UIC John Marshall Journal of Information Technology & Privacy Law

Volume 21
Issue 1 *Journal of Computer & Information Law - Fall 2002*

Article 1

Fall 2002

The Digital Millennium Copyright Act: A Review of the Law and the Court's Interpretation, 21 J. Marshall J. Computer & Info. L. 1 (2002)

Neil A. Benchell

ARTICLES

THE DIGITAL MILLENNIUM COPYRIGHT ACT: A REVIEW OF THE LAW AND THE COURT'S INTERPRETATION

NEIL A. BENCHELL†

I. INTRODUCTION

A. PROGRAMMER ARRESTED

On July 16, 2001, Dmitry Skylarov, a twenty six year-old Russian computer programmer, was arrested and charged with one count of conspiracy to traffic in technology designed to circumvent copyright technology and multiple counts of trafficking in circumvention technology,[1] for which he could have received twenty-five years in prison. He was arrested just as he was about to give a talk describing the weaknesses of Adobe Systems, Inc., an electronic book software.[2] Mr. Skylarov's crime was authoring a computer program that alters the restrictions a publisher may place on a file formatted for Adobe eBook reader.[3]

After eleven days in a Las Vegas jail, Mr. Skylarov was transferred in handcuffs and shackles, to a federal prison in Oklahoma and then to a facility in San Jose, California where he was given the opportunity to post a $50,000 bail.[4] He was released on August 6, 2001 but was not allowed to return to his family in Russia.[5] Five months later, Mr. Skylarov entered into an agreement with prosecutors who dropped all charges against him if he testified against his employer. In December of 2002, a federal jury acquitted Skylarov's employer of any wrongdoing.[6]

---

† After an eighteen-year career in the computer technology field, Mr. Benchell now practices law in the areas of intellectual property and technology law. Special thanks are due to Dr. Jill Weissberg-Benchell, PhD., for her guidance, patience, editing and encouragement.

1. *U.S. v. Elcom Ltd.*, Indictment, No. CR 01-20138 (N.D. Ca. 2001).
2. Lawrence Lessig, *Jail Time in the Digital Age*, N.Y. Times A17 (July 30, 2001).
3. *Id.*
4. Steven Levy, *Busted by the Copyright Cops*, Newsweek 54 (Aug. 20, 2001).
5. *Id.*
6. Matt Richtel, *Russian Company Cleared of Illegal Software Sales*, N.Y. Times C4 (Dec. 18, 2002).

B. Princeton University Professor Threatened Not to Deliver Paper

Princeton University Professor Edward Felten cancelled plans to deliver a research paper in April 2001 after he received a letter threatening a lawsuit if he presented his work, which was in direct response to a challenge issued by the Secure Digital Music Initiative ("SDMI"). The SDMI developed a system to protect the copyrights of digital recordings for the music recording industry. The challenge was an attempt to prove their copyright protection mechanism was foolproof;[7] however, Professor Felten's team discovered ways to circumvent the security system. Professor Felten was planning to deliver a paper on his research when he received a letter from the Recording Industry Association of America ("RIAA") threatening a lawsuit if the paper was presented and instructing Professor Felten to destroy any workshop materials and avoid publicly discussing his research.[8]

On June 6, 2001, Professor Felten filed a complaint for declaratory judgment and injunctive relief against RIAA, and others.[9] After Professor Felten met with the defendants and representatives of the recording industry, the RIAA no longer objected to Professor Felten's paper; nevertheless, Professor Felten chose to continue with his lawsuit. On November 28, 2001, the U.S. District Court for the District of New Jersey held there was no justiciable issue since the defendants no longer objected to the paper being presented.[10] Professor Felten has since received assurances from the recording industry that his team will not be sued and has decided not to appeal his case. Professor Felten ultimately published his paper on August 15, 2001.[11]

C. America Online Cleared of Copyright Infringement

America Online, Inc. ("AOL") is the world's leader in interactive services and Internet access. One service AOL provides is access to the USENET, a collection of organizations whose computers connect with each other in order to exchange messages on various topics or "new-

---

7. SDMI, *Challenge FAQ* § 2 <http://www.cs.princeton.edu/sip/sdmi/faq.html#A1> (accessed Mar. 6, 2003).

8. Letter from Matthew J. Oppenheim, Sen. V.P., RIAA to Prof. Edward Felten, Princeton University, *RIAA/SDMI Legal Threat Letter* ¶ 6 (Apr. 9, 2001) (available at <http://www. eff.org/legal/cases/felten_v_RIAA/20010409 _riaa_sdmi_letter.html>).

9. *Id.*

10. *Felten v. RIAA*, No. CV 01-2669 <http://www.eff.org/IP/DMCA/Felten_v_RIAA/2001/128_hearinf_transcript.pdf> (D.N.J. Nov. 28, 2001).

11. Scott A. Craver et al., *Reading Between the Lines: Lessons from the SDMA Challenge,* 10th USENIX Security Symposium (Aug. 2001) (available at <http://www.usenix.org/events/sec01/craver.pdf>).

sgroups."[12] When a new message is posted to a USENET newsgroup, all of the computers connected to the USENET receive a copy of the message.

In *Ellison v. Robertson*, AOL was accused of copyright infringement because Mr. Ellison's copyrighted stories were stored on AOL's USENET server. Mr. Robertson originally posted the stories on a server not affiliated with AOL, but the stories were transmitted to AOL through the USENET. Even though the court felt AOL had constructive knowledge of the infringing material and therefore materially contributed to the infringement,[13] the court granted AOL's motion for summary judgment.[14]

D. THE DMCA

Each of these cases appears to be substantially different, yet, they all have one common thread, the *Digital Millennium Copyright Act of 1998* ("DMCA").[15] The DMCA was ostensibly a reaction to the increase in digital copyrighted material and the resulting explosion in pirating of this new medium. The Act essentially consists of two distinct parts. Title I – WIPO Treaties Implementation[16] – addresses the problem of ensuring the integrity of copyrighted works in a digital format by criminalizing the circumvention of measures meant to protect digital works.[17] Title II – Online Copyright Infringement Liability Limitation – limits an Internet Service Provider's ("ISP") liability for transmitting or maintaining copyrighted material by codifying much of the case law dealing with ISPs and service provider liability.[18]

This article will briefly review the pertinent sections of the copyright law affected by Titles I and II of the DMCA, and consider the significant case law involving the Act since it was enacted. Finally, this article will provide a direction for the future of the DMCA.

II. 17 U.S.C. § 1201 - 1205 – ANTI-CIRCUMVENTION

A. THE STATUTE

By far the most controversial piece of the DMCA is Title I and its anti-circumvention provisions. Under 17 U.S.C. § 1201, a person who circumvents or traffics in products meant to circumvent an access control measure used to protect a copyrighted work will be in violation of the

12. *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1054 (C.D. Cal. 2002).
13. *Id.* at 1059.
14. *Id.* at 1072.
15. 17 U.S.C. § 1201 (2000).
16. *Id.*
17. *Id.*
18. *Id.*

DMCA.[19] An example of an access control measure might be encryption technology, where a person wanting access to an encrypted work would need a key to decrypt the work before using it. In this case, the unauthorized use of a product that decrypts the copyrighted work or the trafficking of such a product is illegal.

A number of high profile cases have already dealt with the public disclosure of methods to circumvent access control technologies.[20] In these cases, violators of the DMCA have found ways to circumvent the protection mechanisms applied to the digital works. Under the DMCA, the public release of this information is considered trafficking in circumvention technology and it is illegal.

The statute has a limited number of fair use exceptions to the anti-circumvention provisions. Circumvention of access control technology for a computer program is lawful for the strict purpose of creating interoperability between the protected work and independently created programs.[21] Likewise, the circumvention of copyright protection technology is allowed for encryption research;[22] however, both of these sections require the party to have acquired the work lawfully and in good faith. There are additional exceptions for certain entities, such as nonprofit libraries and educational institutions, where possession of circumvented materials are allowed in determining whether to acquire the work.[23] This creates an interesting conundrum in that it is illegal for an institution to remove copyright protections from a work, but permissible to obtain works where the technological protections were illegally removed. The government may also violate the DMCA with impunity for lawfully authorized investigative activities of a government agent.[24]

The anti-circumvention provisions are punishable by both civil and criminal penalties. Section 1203 assesses civil remedies for a violation of the anti-circumvention provisions including temporary or permanent injunctions and either actual or statutory damages ranging from $200 to $25,000 per violation, plus attorney's fees. Treble damages may also be awarded for repeat violations.[25] In addition, any person willfully violating the anti-circumvention provisions for commercial advantage or private gain is open to criminal liability under 17 U.S.C. § 1204.[26] The punishment under these provisions includes up to $500,000 in fines and five years imprisonment for the first offense, and up to $1,000,000 in

19. 17 U.S.C. § 1201(a)(1).
20. *See e.g. Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001).
21. 17 U.S.C § 1201(f).
22. *Id.* § 1201(g).
23. *Id.* § 1201(d).
24. *Id.* § 1201(e); H.R. Rpt. 105-551, at 42 (May 22, 1998).
25. 17 U.S.C. § 1203.
26. *Id.* § 1204.

fines and ten years imprisonment for each subsequent offense.[27]

B. The Anti-Circumvention Provisions in Practice

The reported cases to date regarding the anti-circumvention provisions of the DMCA have all been civil infringement cases and not criminal.[28] *Realnetworks, Inc. v. Streambox, Inc.*[29] was one of the first cases to charge copyright infringement under the anti-circumvention provisions of the DMCA. Although this case only went to the preliminary injunction stage, it provides a good example of how the anti-circumvention provisions of the DMCA are being used and interpreted by the courts.[30]

Realnetworks, Inc. develops software products for sending multimedia content over the Internet through a process called streaming.[31] In the streaming process, the server software, or RealServer, initiates a handshake – a request to acknowledge that it is communicating with receiving software, the RealPlayer – in order to authenticate that both components are Realnetworks products. Once the handshake is established, the content is sent in an encrypted format. One of the attractive features of Realnetworks' products is the ability to restrict whether a user can save the content, based on setting a switch on the streaming file called the Copy Switch.[32] In addition to content providing software, Realnetworks offers a search engine that looks for audio and video clips on the Internet. The search capability is supplied through a contract with Snap! LLC.[33]

Streambox also develops software for providing multimedia content over the Internet. Steambox's VCR product has the capability of accessing and making copies of Realnetworks streaming files by emulating Realnetworks' handshake protocol. Once the handshake is established, VCR ignores the Copy Switch on the streaming file.[34]

---

27. *Id.*

28. The case against Dmitry Skylarov was a criminal indictment, but since the case has settled, there were no pertinent substantive rulings. The decision in Mr. Skylarov's employer's case has not been reported. In another DMCA case, on March 28, 2002, Mohsin Mynaf pled guilt to charges of violating the DMCA. *See California Video Bootlegger Pleads Guilty in Rare Case*, Business Recorder (Mar. 30, 2002).

29. *Realnetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

30. *See* Jim Hu, *Realnetworks Settles Lawsuit with Streambox*, CNET News.com (Sept. 8, 2000) <http://news.com.com/2100-1023-245482.html> (accessed Mar. 4, 2003) (stating that Realnetworks and Streambox entered into an out-of-court settlement).

31. *See Realnetworks*, 2000 WL 127311 at *1 (stating that multimedia content is audio, video, and a combination of audio and video).

32. *Id.* at *2.

33. *Id.*

34. *Id.* at **5, 6 (stating there was also an allegation about Streambox's Ripper and Ferret products). Ripper can convert a file from Realnetworks format into something else. *Id.* at *10. The court found that since the file had to already be on the users computer and

The court paraphrased the three prong test articulated by the DMCA to determine which products violate the Act: (i) primarily designed to circumvent copyright protections, (ii) limited commercially significant purposes other than circumvention, and (iii) marketed as a means for circumvention.[35] In granting Realnetworks preliminary injunction, the court found that Realnetworks' handshake and Copy Switch constitute technological measures that control access to copyrighted works[36] and that Streambox VCR violated the DMCA as a circumvention tool. The court said that VCR is a product designed to circumvent Realnetworks' copyright protection technologies with no other significant commercial value. Steambox's argument that VCR allows users to create "fair use" copies was rejected by the court, because, unlike the case in *Sony Corp. v. Universal City Studios*,[37] the owners of copyrighted works have taken affirmative actions to prevent people from copying their works and VCR is circumventing those actions.[38]

In this case, the court interpreted "technological measures" as applying directly to the digital work – Copy Switch – and to procedures for accessing the digital work in a secured environment, such as Realnetworks' handshake protocol. Broadening the definition to include mechanisms not directly applied to the work creates an additional control over the copyright monopoly granted by the Constitution and further threatens the constitutional rights of non-copyright owner's access to such works.

C. Constitutional Challenge to the DMCA

In *Universal City Studios, Inc., v. Corley*,[39] the issue was the protection of video distributed in Digital Versatile Disks ("DVD") format. When the motion picture studios began distributing films on DVD, the files were encrypted using a process called Content Scramble System ("CSS"). In order to view a CSS encrypted DVD, a player – DVD player or computer with a DVD drive – must be programmed to decrypt the code, although the decryption process does not allow the user to copy the film. In 1999, a Norwegian teenager collaborated with two other people

---

Ripper had a commercially legitimate purpose, it did not infringe Realnetworks copyrights. *Id.* Ferret is a "plug-in" application that alters RealPlayer to allow access to Streambox's search engines. *Id.* The court found that since it altered the RealPlayer Ferret created a derivative work of RealPlayer in violation of Realnetworks copyright. *Id.*

35. *Realnetworks,* 2000 WL 127311 at *7 (paraphrasing 17 U.S.C. §1201).

36. *Id.*

37. *Sony Corp. of America. v. Universal City Studios, Inc.,* 464 U.S. 417 (1984).

38. *Realnetworks,* 2000 WL 127311 at *9.

39. *Corley*, 273 F.3d at 429.

who have remained anonymous[40] to create DeCSS, a program that decrypts the DVD code. Originally created for computers running non-Microsoft operating systems, DeCSS also allows viewing and copying of DVD files from Windows based computers.[41]

Eight motion picture studios filed the original complaint against Shawn Reimerdes, Eric Corley and Roman Kazan, (Reimerdes and Kazan entered into consent decrees, leaving Corley as the sole defendant)[42] alleging the defendants listed the program instructions – also called code – on their Web sites, making DeCSS available to anyone on the Internet. Corley is the owner of 2600 Enterprises, Inc., which publishes a magazine called *2600: The Hacker Quarterly*,[43] which was subsequently added as a defendant. In November 1999, Corley wrote an article about DeCSS and placed the article, with the DeCSS code, on the magazine's Web site.[44] The district court enjoined Corley from listing the code and from hyperlinking[45] to other Web sites that maintain copies of the code.[46] On appeal, Corley challenged the constitutionality of the DMCA on Copyright Clause and First Amendment grounds.[47]

Under the Copyright Clause of the Constitution, the copyright protection is limited in time before it enters the public domain.[48] Since the anti-circumvention provisions of the DMCA would continue to protect a work after the copyright monopoly on a digital work has expired, the DMCA unconstitutionally confers a perpetual copyright grant.[49] The

---

40. *See* Linuxworld's, *Interview with Jon Johansen* <http://www.linuxworld.com/linuxworld/lw-2000-01/lw-01-dvd-interview.html> (accessed Mar. 6, 2003). Initially, it was understood that the teenager, Jon Johansen, was the creator of the program, however, Johansen has since stated that one of the other people he was collaborating with actually wrote it. *Id.* Johansen has also said that the two other people have remained anonymous because they are adults and work in the computer industry. *Id.* In January, 2003, a Norwegian judge acquitted Johansen on digital piracy charges. Dan Gillmor, *Cartel's Copyright Control Loosening*, San Jose Mercury News 1F (Jan. 12, 2003).

41. An operating system is the base program run on a computer. Most people are familiar with Microsoft's Windows operating systems. Non-Microsoft operating systems include Linux, MAC/OS and UNIX.

42. *Universal v. Reimerdes*, 111 F. Supp. 2d 294, 312 n. 91 (S.D.N.Y. 2000).

43. *2006: The Hacker Quarterly* is a magazine designed for computer hackers. For more information on the magazine and the origin of its name *see Corley*, 273 F.3d at 435-436.

44. *Corley*, 273 F.3d at 439.

45. *Id.* at 455 (quoting "a hyperlink is a cross-reference (in a distinctive font or color) appearing on one web page that, when activated by the point-and-click of a mouse, brings onto the computer screen another web page").

46. *Id.* at 441.

47. *Id.* at 439.

48. U.S. Const. art. I, § 8, cl. 8.

49. *See generally* John R. Therien, *Exorcising the Specter of a "Pay-Per-Use" Society: Toward Preserving Fair Use and the Public Domain in the Digital Age*, 16 Berkeley Tech. L.J. 979 (2001); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*,

court rejected this argument as being premature and speculative because the copyright monopoly of protected digital works has yet to expire.[50]

Corley also argued that computer code is speech and, as such, protected by the First Amendment. The court first considered whether computer code could be protected speech and found, "[i]nstructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by computer or human (or both)."[51] But, the court also stated that computer programs have a speech component – the information conveyed to a human – and a non-speech component – the information the computer uses to execute the program. It is the latter, non-speech component that the DMCA is concerned with and, thus, the DMCA is content-neutral as it relates to the First Amendment.[52] A content-neutral restriction is permissible if it serves a substantial governmental interest unrelated to the suppression of free expression and does not substantially burden more speech than necessary.[53] Ultimately, the court held the injunction restricting the posting of the DeCSS code was constitutional because the government's interest in preventing unauthorized access to encrypted works is "unquestionably substantial," and the injunction plainly served that interest. In addition, the injunction is unrelated to the suppression of free speech and since a less restrictive way to curb the distribution of the non-speech component of the DeCSS code was not available, the injunction did not substantially burden free speech more than necessary.[54] The court applied the same analysis in deciding the restriction on hyperlinking to DeCSS code on other Web sites was also constitutional.

In finding as it did, the court established for the first time the constitutionality of the DMCA. It also created a tension between the constitutional rights of the copyright owners and the constitutional freedoms of non-copyright owners. The Supreme Court will ultimately be placed in the position of determining the DMCA's constitutionality.

---

148 U. Pa. L. Rev. 673 (2000) (stating that there are actually two components to this argument). First, since technologies that prevent access to the works cannot be disabled, there is a restriction on a works fair use. *Id.* Second, as *Corley* argues, the use of such technologies grants a copyright owner perpetual protection, not a limited protection as contemplated by the Constitution. *Id.*

50. *Corley*, 273 F.3d at 445 (citing *U.S. v. Elcomsoft*, 203 F. Supp. 2d 1111, 1141 (N.D. Cal. 2002)) (finding that the DMCA does not unconstitutionally prevent the work from entering the public domain).

51. *Id.* at 448.

52. *Id.* at 454.

53. *Id.* (quoting *Turner Broadcasting System, Inc. v. F.C.C.*, 512 U.S. 622, 662 (1994)).

54. *Id.* at 454-55.

III. 17 U.S.C. § 512 – ISP SAFE HARBOR

A. THE STATUTE

An ISP supplies access to the Internet and provides other related services.[55] Prior to the DMCA, it was unclear what liability an ISP had for copyright infringement caused by one of its customers. The DMCA codifies the existing case law by offering a safe harbor for ISP's limiting liability to certain circumstances.[56] Under this section of the DMCA, a party is protected from liability against monetary and injunctive relief if they can be classified as a service provider and if they follow specific steps to remove the infringing material.[57]

A service provider is defined as:

> an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[58]

Section 512(k) further defines a service provider as one who provides "online services or network access."[59] It is important to note that in order to be shielded under the DMCA, a service provider must offer their services without modifying the materials. Service providers must also provide a stated policy for termination of repeat infringers to maintain their protection under the DMCA.[60]

A service provider can limit its liability for three modes of storing infringing material under the DMCA: 1) transitory communications, 2) material coming from outside the ISP's control and temporarily cached on the ISP's system, and 3) material stored by one of the ISP's users.[61] *Transitory communications* are those communications that are transmitted from the Internet and routed through a service provider's systems.[62] This typically occurs when data, such as e-mail, is communicated through a service provider to another user on the Internet. In this case, the service provider does not save this data on its systems. *Temporarily caching data* is an automatic technical process that occurs when an outside user sends data to one of the service provider's users, such as when a user from another service provider sends an e-mail to the service provider's user. The data would be temporarily stored on the service pro-

55. SearchWebServices.com, *ISP* ¶ 1 <http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci214028,00.html> (accessed Mar. 6, 2002).

56. H.R. Rpt. 105-551, at 11 (May 22, 1998).

57. 17 U.S.C. § 512.

58. *Id.* § 512(k)(1)(A).

59. *Id.* § 512(k)(1)(B).

60. *Id.* § 512(i)(1)(A).

61. *Id.* §§ 512(a)-(c).

62. 17 U.S.C. § 512(a).

vider's systems until the receiving user decides to remove it.[63] Here, the service provider's user does not create the offending data, rather the data comes from an outside source.[64] *Material stored by a service provider's user*, occurs when a service provider's user stores copyrighted material on the service provider's systems. This typically occurs when a service provider hosts a Web site for the user. The DMCA would protect the service provider from liability for copyright infringement, however, the service provider would have to take extreme measures to remove the offending material.

The service provider must satisfy three requirements to claim protection from liability for storing infringing material. First the service provider can have no actual or constructive knowledge of the infringing activity, and must act expeditiously to remove the material once they are aware of the infringement.[65] Second, the service provider cannot receive any financial benefit directly attributable to the infringing activity.[66] Finally, the service provider must promptly remove or disable access to the offending material once they receive notice of copyright infringement.[67] The elements of the notice must be in the manner prescribed by the statute[68] and sent to a designated agent of the service provider.[69]

Linking or directing users to areas with infringing material is also considered infringing activity.[70] If a service provider's user creates a Web site directing people to infringing material, the service provider may be liable for infringement. To avoid liability, the service provider must act upon the links in the same way offending material on the service provider's systems is addressed.[71]

The statute also protects the service provider against liability for two other forms of infringement. First, if the service provider is an institution of higher learning, the service provider cannot be held financially liable for any activity considered fair use.[72] The other safe harbor is for liability from the service provider's own user if the service provider is forced to remove or disable access to claimed infringing material, (called "taking down").[73] The removal of material must have been in good faith and the service provider must have notified the user of the take down.

63. *Id.* § 512(b)(1).
64. *Id.* § 512(b)(2)(E).
65. *Id.* §§ 512(c)(1)(A)(i)-(iii).
66. *Id.* § 512(c)(1)(B).
67. 17 U.S.C. § 512(c)(1)(C).
68. *Id.* § 512(c)(3).
69. *Id.* § 512(c)(2).
70. H.R. Rep. No. 105-551, at 56 (May 22, 1998).
71. 17 U.S.C. § 512(d)(1-3).
72. *Id.* § 512(e).
73. *Id.* § 512(g).

The service provider is also responsible for forwarding any counter notice from the user to the party alleging infringement.

The courts have consistently been challenged by this title of the DMCA in two areas: the definition of a service provider and what is sufficient for notice of copyright infringement. The following cases illustrate the arguments made on both sides of these issues.

B. Qualifying Under the Safe Harbor Provisions of DMCA

Since the enactment of the DMCA in 1998, a number of cases have shaped the interpretation of the statute's safe harbor provisions. In *Costar Group Inc. v. Loopnet, Inc.*,[74] Costar, a national supplier of real estate information services, alleged that Loopnet, an online brokerage service, was displaying Costar's copyrighted photographs on their Web site. Costar claimed that over three hundred of the pictures on Loopnet's site were copyrighted by Costar and were being infringed. In their defense, Loopnet invoked the safe harbor provisions of the DMCA claiming to be an online service provider.[75] Costar argued Loopnet cannot claim safe harbor because the photographs were reviewed and stored on the Web site at Loopnet's direction, Loopnet has no termination policy in place, Loopnet obtained a direct financial benefit from the photographs and Loopnet did not act expeditiously to remove the infringing material.[76]

On cross-motions for summary judgment, the court considered whether Loopnet could be shielded by the DMCA's safe harbor provisions, and agreed that, under the DMCA, Loopnet is a "provider of online services" eligible for safe harbor protection.[77] Since Loopnet only reviewed the pictures to ensure they were commercial properties not to assess whether they might be obviously infringing material, it was up to the users of the system to direct the storing and display of the photographs.[78] Loopnet did not challenge the sufficiency of the notice provided by Costar, so the court found Loopnet had knowledge of the infringement resulting from Costar's notice.[79] However, the court agreed with Loopnet's argument that they did not derive a financial benefit from the specific infringement given that Loopnet did not receive an additional benefit for showing the pictures.[80] The court had concerns about whether Loopnet's termination policy for repeat offenders and their "take down" policy were sufficient. On this point, the court said that

74. 164 F. Supp. 2d 688 (D. Md. 2001).
75. *Id.* at 691-692.
76. *Id.* at 692.
77. *Id.* at 701.
78. *Id.* at 702.
79. *Costar,* 164 F. Supp. 2d at 703.
80. *Id.* at 705.

there were several issues of material fact, so the parties were not entitled to summary judgment on this point.[81]

In sum, the court denied summary judgment on the issue of whether Loopnet was entitled to safe harbor under the DMCA since there was still an issue of material fact about whether Loopnet's termination and take down policies were sufficient. However, the court did consider Loopnet a service provider under the DMCA even though Loopnet was not an uninterested party such as an ISP.

C. Sufficiency of Notice

In *ALS Scan, Inc. v. RemarQ Inc.*,[82] the court was asked to determine what is sufficient notice of infringement before an ISP is afforded safe harbor protection. ALS Scan creates and markets copyrighted "adult" photographs. ALS Scan determined that RemarQ, an ISP, had hundreds of ALS Scan's pictures grouped in two "newsgroups" – 1) alt.als and 2) alt.binaries.pictures.erotica.als. ALS Scan contends these two newsgroups were created solely for the purpose of distributing ALS Scan's pictures. ALS Scan sent a cease and desist letter to RemarQ naming the two newsgroups containing infringing material, although ALS Scan did not list the specific images of concern.[83] RemarQ refused ALS Scan's demand stating the infringing material was not identified with sufficient specificity.[84]

ALS Scan sued RemarQ for copyright infringement and violating Title II of the DMCA.[85] The DMCA charge was related to RemarQ's failure to expeditiously remove the infringing material once they had notice of its existence. In their defense, RemarQ claims ALS Scan failed to identify the infringing material in compliance with 17 U.S.C. § 512 (c)(3)(A)(iii) because ALS Scan never provided them with the identity of the infringing pictures.[86] The court held that ALS Scan had substantially complied with the notice requirement even though they did not give every element of the notice,[87] thereby denying RemarQ its safe harbor defense.

---

81. *Id.* at 704.

82. 239 F.3d 619 (4th Cir. 2001).

83. *Id.* (stating that similar letters were sent to AOL, Erol's, Mindspring and others each of which complied with the letter).

84. *Id.* at 621.

85. 17 U.S.C. § 512 (stating where Title II of the DMCA is codified).

86. *ALS Scan*, 239 F.3d at 622.

87. *Id.* at 624.

D. Broad Definition of Service Provider/Proper Notice

In *Costar*, the court used a broad interpretation of the term "service provider" when it declared Loopnet was a service provider under the DMCA. At virtually the same time, the court in *Hendrickson v. eBay, Inc.*[88] was likewise employing a broad definition of service provider when applied to eBay. However, unlike the court in ALS Scan, the *Hendrickson* court did not find the incomplete notice of infringement to be substantially compliant with the Act.

EBay is an online auction service, which allows users to list descriptions of items they offer for sale. Hendrickson sent a letter, *pro se*, advising eBay that he was the copyright owner of a documentary called "Manson" and that pirated copies of the film were being offered on eBay's Web site. The letter demanded that eBay cease and desist from any conduct considered infringing. EBay's requests for additional information on Hendrickson's copyrights and the identification of specific infringing material were ignored prior to Hendrickson filing suit.[89]

Before addressing the issue of whether eBay could be held liable for copyright infringement, the court had to determine if the DMCA safe harbor provisions applied to eBay. Consistent with the court's finding in *Costar*, this court found that eBay was a service provider under the DMCA since they were providing an online service in the form of an online auction site.[90]

Ultimately, the court found that Hendrickson's notification did not comply with the DMCA's notice requirements in two ways. First, even though Hendrickson identified himself as the copyright owner of the documentary "Manson," the court was troubled that there was no written statement, under penalty of perjury, attesting to the fact that the information in the notification was accurate pursuant to 17 U.S.C. § 512(c)(3)(A)(vi).[91] Second, since Hendrickson did not give the specific item numbers of the infringing materials, the court felt his identification of the items were inadequate. The court did acknowledge that there would be instances where this amount of specificity would not be needed but did not believe this was such a situation, a result contrary to that in *ALS Scan*. Thus, the court decided eBay was a service provider under the DMCA, but Hendrickson's notification regarding pirated copies of "Manson" was insufficient, so eBay was entitled to safe harbor protection.[92]

---

88. 165 F. Supp. 2d 1082 (C.D.Cal. 2001).

89. *Id.* at 1084-1085.

90. 17 U.S.C. § 512(k)(1)(B).

91. *Hendrickson,* 165 F. Supp. 2d at 1089.

92. *Id.* at 1090.

E. Safe Harbor Conclusion

The cases interpreting the safe harbor provisions of the DMCA have construed the statute broadly albeit, at times, inconsistently. It is clear that Congress anticipated an ISP offering access to the Internet to be a service provider under the DMCA. However, the courts have broadened the statute to include organizations offering any type of online service. On the other hand, the courts have been inconsistent about interpreting the notification requirements of the DMCA. The conflicting outcomes of *ALS Scan* and *eBay* demonstrate that more guidance is needed before parties will know what constitutes an acceptable notice of copyright infringement.

IV. WHERE DOES THE DMCA GO FROM HERE?

Since its inception, questions regarding the constitutionality and equity of the DMCA have been raised. Upon enactment of the statute, the implementation of the DMCA, at times, has been unbalanced and controversial. The complaints have been heard on Capitol Hill where, in January 2002, U.S. Rep. Rick Boucher (D-Va.) announced he would introduce legislation late in 2002 to narrow the anti-circumvention provisions of the DMCA.[93] Stating that "the fair use doctrine is threatened today as never before,"[94] Rep. Boucher reintroduced the *Digital Media Consumers' Rights Act* ("DMCRA")[95] on January 7, 2003 after introducing it at the end of the 107th session of Congress. Cosponsored with John Doolittle (R-CA), Spencer Bachus (R-AL) and Patrick Kennedy (D-RI), the DMCRA seeks to reduce the restrictions on copyright fair use that the DMCA created.

Unfortunately, Rep. Boucher and his cosponsors stand virtually alone among their colleagues in the belief that the DMCA needs changing. Can the DMCA be amended so that it can equitably protect the rights of copyright owners while still allowing non-copyright owners access to fair use and public domain copyrighted materials? And can this be done without the harsh threat of criminal sanctions?

A. Title I – Anti-circumvention

Although the stated purpose of Title I was to bring the United States in compliance with two WIPO treaties, this simple description does not begin to illustrate how it affects copyright law in the digital age. The

93. *See generally* Rick Boucher, *Time to Rewrite the DMCA*, CNET News.com (Jan. 29, 2002).

94. Rick Boucher, *Lawmakers Urge Protection of Fair Use Digital Media Consumers' Rights Act Re-Introduced*, Press Release (Jan. 7, 2003).

95. H.R. 107, 108th Cong. (2003).

Supreme Court will ultimately determine the constitutionality of the DMCA, but it appears that the DMCA is in conflict with the Constitution on a number of points. First, the grant of a copyright monopoly was never intended to be perpetual. The Framers of the Constitution only intended artists to have exclusive rights to their works for a limited time. If a work is encrypted with a copyright protection measure, that work is effectively protected forever. Under the DMCA, it is possible for someone to take public domain material, combine it with protected material in a digital format, apply a protection measure to the medium and effectively lock the public domain material indefinitely. Attempting to circumvent the protection measures applied to the public domain material would be a violation of the anti-circumvention provisions of the DMCA. Second, the DMCA does not allow the disclosure of methods of circumvention. As was argued in *Corley*, this has potential First Amendment ramifications. The court in *Corley* stated that disclosing computer code could be considered protected speech, but still restricted its publication. The Supreme Court will undoubtedly decide the constitutionality of the DMCA, but until then there will always be a specter of invalidity associated with the Act.

The implementation of criminal sanctions against a violator of the DMCA's anti-circumvention provisions seems incomprehensible to many. The impact of this Act was not understood until the arrest of Dmitry Skylarov. The fact that a computer programmer from another country could be arrested for writing a commercially available program, in his own country, sends a shiver down the collective spine of all people working in the digital industry. Although it is arguable whether Mr. Skylarov intended his product to be used to circumvent copyright protections, he spent months in jail for conducting activity legal in his own country. In this case, the punishment seems to be cruel and unusual compared to the crime. And yet, Mr. Skylarov knows better than anyone how the DMCA can be used to punish.

Along similar lines, the DMCA has no provisions for the fair use of copyrighted material. The *Copyright Act* has long recognized that there are situations where a copyright can be infringed with impunity.[96] Digital material that contains technological measures to prevent copying cannot be used pursuant to copyright fair use provisions. The DMCA makes any use, fair or not, illegal. Although it is true that a library or educational institution may possess copyrighted material where the copy protection has been compromised, that is only for the limited purpose of determining whether to acquire the work. It is still illegal for the institution to circumvent the protections which leads to the catch-22 that they may possess the material after the illegal activity is completed but

96. 17 U.S.C. § 107.

cannot partake in the illegal activity. Although the DMCA affirms the fair use of copyrighted material,[97] there are no accommodations for obtaining a work for fair use. Therefore, the traditional fair uses in the *Copyright Act* cannot apply to protected digital material.

Perhaps the amendment to the DMCA proposed by Rep. Boucher will resolve some of these problems. The DMCRA proposes two significant changes relating to copyright fair use. First, it would amend the law to specify that using a circumventing technology is not a violation of the DMCA if it does not result in a copyright infringement. Second, it reestablishes the principles of *Sony v. Universal City Studios* by allowing the manufacture and distribution of circumvention technology if there is a significant non-infringing use. These are positive steps towards correcting the problems inherent with the DMCA, but they only address a small portion of the DMCA, and still must make the long trek through Congress before becoming part of the copyright statutes.

One unintended side effect of the DMCA became clear in the *Felten* case where the RIAA threatened to sue Professor Felten if he revealed his research on circumvention of the SDMI. Not only does this lead to serious issues of prior restraint, but also it effectively provides judicial enforcement of corporate trade secrets. The SDMI was a trade secret of the RIAA, there was no intent to patent the technology – that would publicly disclose the technology and render it useless. Similarly, the SDMI code was not copyrighted nor was there any intent to copyright the code for the same reason. In fact, the threat against Professor Felten does not stem from his disclosing the SDMI code, rather Professor Felten intended to show how to bypass the SDMI protections. If the actions of the RIAA had not been made public, they would have successfully restrained Professor Felten from disclosing the secrets of the SDMI. Consequently, RIAA would have succeeded in protecting their trade secret – SDMI – through the threat of lawsuit based on the DMCA anti-circumvention provisions.

There are no easy resolutions to this problem. Prior restraint could be considered reasonable in view of the ramifications in disclosing this type of information. However, when the prior restraint is protecting a corporate trade secret, it becomes less reasonable. This issue may become lost within the other more obvious problems with the DMCA, yet it is another example of what critics point to as a bias toward corporate copyright holders and away from individuals who are not intending to run afoul of the DMCA.

97. 17 U.S.C. § 1201(c)(1).

B. TITLE II – SAFE-HARBOR

Title II codifies a badly needed safe harbor for service providers such as ISPs. Prior to the enactment of Title II, service providers could be held liable for acts of copyright infringement committed by users of the service provider's computers. That would be tantamount to banks being held liable to the victim of a purse snatching because the thief deposited his ill-gotten gains with the bank.

When applying Title II, the courts have not only classified service providers as those who simply offer access to the Internet, but have also included those parties offering other online services. As a result, the safe harbor provisions of the DMCA potentially cover traditional brick and mortar businesses that offer services through the Internet, along with ISPs.[98] The courts have not addressed the situation where businesses have added online services to their core businesses – such as airlines – but, taken to the extreme, those industries will also fall under the DMCA's safe harbor protections in some manner. The question the courts will have to grapple with is how far to extend the safe harbor protections. Would a traditional company be liable for maintaining infringing material on their Web site if the site also has an online catalog of their products? Arguably, the catalog is an online service that the business is providing to their customers; therefore they can be considered a service provider under the DMCA. Then, is it too far to say simply maintaining a presence on the World Wide Web is tantamount to providing the service of giving information about a business – commonly referred to as advertising – and therefore the business is not liable for copyright infringement on its Web site? Obviously, this is not what Congress intended, and the courts should not interpret the DMCA so broadly. Rather, the courts should limit the scope of "service provider" such that the online service is an interactive service not just one that provides information. Although, a service provider need not offer the complete set of services of an ISP, they should be more than just a passive disseminator of information on a Web site. Further, the courts should narrow the scope of the safe harbor protections to infringing activity relating only to the online service. This would prevent a business from claiming protection from liability when the infringing activity is completely unrelated to the service being provided.

Courts have been inconsistent regarding what is substantially conforming notification. Congress gave the courts some room to determine what is required of the notice provisions in 17 U.S.C. § 512(c)(3). This area of confusion allows the courts to decide for themselves how much notice is enough. The result is that two courts could come to different

98. Examples of this would include Amazon.com which has brought a traditional bookstore to the Internet and eToys.com, which has done the same thing with toy stores.

conclusions based on the same set of facts as was seen in *ALS Scan* and *eBay*. In both cases, incomplete notice was given, however one court found it to be substantially conforming to the law while the other court found the notice to be insufficient. In fact, in *eBay*, where the court found that the notice did not substantially follow what was required, the court admitted there would be circumstances where the amount of notice given would be sufficient. The courts must develop a standard to consistently determine when notice is proper so the infringed parties will know what and how much information must be included for proper notice. A firm definition would also prevent courts from being accused of bias when they should be impartial.

The purpose of this article was to comprehensively review Titles I and II of the DMCA looking at the statutes and the relevant court cases interpreting the laws. Many of the problems with the DMCA are fundamental to the purpose and implementation of the Act. Some of these issues will be addressed by those legislators like Rick Boucher who are willing to take a stand that may not be favorable on Capitol Hill. Others of these problems will be challenged in the courts by people like Edward Felten, who are willing to risk both civil and criminal penalties in the pursuit of what they feel to be fair and just. And there will also be those like Dmitry Skylarov who are the unintended protectors of copyright freedoms. As computers and digital material become more prevalent in our society, a balance must be found between protecting the rights of copyright owners and the free transmission of those copyrighted materials.