to view it.[46] Second, the downloaded files would be easy fodder for piracy. As the court observed, "[o]nce an unauthorized, digital copy of a RealMedia file is created it can be redistributed to others at the touch of a button."[47]

Lanham Act Violations at ¶¶ 31-46, *RealNetworks* (No. C99-2070P), *available at* http://www.realnetworks.com/company/pressroom/pr/99/rnwk_complaint.html.

[38] *Id.* at ¶¶ 47-60.

[39] *RealNetworks*, 2000 U.S. Dist. LEXIS 1889 at *7.

[40] *See id.* at *27-29.

[41] *See id.* at *33-34.

[42] *Id.* at *2-3.

[43] *See id.* at *18-19.

[44] *See id.* at *33. Since the claim was not brought under the anti-circumvention provisions, this Note will not discuss the court's analysis of the Ferret.

[45] *Id.* at *27-30.

[46] *Id.* at *7-8.

[47] *Id.* at *13.

Streambox argued that there were substantial noninfringing uses of the Streambox products, analogizing to the foundational fair use case of *Sony Corporation of America v. Universal City Studios, Inc.*[48] The court, however, held that the *Sony* doctrine did not apply to the circumvention device bans of section 1201 of the DMCA.[49] The court reasoned that the user's conduct was irrelevant to the circumvention device ban, since "Congress specifically prohibited the distribution of the tools by which such circumvention could be accomplished."[50] The court cited *Nimmer on Copyright* for the proposition that manufacturers of consumer products with substantial noninfringing uses that would otherwise immunize them from liability under the *Sony* doctrine are nonetheless subject to prohibition by section 1201.[51]

Streambox also asserted that it was not required to manufacture its VCR with features responding to the copy switch because of the no-mandate provision of the DMCA.[52] The court did not rule on the validity of this defense, concluding instead that the circumvention of the secret handshake access control measure was sufficient to warrant the injunction against the Streambox VCR.

B. Universal City Studios, Inc. v. Reimerdes

The prospect of unauthorized parties distributing motion pictures in digital format for sale on the home market led the movie studios to develop an encryption system for Digital Video Disks ("DVDs") that would prevent the piracy of their movies.[53] Though DVDs allow movies to be presented in a higher quality and longer-lasting format than videotape, the movie studios, who collectively own a large fraction of all copyrighted motion pictures, were concerned that DVDs also facilitate making limitless copies of movies without a reduction in quality.[54] CSS, or Content Scrambling System, is an encryption-based system that embeds the digital sound and graphics files on a DVD in an encryption algorithm.[55] A DVD

[48] 464 U.S. 417 (1984) (holding that the private home viewing of TV programs on copies made by videotape recorders is considered "fair use" and that manufacturers of those recorders cannot not be held liable for vicarious or contributory infringement).

[49] *RealNetworks*, 2000 U.S. Dist. LEXIS 1889 at *22.

[50] *Id.* .

[51] *Id.* (citing 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §12A.18[B] (1999 Supp.)).

[52] *Id.* at *24-25.

[53] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d. 294, 309-10 (S.D.N.Y. 2000).

[54] *Id.* at 309.

[55] *Id.* at 309-10.

that contains CSS "can be decrypted by an appropriate decryption algorithm that employs a series of keys stored on the DVD and the DVD player."[56] The DVD Copy Control Association ("DVD-CCA"), a group made up of consumer electronics manufacturers and movie studios, licenses the technology that contains the key to decrypt CSS so that the content can be viewed.[57]

Jon Johansen, a Norwegian teenager, reverse-engineered a licensed DVD player, discovered the CSS encryption algorithm, and developed a program that was capable of performing the decryption.[58] He then posted the program, named DeCSS, on his website, and informed software developers for Linux, who needed the decryption of CSS for the development of a Linux-compatible DVD player.[59]

In late 1999, defendant Eric Corley, who publishes the magazine *2600: A Hacker Quarterly*, posted the source and object code of DeCSS on the 2600.com website as part of a story on the hacking of the DVD encryption system.[60] In addition to making DeCSS available for download, 2600.com included links to other locations on the Internet where DeCSS was available.[61] Upon learning of the existence of DeCSS, the major movie studios[62] sent cease and desist letters to website operators that had the program on their website and eventually filed suit against 2600 Enterprises and two other defendants.[63] Since Eric Corley was not the actual developer of DeCSS and since there was no act of circumvention involved in posting or linking to the code, the movie studios filed a motion for a preliminary injunction charging that making the program available for download was in violation of the "trafficking" ban on circumvention devices.[64] The U.S. District Court for Southern District of New York granted the injunction

[56] *Id.* at 310.

[57] *Id.* at 310 & nn.60 & 63.

[58] *Id.* at 311. Jon Johansen worked on the project with two other unnamed individuals.

[59] *Id.* Johansen posted the program to the LiViD mailing list, an Internet community of software developers working on creating a Linux DVD player.

[60] *Id.* at 308-09.

[61] *Id.* at 312.

[62] Universal City Studios, Inc.; Paramount Pictures Corp.; Metro-Goldwyn-Mayer Studios Inc.; TriStar Pictures, Inc.; Columbia Pictures Industries, Inc.; Time Warner Entertainment Co.; Disney Enterprises, Inc.; and Twentieth Century Fox Film Corp.

[63] *Universal*, 111 F. Supp. 2d. at 309-10.

[64] Complaint for Violation of Provisions Governing Circumvention of Copyright Protection Systems, 17 U.S.C. §§ 1201 et seq., *Universal* (No. 00 Civ. 0277 (LAK)), *available at* http://www.eff.org/IP/MPAA_DVD_cases/20000114_ny_mpaa_complaint.html.

and barred the defendants from posting DeCSS.[65] While all three defendants removed the DeCSS program and source code from the their websites, Eric Corley continued to maintain a list of over 500 external links to locations where DeCSS was available on the Internet as an act of "electronic civil disobedience."[66] The movie studios subsequently amended their complaint seeking to expand the preliminary injunction to include linking to websites which contained DeCSS.[67]

Due to the decrypting function of DeCSS, the court held that DeCSS was clearly "a means of circumventing a technological access control measure."[68] The court explained that DeCSS was prohibited under the statute since "[o]ne cannot lawfully gain access to the keys [embedded in CSS] except by entering into a license with the DVD-CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license."[69] The court then noted that offering DeCSS on the 2600.com website therefore violated the trafficking ban of the anti-circumvention provisions unless one of the "statutory exceptions applie[d] to their actions."[70]

The movie studios argued that their copyrighted works were vulnerable to piracy over the Internet as long as DeCSS was readily available and that Eric Corley was encouraging the theft of their intellectual property. Defendants argued that DeCSS was not designed to facilitate piracy, but rather was created as part of a project to develop a DVD player for Linux.[71] However, the court held that "whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants . . . violated the anti-trafficking provision of the DMCA."[72] The court interpreted the anti-trafficking provision as indifferent to the actual use of the technology or the context in which it developed, concluding that whether 2600 Enterprises made DeCSS available "in order to infringe, or to permit or encourage others to infringe, copyrighted works . . . simply does not matter for purposes of Section 1201(a)(2)."[73] The fact that DeCSS circumvented the protection measure in DVDs, reasoned the court, was sufficient for violation of the anti-

[65] *Universal*, 111 F. Supp. 2d. at 312.
[66] *Id.* at 312-13.
[67] *Id.* at 324.
[68] *Id.* at 317.
[69] *Id.* at 317-18.
[70] *Id.* at 317.
[71] *Id.* at 319.
[72] *Id.*
[73] *Id.*

trafficking provision, "except to whatever extent motive may be germane to determining whether their conduct falls within one of the statutory exceptions."[74] The court noted that defendants' claim that DeCSS was created as part of an effort to create a Linux DVD player was not credible since they were aware of the program's utility in facilitating the copying of movies.[75]

The defendants further argued that embedding CSS in DVDs prevented some of the legitimate uses that one can make of a DVD.[76] The court acknowledged that "technological means of controlling access to works create a risk, depending upon future technological and commercial developments, of limiting access to works that are not protected by copyright."[77] The court concluded that Congress considered this impact and decided nonetheless that protection of copyright against device circumvention trumped "fair use."[78] The inclusion of statutory exemptions and the Copyright Office's rulemaking proceedings on exempted classes of works circumscribe the legitimate uses that can be made of works protected by technological measures.[79]

Defendants also defended their actions under the reverse engineering exemption in section 1201(f) since "DeCSS is necessary to achieve interoperability between computers running the Linux operating system and DVDs."[80] The court dismissed this claim as irrelevant because Eric Corley was not the person who reverse-engineered the DVD player.[81] Even if Corley had originally obtained the information, the court reasoned that the exemption does not allow for the public dissemination of a software developer's work, but rather permits him only to share that information with individuals collaborating on the interoperability project.[82]

[74] *Id.*

[75] *Id.* at 320.

[76] *See id.* at 322 (using the example of "the preparation by a film studies professor of a single CD-ROM or tape containing two scenes from different movies in order to illustrate a point in a lecture on cinematography").

[77] *Id.* at 322 n.159.

[78] *See id.* at 304.

[79] *Id.* at 323.

[80] *Id.* at 320.

[81] *Id.*

[82] *Id.*

III. DISCUSSION

A. The Priority of Public Access in the Copyright Balance

As highlighted by the Supreme Court in the *Sony v. Universal*[83] decision, "[t]he monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved."[84] The Court emphasized the appropriate prioritization of this balance of interests, declaring that Congress "has been assigned the task of defining the scope of the limited monopoly that should be granted to authors or inventors *in order to* give the public appropriate access to their work product."[85] These principles are inconsistent with the district courts' interpretation of the anti-circumvention provisions of the DMCA. Holding that legitimate noninfringing uses of the Streambox VCR and DeCSS were rendered irrelevant by the use of technological measures endangers the balance that was sought in the Copyright Clause.[86]

The anti-circumvention provisions of the DMCA reserve broad authority over access for copyright owners utilizing technological protection systems on their copyrighted works. As is evident from the statutory definitions of a "technological measure" and "circumvention" of such a measure, the boundaries of access control are the authority of the copyright owner.[87] Congress introduced these legal protections for access control systems in order to "make digital networks safe places to disseminate and exploit copyrighted material."[88] Yet, without meaningful exemptions to the anti-circumvention provisions, the limited monopoly over use of and access to copyrighted works ensured by copyright law would be transformed into absolute control by copyright owners.[89]

The district courts in *RealNetworks v. Streambox* and *Universal v. Reimerdes* were the first to interpret this structurally complex act. In both cases, the courts interpreted the various exemptions to the exclusive right to authorize access as being separate from the circumvention device ban.[90]

[83] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984).

[84] *Id.*

[85] *Id.* (emphasis added).

[86] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-circumvention Regulations Need to be Revised*, 14 BERKELEY TECH L.J. 519, 545-46 (1999).

[87] 17 U.S.C. § 1201(a)(1), (3) (Supp. IV 1998); *see also supra* text accompanying notes 10-11.

[88] S. REP. NO. 105-190, at 2 (1998).

[89] Nimmer, *supra* note 8, at 720-21.

[90] *See supra* text accompanying notes 49-52, 73-75, 77-78.

Disconnecting inquiry into the uses of circumvention from prohibitions on circumvention devices can extend a copyright owner's authority over use to cover access as well when the technological systems are designed to protect both. In light of this, Congress explained that copyright law "historically advanced th[e] constitutional objective" of the Copyright Clause of the Constitution by "regulating the use of information—not the devices or means by which the information is delivered or used by information consumers—and by ensuring an appropriate balance between the interests of copyright owners and information users."[91] Unfortunately, the potential noninfringing uses of the Streambox VCR and DeCSS were essentially ignored by the district courts.

B. Legitimate Uses of the Streambox VCR

The *Streambox* court's ruling that the *Sony* doctrine is irrelevant to the anti-circumvention prohibitions is inconsistent with the provision preserving the traditional defense of "fair use" in copyright infringement analysis.[92] As a technology that can record broadcast media and store that information on a user's local device, the Streambox VCR is the Internet equivalent of the Betamax video tape recorder. In *Sony*, the Supreme Court determined that the Betamax was capable of noninfringing uses of television broadcasts because it facilitated the "private, noncommercial time-shifting in the home."[93] The biggest difference between the legitimate uses of the Betamax and the Streambox VCR stems from the difference between broadcast television and the Internet. Since streamed programming is available on demand whenever a user is connected to the Internet, the convenience of "time-shifting" is rendered unnecessary. The convenience afforded by the Streambox VCR, as suggested in Streambox's advertising, is that Internet users can "'download RealAudio and RealMedia files as [they] . . . would any other file, then reap the benefits of clean, unclogged streams straight from [their] hard drive."[94] The majority of users do not have a fast Internet connection that is always on, and the streaming "RealMedia" clips are susceptible to skipping during times of heavy Internet traffic and can also get interrupted due to software mal-

[91] H.R. REP. NO. 105-551, pt.2, at 24 (1998).

[92] *See supra* text accompanying note 51.

[93] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

[94] RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889, at *13 (W.D. Wash. 2000).

function.[95] The Streambox VCR therefore provides the useful service of "space-shifting" the RealMedia files so that they can be viewed without the limitations of Internet connection speeds and unstable streaming transmissions.

RealNetworks insisted that the downloading of files enabled by the Streambox VCR subverts the access and copy protection features that "empower the copyright owner to determine how to distribute the content and how to obtain remuneration for it."[96] The court was persuaded by the primacy of the copyright owners' authority, distinguishing the case from *Sony* because "copyright owners have specifically chosen to prevent the copying enabled by the Streambox VCR by putting their content on RealServers and leaving the copy switch off."[97] RealNetworks argued that "by circumventing protections for copyright holders, Streambox's VCR and Ripper enable the widespread infringement of works that were not supposed to be copied or modified by end-users."[98] Regarding the legitimate uses individuals may have for the Streambox VCR, RealNetworks argued that the fair use exceptions available to defendants in copyright infringement cases do not apply to violations of the anti-circumvention provisions of the DMCA.[99]

RealNetworks responded to Streambox's claim that the VCR allows end-users to access otherwise unobtainable files by declaring that those "files are unobtainable because the content owners want it that way."[100] It is unclear whether or not the proprietary aspect of the secret handshake allows RealNetworks to have the exclusive authority for granting access to all RealMedia files. Regulating the Streambox VCR's access to RealMedia files that are in the public domain is certainly outside the authority of copyright owners.[101] For example, most audio and video clips of court-

[95] *See* RealPlayer Plus 5.0 FAQs, *available at* http://pluszone.real.com/pp5backnew.html#traffic and http://pluszone.real.com/pp5general.html#multiple (last visited Feb. 5, 2001).

[96] Plaintiff's Reply Brief in Support of Preliminary Injunction at § I(B), *RealNetworks* (No. C99-2070P) *available at* http://www.realnetworks.com/company/pressroom/pr/99/m_replybrief.html. [hereinafter RealNetworks Reply Brief].

[97] *RealNetworks*, 2000 U.S. Dist. LEXIS 1889, at *22.

[98] RealNetworks Reply Brief, supra note 96, at § III.

[99] *See id.* at § I(B).

[100] *Id.* at § I(A).

[101] *See generally* Yochai Benkler, *Free As The Air To Common Use: First Amendment Constraints On Enclosure Of The Public Domain*, 74 N.Y.U. L. REV. 354 (1999). (arguing that laws which conceive of information as an owned commodity remove uses of information from the public domain and place them under the copyright owner's exclusive control).

room proceedings or congressional hearings remain on the CSPAN website for only a few days.[102] After they are removed, users cannot have access to them without having downloaded them with the Streambox VCR. As this example shows, the exclusive right to authorize access for all works encrypted behind technical protection systems is overreaching if not limited by exemptions allowing for circumvention according to the principles of fair use.[103]

C. Fair Use Exemptions

At the heart of the debate over the interpretation of the DMCA is the survival of fair use as a defense against liability under the anti-circumvention provisions. Section 1201(c)(1) explicitly states that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use."[104] The tension over the interpretation of this exemption is whether the defenses can be applied to violations of the anti-circumvention provisions or whether they only apply in cases of copyright infringement. If the anti-circumvention prohibitions are distinct from copyright infringement, defendants can be held liable for circumventing an access control measure even if the uses made of the work are held not to infringe on the rights of the copyright owner.[105] Professor Pamela Samuelson, though, urges courts to "distinguish between circumvention aimed at getting unauthorized access to a work and circumvention aimed at making noninfringing uses of a lawfully obtained copy."[106] Professor Jane Ginsburg points out that the comma before the clause "including fair use" may indicate that fair use is applicable not only to copyright infringement claims but also to all provisions under Title 17.[107]

The *Streambox* court did not even mention section 1201(c)(1) in its decision. Rather, the court relied on *Nimmer on Copyright* to support the inapplicability of fair use to manufacturers or distributors of circumvention devices.[108] The *Universal* court also distinguished the application of

[102] *See* http://www.cspan.org (stating that "[m]ost events will remain in the archive for 15 days or less" when one searches for an old event in the Search the Program Archives feature).

[103] *See* Samuelson, *supra* note 86, at 543.

[104] 17 U.S.C. § 1201(c)(1) (Supp. IV 1998).

[105] *Cf.* Samuelson, *supra* note 86, at 539 n.108.

[106] *Id.* at 539.

[107] Jane C. Ginsburg, From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law, 15 (Public Law & Legal Theory Working Paper Group 2000), *available at* http://papers.ssrn.com/paper.taf?abstract_id=222493.

[108] *See supra* text accompanying note 51.

fair use to circumvention violations from copyright infringement claims, stating that "[i]f Congress had meant the fair use defense to apply to such actions, it would have said so."[109]

Congress did in fact establish a forum for reviewing the fair use implications of the anti-circumvention provisions in the biennial rule-making proceedings established in section 1201(a)(1)(C).[110] The statute provides that exemptions created by the rule-making process apply only to the act-of-circumvention ban and explicitly states that such exemptions may not be "used as a defense in any action to enforce any provision of this title other than this paragraph."[111] Nevertheless, in the discussion of DVDs as a possible class for exemption in the first rulemaking decision, the Copyright Office recognized that the uses of a copyrighted work are in fact implicated by the restriction of access but deferred the question back to Congress.[112] The Copyright Office noted that it "would be helpful if Congress were to clarify its intent," since Congress "did create a distinction between the conduct of circumvention of access controls and the conduct of circumvention of use controls by prohibiting the former while permitting the latter."[113] Technological protections adopted by copyright owners that merge these two types of controls "would undermine Congress' decision to offer disparate treatment for access controls and use controls."[114]

D. The Threat to Interoperability

Copyright law has traditionally allowed reverse engineering of products in the open market. Reverse engineering promotes the production of improved products and enhances competition. Of particular importance to the information technology industry is the ability to make products that are interoperable with industry standards. For example, software applications require interoperability with software platforms so they can run smoothly together.[115] In apparent accordance with this tradition, the DMCA allows

[109] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 322 (S.D.N.Y. 2000).

[110] 17 U.S.C. § 1201(a)(1)(C) (Supp. IV 1998). *See supra* text accompanying notes 25-27.

[111] 17 U.S.C. § 1201(a)(1)(E) (Supp. IV 1998).

[112] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201).

[113] *Id.*

[114] *Id.*

[115] *See* American Committee for Interoperable Systems ("ACIS"), Comments on "Intellectual Property and the National Information Infrastructure," at 2-3 (Sept. 1, 1994), *available at* http://www.interop.org/greenComments.html [hereinafter ACIS Comments].

circumvention of technological protection measures in order to achieve interoperability.[116]

Unfortunately, the DMCA's reverse engineering exemption was interpreted too narrowly by the *Universal* court. The court ruled that the manner in which Jon Johansen shared his reverse engineering results was outside the scope of legitimate collaboration and instead was a "public dissemination of means of circumvention."[117] The ruling affects the development structure of open source software, which is organized to facilitate collaborative projects within a particular community but is open to all Internet users.[118] This type of product development has been an integral element in the success of Linux in the computer industry. The further acceptance of Linux in the consumer market as a practicable operating system alternative to Windows depends on the ability of users to utilize the same mainstream applications, including the ability to view DVD movies. The court doubted the credibility of the developers of DeCSS, finding that the developers of DeCSS were aware "that DeCSS could be used to decrypt and play DVD movies on Windows as well as Linux machines."[119] The court noted that the piracy of copyrighted works was therefore facilitated by DeCSS since "the decrypted files could be copied like any other unprotected computer file."[120] Nevertheless, the court's interpretation of the reverse engineering exemption disadvantages open source software developers, whose collaborative nature does not allow for the same degree of secrecy as traditional product development.[121]

The exemption undermines its own purpose when it is interpreted so that copyright owners maintain control over the authorization to reverse-engineer beyond the point when the work is lawfully acquired. While the various provisions of section 1201(f) exempt software developers from the act-of-circumvention ban and the circumvention device ban, they do not exempt reverse engineering from violations of the copyright protection circumvention device provision.[122] Since the development of software through the use of reverse engineering necessitates the creation of an intermediate copy of the work, the programmer risks copyright infringement

[116] 17 U.S.C. § 1201(f) (Supp. IV 1998).

[117] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d. 294, 320 (S.D.N.Y. 2000).

[118] A message posted to an Internet discussion list that contains information about technological protection systems can be considered dissemination of a circumvention device since the information is potentially available to all Internet users.

[119] *Universal*, 111 F. Supp. 2d at 320.

[120] *Id.*

[121] *See supra* text accompanying note 75.

[122] Nimmer, *supra* note 8, at 701.

in the very act of reverse engineering.[123] The fact that copyright law considers backup copying a privileged activity would not be helpful to the programmer's dilemma if the work was protected behind a technological copy protection measure.[124] The reverse engineering exemption would therefore be rendered meaningless if the copyright owner employed technological measures that control both access to and use of the copyrighted work.[125] A more appropriate construction of the provisions would focus "on the uses to which those devices are put rather than the devices themselves."[126]

IV. CONCLUSION

The Digital Millennium Copyright Act marks a significant departure from copyright law's traditional focus on the infringing acts of violators to the prohibition of devices and services that facilitate circumvention. The provisions upset the balance between copyright protection and public access by assigning absolute rights to the copyright owner while creating only narrow exemptions for technology innovators, academic researchers, and the general public. In the first two cases tried under the new anti-circumvention provisions, the court's rulings exacerbated the imbalance between the protection of copyright in the digital age and the limitations on that right for the sake of public access. The fate of a thriving electronic marketplace, where consumers can enjoy their art and information in ways appropriate to their needs, now rests in the hands of higher courts.

[123] Terril Lewis, *Reverse Engineering of Software: An Assessment of the Legality of Intermediate Copying*, 20 LOY. L.A. ENT. L. REV. 561, 564 (2000).

[124] *See* Samuelson, *supra* note 86, at 550-51.

[125] *See supra* text accompanying notes 112-114.

[126] ACIS Comments, *supra* note 115, at 7.