Special Edition 2001 Volume 18, No. 3

Michigan
COMPUTER LAWYER

Editor
Paul J. Raine
praine@home.msen.com

http://www.michbar.org/sections/computer/

State Bar of Michigan Computer Law Section

Mark Your Calendars!

State Bar of Michigan Annual Meeting
September 12-14, 2001
Lansing Center, Lansing

Computer Law Section

Wed., September 12, 2001

Internet Privacy: *Issues and Solutions*

Mark your calendar for a free program on Privacy law brought to you by the Computer Law Section. The program will be held at 2:30 p.m. on Wednesday, September 12, 2001, at the State Bar Annual Meeting, in Lansing.

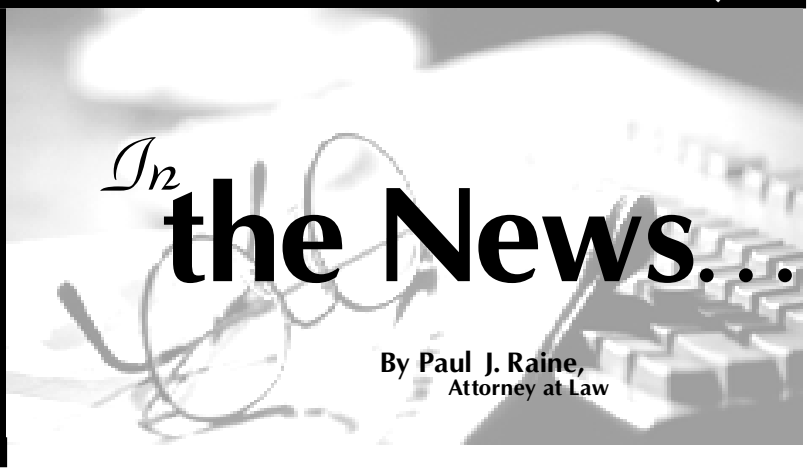
The program will focus on current US and European (EU) legislation. Our well-informed speakers are:

- **Jonathan Cornthwaite**, a noted Solicitor with the London Firm of Wedlake Bell
- **Joan Trusty** of EDS, and
- **Eric Grimm**, of Cyberbrief.

Together, the panelists will present an informative program on current EU legislation, current US legislation, and the outlook for the future of Privacy law.

3 An Analysis of the *Digital Millennium Copyright Act*

11 Meijer Wins Internet Domain Name Dispute



In the News...

By Paul J. Raine,
Attorney at Law

Special Edition Newsletter

This "special edition" of the Computer Law Section newsletter marks a change in the benefits of being a section member. In the past, the section has attempted to publish four newsletters per year, sometimes falling short of that goal. I have received many comments from section members that they look forward to receiving the newsletter and view the newsletter as one of the more significant benefits of paying their annual section dues.

I'm happy to announce in this edition that the newsletter will now be published bi-monthly, for a total of six issues per year. In addition to the award winning papers of the Edward F. Langs writing competition, I have received several articles recently from section members for publication. I look forward to your comments and suggestions regarding the newsletter in the coming year.

Paul J. Raine

Kudos

Kudos to Gregory L. Ulrich of Livonia. Greg is a member of the Computer Law Section and has recently been elected to the State Bar of Michigan's Board of Commissioners. He will represent Wayne County for a three-year term that will expire at the close of the Annual Meeting in 2004.

Greg has served three terms as State Bar commissioner and is a partner with the Livonia-based firm, Cummings, McClorey, Davis and Acho, PLC. His practice includes business litigation, real estate, technology, Alternative Dispute Resolution, and governmental matters.

Interesting People

The Interesting People (IP) e-mail list includes the participation of many technology-interested people. Four or five items a day (or more) are distributed via e-mail on current technology issues, ranging from UCITA to the latest Palm technology, to Domain Name controversies, and more. If you wish to join the list, please send an email request to Bernard Galler (galler@umich.edu). Messages sent to the IP list will always have a subject starting with "IP." Items of interest mainly to people in the Ann Arbor area have a subject starting with "IP (Ann Arbor)."

Bernard A. Galler
E-mail: galler@umich.edu
Fax: 734-668-9998

Award Winning Papers

The main feature by James R.W. McNeill in this "special edition" newsletter was the 1st place ($500) winner of the Edward F. Langs writing competition for 2000. The deadline for last year's competition was extended through December 31, 2000 and winners were announced in the summer edition of this newsletter. The judging for this year's writing competition took place in July and August and winners will be announced at the upcoming annual bar meeting in September. More award winning papers will be published in upcoming editions of the Michigan Computer Lawyer.

- Paul J. Raine

Computer Law Section

An Analysis of the *Digital Millennium Copyright Act* in light of *Universal Studios, Inc. v. Reimerdes*

By James R.W. McNeill
james_rw_mcneill@hotmail.com

TABLE OF CONTENTS

Introduction

The advent and advancement of the Internet have had a huge impact on American society. The dawn of the digital age has brought fundamental changes to both society and the law. An area where it has had an enormous and visible impact is in the field of entertainment. Because of the huge value of copyright goods, infringement is a primary concern. Digital technology has affected copyrighted entertainment in an unprecedented way. Now the ability to copy material without degradation of quality from generation to generation, and the possibility of "instantaneous" transmission worldwide via the Internet, has left copyright holders scrambling to enforce copyright protection. In the United States, Congress has recognized the need for a statute to assist the law in the protection of copyrighted material and passed the *Digital Millennium Copyright Act*[1] (DMCA) as a result. Then, in January of 2000, litigation was commenced, in *Universal City Studios, Inc.*, v. *Reimerdes*,[2] which led ultimately to the testing of the constitutionality of the DMCA. This case dealt with the breaking of the security encryption protecting movies on Digital Versatile Disks (DVDs)[3]; however, the defendants in this case were not sued over the actual 'hacking' of the encryption, but simply the posting of the code and the linking to the code on other websites.

This focus of this paper therefore is on this litigation not only because it is a landmark case with respect to the constitutionality

continued on page 4

of the DMCA, but because the arguments within the decision clearly delineate many of the issues which are, and will be, crucial to a case arising out of the DMCA. First, in order to effect an examination of these issues in the context of this case, a basic technical introduction of DVDs is necessary and the context for the enactment of provisions protecting copyright in the digital age must be established. Then, the circumstances leading up to the litigation which is the focus of this paper will be introduced. This will be followed by an in-depth examination of *Universal Studios, Inc.*, v. *Reimerdes*. This examination will review the court's rationale for deciding that the DMCA is indeed constitutional. As well, it will shed light on other issues relevant to litigation in the digital age. Finally, this examination will serve to reveal the conflict between those who feel that the rules have changed in the digital age in respect to copyrighted material and the copyright holders who are struggling to protect their copyright. In the end the DMCA was found to be constitutional, but it may have extended protection too far beyond the traditional level of copyright protection in an effort to adapt the law to technical developments in today's digital age. This is because this extension may have unexpected effects of stifling technological advancement which is beneficial to society in the long-run. Whether this is the case, however, remains to be seen as it is still too early in the development of the related technology and the case law to truly determine the impact of this statute.

Part I—DVD Background

(i) Technical Outline

The DVD very much resembles its more familiar cousin, the Compact Disk (CD), but it is technologically superior and will therefore replace the CD in the near future. Both are physically similar five inch disks. The DVD, however, can hold much more information. In fact, a DVD can hold up to 4.7 gigabytes of information which is approximately 7 times larger than the 650 megabytes of storage on a CD-ROM.[4] In order to control access to the digital contents of these disks, the content is encrypted with the Content Scramble System (CSS). The encryption-based security authentication system is encoded on the DVD and the chosen medium for playback, whether it be a DVD player or a computer (running a Windows- or Macintosh-based operating system). The system was adopted as the standard for the movie industry and, as a result, has been licenced to hundreds of content providers and manufacturers of DVD players globally.[5] Each DVD has multiple copies of the same decryption key and each of these is encrypted with every unlock code for each licenced player. A hacker, therefore, need only decrypt one of these keys in order to unlock the whole system and that is exactly what happened in this case. Much of the blame for the hack in this case is placed upon the encryption used for CSS. This encryption is not exceptionally strong because the developers had to adhere to export-based restrictions on the strength of the encryption. As a result, CSS is based upon a comparatively weak 40-bit proprietary algorithm, instead of a stronger public-key algorithm.[6] This, therefore, allowed for the code to be hacked much more easily. Interestingly, the U.S. government enforced these encryption limitations[7] and therefore, the copyright holders must rely on the DMCA to protect their interests in this case.

(ii)Intellectual Property Value

The first DVD player went on the market in June of 1997.[8] Since that time, approximately 10 million DVD players have been sold.[9] As well, there are currently more than 8000 DVD titles available in the United States.[10] The value to the American economy of the copyright interests involved here is massive. On December 16, 1999, the International Intellectual Property Alliance (IIPA) released "Copyright Industries in the U.S. Economy: The 1999 Report" which detailed its importance. The key points were as follows:

- The U.S. copyright industries accounted for 4.3% of U.S. GDP or $348.4 billion in value-added in 1997.
- In the last 20 years (1977-1997), the core copyright industries' share of GDP grew more than twice as fast as the remainder of the economy (6.3% vs. 2.7%).
- From 1977 to 1997, employment in the U.S. copyright industries more than doubled to 3.8 million workers (2.9% of total U.S. employment) and increased nearly three times as fast as the annual rate of the economy as a whole (4.8% vs.1.6%).
- The U.S. copyright industries achieved foreign sales and exports of $66.85 billion in 1997, more than all major industry sectors including agriculture, automobiles and auto parts and the aircraft industry.[11]

As a result, copyright holders are zealously attempting to protect their control over this money. For example, in the movie industry, the distribution of DVDs makes up approximately 35% of Warner Brothers Studios revenue of their home video market[12] which accounts for approximately 10% of their total movie distribution income.[13]

(iii) *The Digital Millennium Copyright Act*

As noted above, the value of copyright-protected materials is massively important to both the American and the global economy. There have therefore been initiatives to enhance protection globally. As an example, in December 1996 at a conference in Geneva Switzerland, the World Intellectual Property Organization (WIPO) adopted the WIPO Copyright Treaty. Article 11 declares that Contracting States, of which the United States is one, "shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights of their works, which are not authorized by the authors concerned or permitted by law".[14] There ensued lengthy Congressional consideration of related issues[15] and finally the DMCA was enacted in October 1998 both in response to his obligation and to protect American financial interests.

The relevant provisions within the DMCA which are the

focus in this case are the two anticircumvention provisions. The first, section 1201(a)(1)(A), states: "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title."[16] In *Reimerdes* this was a relevant consideration, but it was not the primary focus of this case. The focus was on the second provision which extended this protection even further in that it "supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies ... developed or advertised to defeat technological protections against unauthorized access to a work".[17]

Part II—Litigation Background

After DVDs were launched, there were those in the computer community who set out to hack the encryption system. Their expressed rationale for doing so was to allow for the playback on the open source operating system Linux because there were at the time only applications allowing for the playback in the Windows and Macintosh operating systems. In late 1999, Jon Johansen, a fifteen-year-old Norwegian, with the aid of two people he had contact with over the Internet (but who remained anonymous due to their use of pseudonyms) succeeded in hacking CSS. They reverse-engineered a DVD player and discovered the encryption algorithm and keys. This program, dubbed "DeCSS"(the "De" stands for "decrypt") was then posted "the executable code,[18] (but not the source code)[19]" on his Internet website in October of 1999. Johansen also announced on an Internet mailing list that he had done so.[20] In January of 2000, Norwegian police raided Johansen's home, seized his equipment and filed charges against him.[21]

Because of Johansen's efforts, DeCSS was widely available on the Internet. Many Internet site operators, in an effort to disseminate this material, posted (or "mirrored) it on their sites. As a result of the posting of DeCSS, the Motion Picture Association of America[22] (MPAA) sent out cease and desist letters on November 18, 1999.[23] Many complied with these orders. Among those who did not comply were Shawn C. Reimerdes, Eric Corley a/k/a "Emmanuel Goldstein,"[24] and Roman Kazan. In November of 1999, the three abovementioned parties posted DeCSS on their website to make it available for downloading.[25] As well, they listed links to other sites which simply had DeCSS directly available for download or linked to another sites which then had DeCSS available for download. As a result, on January 20, 2000, Justice Kaplan of the United States District Court, S.D. New York issued a preliminary injunction against the abovementioned parties enjoining them, broadly speaking, from posting DeCSS on their site,[26] but did not enjoin them from linking to other sites because the plaintiff failed to raise the issue in their motion papers.[27] Subsequently, Reimerdes and Kazan entered into consent decrees with the plaintiffs. The plaintiffs then added Corley's company, 2600 Enterprises, Inc., as a defendant.[28]

After the issuance of the preliminary injunction, DeCSS was removed from the 2600.com website, however the operators still provided links to other sites which offered DeCSS for download. The defendants were attempting their own form of civil disobedience and openly instructed others to mirror the files because, as the court later stated, the "defendants obviously hoped to frustrate the plaintiffs' recourse to the judicial system by making effective relief difficult or impossible".[29] Arguably, this act of effectively flouting the intent of the preliminary injunction did not win the defendants favour with the court and may in fact have prejudiced their case somewhat by demonstrating what the court perceived as bad faith on their part.[30]

Part III—*Reimerdes*

The lawsuit against Corley and the others was filed simply to get the defendants to stop posting DeCSS and, in the final decision, to stop linking to sites that provided access to DeCSS as well. As mentioned above, the preliminary injunction was successful in enjoining the defendants from posting DeCSS and the rationale of the court in coming to this conclusion will be discussed here in some detail with only a cursory mention of the linking issue.

The plaintiffs contended that Corley had contravened Section 1201(a)(2) of the DMCA which states:

> No person shall... offer to the public, provide or otherwise traffic in any technology... that –
> (A)is primarily designed or produced for the purposes of circumventing a technological measure that effectively controls access to a work protected under [the United States *Copyright Act*];
> (B)has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under [the United States *Copyright Act*];
> (C)is marketed by that person or another acting in concert with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [the United States *Copyright Act*].[31]

(i) Defense Argument – CSS and DeCSS do not fall within the scope of the DMCA.

The plaintiffs' first line of defense was to argue that the CSS does not fall under Section 1201(a)(2)(1) at all because it does not "effectively control" access to the plaintiffs' copyrighted material because the 40-bit encryption key was so weak. Necessarily, the court found that this argument failed because, under Section 1201(a)(3)(B), "a technological measure 'effectively controls access to a work' if the measure, 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 a work". Because access requires application of CSS, obtainable through permission of the owner,

continued on page 6

the strength of the encryption, therefore, is irrelevant;[32] a technological measure "effectively controls access" simply if its function is access control.[33] The court goes on to point out that the defendants' definition implicit in its argument here, that the control was not "effective" because it was broken, would lead to the somewhat absurd interpretation that the DMCA could only offer protection to measures which could not be broken (thereby remaining "effective"). Here the bottom line was that the court held that CSS effectively controlled access and was therefore covered by the DMCA.[34]

What, then, was the primary purpose of DeCSS? As a result of this finding, the court reasoned that, therefore, at this point "the only remaining question under Section 1201(a)(2)(A) is whether DeCSS was designed primarily to circumvent CSS."[35] Relying on the admissions of Johansen and Corley himself, the court found that this was indeed the case and, in fact, "that's all it does".[36] As a result, the court found that, barring the applicability of any statutory exception (discussed below), the defendants violated Section 1201(a)(2)(A) by posting DeCSS on the website. Further, this also proved sufficient to establish a prima facie violation of Section 1201(a)(2)(B).[37]

The court then goes on to examine what it refers to as the "centerpiece" of the defendants' defense – that DeCSS was not created to pirate copyright-protected movies, but was written to allow for the playing of movies on computers employing the Linux operating system. This raises an interesting point because it would indeed be possible for a legitimate owner of a DVD movie to play it on A Linux-based computer. This, however, is missing the point. What is at issue in this case was whether the defendants had violated the anti-trafficking portion of the DMCA. If the technology (DeCSS) falls within the parameters outlined in the DMCA as the court found, then the defendants' reasons for creation of DeCSS are completely irrelevant. Prior to the enactment of the DMCA, this may indeed have been a valid defense to copyright infringement (or at least the facilitation of copyright infringement) – post-DMCA this consideration was irrelevant. The only way, therefore, for DeCSS to be removed from the clutches, so to speak, of the DMCA would be for its creation to fall within one of the statutory protections.

(ii) Defense Arguments — Statutory Exceptions

(a) Reverse Engineering

Under 1201(f), a party may, in effect, develop a technological means to circumvent access control for the purpose of achieving interoperability with another computer program provided the copyright is not infringed.[38] As well, a party may make that information available if it is done "solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement".[39]

The court ruled that this defense failed for several reasons. First, Section 1201(f)(3) applies to those who actually have done the reverse engineering disseminating the information.[40] In this case, Corley had not, by his own admission, done the reverse engineering. Further, the statute provides that the right to disseminate applies "'solely for the purpose' of achieving interoperability".[41] As the court stated, "[i]t does not apply to public dissemination of means of circumvention, as the legislative history confirms".[42] Further, this line of defense argument failed in the eyes of the court for yet another reason; even if the person who reverse engineered the program tried to assert this defense it would fail. This is because Johansen admitted that DeCSS was developed on, and runs on, Windows. Therefore, the court reasons that DeCSS was not developed solely for the Linux system. This line of the court's reasoning is not however, necessarily true. The development on Windows may simply have been a necessary step toward the development of a Linux-based system. What seems to be at issue here is not the technical process for the development of the Linux-complaint system, but the credibility of Johansen. Simply put, the court does not believe his assertion that the interoperability of the program was the sole purpose. As the court tellingly noted, "Mr. Johansen is a very talented young man and a member of a well-known hacker group who viewed 'cracking' CSS as an end i[n] itself and a means of demonstrating his talent and who fully expected that the use of DeCSS would not be confined to Linux machine".[43] Where the court gets these assertions, we are unsure, but it certainly does illustrate something about the mindset of the court with respect to the initial hacking and perhaps this does inform the analysis of the decision somewhat. In fact, this point is not even wholly relevant to the decision of the matter before the court and the fact the court chose to take the time to comment on it regardless comments on the court's disdain for the actions of the defendants.

(b) Encryption Research

Broadly speaking, Section 1201(g)(4) allows for good faith encryption research to be a statutory exception. In making this determination the court examined: "whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement, whether the person in question is engaged in legitimate study of or work in encryption, and whether the results of the research are communicated in a timely fashion to the copyright owner."[44] The court, relying in part on the testimony of Corley himself,[45] found that the defendants' arguments failed on all counts primarily because the court found that they did not act in good faith.

(c)Security Testing

The defendants further argued that their actions should be considered security testing and therefore be exempt under Section 1201(j) of the DMCA. Again, the defendants fail with this defense in that actions are exempt only if they are "solely for the purpose of good faith testing".[46] By the defendants own admission, this was not their sole purpose. However, arguably by its very nature this is what Corley and his cohorts at 2600.com do when they hack programs. In fact, the court notes with disdain that *2600:The Hacker Quarterly*, a magazine

Corley began publishing in 1984, has included articles on "how to steal an Internet domain name,[47] access other people's e-mail,[48] intercept cellular phone calls,[49] and break into Costco stores[50] and Federal Express[51] ." On the surface these would seem like socially useless exercises doing more harm than good. However, when the results of these hacks and their posting are examined, it raises some questions about the social utility of criminalizing all of these types of actions under the DMCA. For example, Corley himself points out that when the article on stealing domain names was published, Network Solutions became aware of the security breach and took steps to remedy the problem.[52] Therefore, without the system being hacked and the entity in question, in this case Network Solutions, becoming aware of the problem, there would have been no technological improvements made to the system. The question then arises, does the DMCA go too far in this instance by hampering societal advancement? This is one of the age-old questions with respect to the balance between the rights of the copyright holder and society at large. Perhaps the law with reference to this issue should be reexamined.

(d) Fair Use

Traditionally, fair use was one of the exceptions to copyright infringement as the law attempted to balance the rights of the copyright holder and society at large. This concept is of vital importance in that it has "traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression". [53] This concept is codified in Section 107 of the *Copyright Act*.[54] This doctrine "limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement".[55] This, therefore, allows for the reconciliation of First Amendment rights and the rights of the copyright holder.

In the case of CSS, it does indeed limit fair use of the material in question. The defendants argued that the DMCA could not be construed to make it difficult or even impossible to make fair use of copyrighted contents of DVDs and therefore the law is not applicable to them because the provision of DeCSS to users merely enables others to make fair use of the material. The court noted that, under Section 107 of the *Copyright Act*, that certain uses which would otherwise infringe, do not constitute infringement under this doctrine. However, the court notes here that the defendants are not being sued for infringement, but for "offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act".[56] The court, in addressing this point, analysed the statute as well as the legislative history and concluded that Congress made a deliberate [57] decision not to make fair use a defense to a violation under Section 1201(a).[58] The court concluded that Congress carefully constructed the statute to balance the interests of the public and those of the copyright holder. Only circumvention itself is prohibited under this section. Fair use defenses, therefore, would be available to those who had "authorized' access to the material.[59] As well, Congress delayed the effective date if this section for two years so that fair use issues could be examined.[60] Further, Congress "created a series of exceptions to aspects of Section 1201(a) for certain uses that Congress thought 'fair,' including reverse engineering, security testing, good faith encryption research, and certain uses by nonprofit libraries, archives and educational institutions".[61]

Interestingly, the court considers the case *Sony Corp*. v. *Universal City Studios, Inc*.[62] and found that it was not applicable in this instance. In *Sony*, the defendants were sued for contributory infringement for manufacturing Video Cassette Recorders (VCRs). In the end, the defendants in that case were acquitted. Ironically the subsequent proliferation of VCRs in households worldwide brought a whole new market to the plaintiffs – a market which they themselves had not foreseen, but which now accounts for millions of dollars in revenue each year. The court found in this instance that the case at hand deals with slightly different activities here, but goes on to state that Sony would not apply regardless because that case "involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between Sony and the new statute".[63] Further, "[b]y prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape".[64] Arguably, this alteration defeats the spirit of copyright law which acknowledges society's need to have process not stifled by overly restrictive laws. Conceivably there are technological advancements which may arise, which in the long run may benefit society, but would be stifled by the DMCA. The court concluded on this point by noting that "[t]he fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyright works without the technical means for doing so is a matter for Congress unless Congress, decision contravenes the Constitution...".[65]

(iii) Defense Argument - First Amendment

The court concluded that computer code is speech which is *prima facie* protected by the First Amendment. However, "[r]egulation of different categories of expression is subject to varying levels of judicial scrutiny".[66] The court then concluded that a lower level of scrutiny should be applied in this case because this was not a "content-based" restriction (which would warrant strict scrutiny), but instead is a "content neutral" restriction warranting an "intermediate level"of scrutiny. The court accepted that DeCSS is expressive, but disagreed that it is a content-based regulation of speech stating that this approach "would be a unidimensional approach to a more textured reality and entirely too facile".[67] The court stated that "[t]he reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality – with preventing people for circumventing technological access control measures".[68] The level of scrutiny ap-

continued on page 8

plied in this case then is much lower. However, the court also noted that a regulation need not be the least restrictive means of advancing the governmental interests[69] and that the regulation would be considered to be sufficiently narrowly tailored "'so long as the ... regulation promotes a substantial government interest that would be achieved less effectively absent the regulation'".[70] The court went on to note that this level of scrutiny was justified because dissemination of the code would lead directly to infringement. If the code was out there, people would use it. In making this determination the court noted that "the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality".[71] Under this level of scrutiny the DMCA was found to be constitutional.

(iv) Defense Argument - Prior Restraint

The defense then tried unsuccessfully to argue that the injunctive relief against the dissemination of DeCSS should be barred by the doctrine of prior restraint. The court noted that "administrative preclearance requirements for and at least preliminary injunctions against speech as conventionally understood are presumptively unconstitutional".[72] However, the court simply ruled that this was not the case here because "the enjoined expressive element is minimal and because a full trial on the merits had been held".[73]

(v) Defense Argument - Overbreadth.

The defense also tried to argue that the DMCA was overbroad because of its effects on third parties in preventing those lacking technical expertise from having the ability to make fair use of the plaintiffs' encrypted copyrighted content. The court noted a variety of fair uses to the copyrighted material in this case, but noted simply that:

> ... each necessarily involves one or more of three types of use: (1) quotation of the words of the script, (2) listening to the recorded sound track, including both verbal and non-verbal elements, and (3) viewing of the graphic images. [74]

The court concluded that these were all affected by the DMCA, "but probably only to a trivial degree".[75] Further, the court justified this finding by reasoning that the material is available because most movies are also available on videotape, thus DMCA does not materially impair access in this context, but even if this was not the case, compliant DVD players allow for playing a movie without infringing. This reasoning seems somewhat strained at best in that this defense is disallowed because the material is available elsewhere through other media this is not a valid defense. Interestingly, however, the court goes on to note that:

> [t]he same point might be made with respect to copying of works upon which copyright has expired. Once the statutory protection lapses, the works pass into the public domain. The encryption on a DVD copy of such a work, however, will persist. Moreover, the combination of such a work with a new preface or introduction might result in a claim to copyright in the entire combination. If the combination then were released on DVD and encrypted, the encryption would preclude access not only to the copyrighted new material, but to the public domain work. As the DMCA is not yet two years old, this does not yet appear to be a problem, although it may emerge as one in the future.[76]

Arguably, this should have been considered and given more weight by the court. In the end the court stated that the overbreadth challenge fails and based this decision to a large degree on the fact that there was not enough information from the third parties who would be affected by the DMCA. The court states that the information before the court is "scanty and fails to adequately address the issues".[77]

(vi) Defense Argument - Vagueness

The court quickly discounted the argument that the DMCA is void for vagueness because "the terms it employs are not understandable to persons of ordinary intelligence and because they are subject to discriminatory enforcement."[78] The court found that the conduct fell squarely within the parameters of the DMCA and therefore was not vague.

(vii) Defense Argument - Linking

The defense tried to challenge the concept that linking to sites providing DeCSS is not consistent with First Amendment principles. The court found that links have both expressive and functional elements and therefore must be subject to the "same O'Brien[79] standard that govern trafficking in the circumvention technology generally".[80] Further, posting and linking were found to be essentially the same thing. Linking, therefore, is enjoined as well. The court was careful to note that the ruling in this instance would not open just any website operator to legal liability for all content on all sites linked to. The court here is recognizing the societal value of the Internet and did not want to have a chilling effect on the Internet by making this part of the ruling too expansive. Liability will only be found in circumstances where there is:

> clear and convincing evidence that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.[81]

In this case however, the court found, from the defendants' conduct and statements that they were fully aware of what they were doing and therefore found them liable under the DMCA.

Part IV—Relief

The defendants had argued that the plaintiffs failed to prove that decrypted movies were in fact available.[82] The judge was satisfied, that this was the case. Nevertheless in order to obtain an injunction under Section 1201(b)(1) there need only be a

threat. So this point is moot. Second, the defendants' claim that the plaintiffs exaggerate the threatened injury and that the studios do not perceive DeCSS as a threat.[83] The judge discounted this argument. Third, the defendants contend that there is no evidence that there were any movies decrypted with DeCSS.[84] This argument necessarily failed because, even though the court acknowledged the existence of other programs with a similar function, the movies were obviously decrypted using DeCSS or another program. These other utilities, absent evidence to the contrary, would be seen to contravene the DMCA. As a result the court applied the principle from *Summer* v. *Tice*.[85] The court explained that:

> [w]here, as here, two or more persons take substantially identical wrongful actions, one and only one of which had to be the source of the plaintiffs' injury, and it is equally likely that one inflicted the injury as the other, the burden of proof on causation shifts to the defendants, each of which is liable absent proof that its action did not cause the injury. [86]

In response the defendants argued that this principle should not be employed unless they joined all possible defendants (those who contributed to the injury). The court dismissed this concept as "nonsensical",[87] particularly in the context of the Internet where the defendants are innumerable, often anonymous and distributed worldwide. The court found that there was not an adequate remedy because the damages could not be accurately assessed. Damages could be assessed up to $2500 per offer of DeCSS under section 1203(c). A permanent injunction was therefore ordered. The court then made another crucial determination in the context of copyright infringement cases on the Internet. The defendants asserted that to issue an injunction would be like "locking the barn door after the horse is gone".[88] Finally, the court wanted to send a clear message in the context of these actions on the Internet when Kaplan J. stated:

> the likelihood is that this decision will serve notice on others that "the strong right arm of equity" may be brought to bear against them absent a change in their conduct and thus contribute to a climate of appropriate respect for intellectual property rights in an age in which the excitement of ready access to untold quantities of information has blurred in some minds the fact that taking what is not yours and not freely offered to you is stealing.[89]

In the end, the court issued injunctive and declaratory relief. Under the DMCA, Section 17 U.S.C. § 1203(b)(4), (5) allows for a discretionary order for costs and attorneys' fees may be awarded to the successful litigant. In this case the judge decided against awarding costs because this was no important test case.[90] In conclusion the judge noted that the defendants "have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era". [91]

Conclusion

In the end, *Reimerdes* deemed the DMCA constitutional. Careful scrutiny of this decision reveals a wide variety of possible defenses, all of which failed in the context of the DMCA. Further, this examination reveals the fact that Congress carefully crafted this statute in a way that extended the traditional protections for copyright in a way that caught the defendants in their provision of the ability to infringe over the Internet. Whether this piece of legislation has gone too far in that it will go against the carefully measured balance of the rights of the copyright holder and the public-at-large by stifling progress and innovation remains to be seen. Only a review of the litigation and the case law as it develops over the coming years will provide better insight into this issue. What the future of the Internet holds in respect to this issue remains to be seen.

Endnotes

1 17 U.S.C. § 1201 seq.

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

3 DVDs are primarily used for movie distribution although there are other formats which are in the process of being developed for market like DVD-RAM, DVD-ROM, and DVD-Audio. It should be noted that the planned release of the format which many in the entertainment industry will eventually replace the CD as the standard for music distribution, DVD-Audio, was delayed from hitting the market by the hack of the DVD security system. A discussion of this aspect of the hack, however, is outside the scope of this paper.

4 A. Patrizio, *DVD-Audio – The Sound of Silence*, Wired, at: http://www.wired.com (last visited: April 1, 2000).

5 DVD-Copy Homepage, at: www.dvd-copy.com (last visited: April 1, 2000).

6 *Id.*

7 See, for example, E. Messmer, *Government Restrictions on Encryption Pose Obstacles for Internet Security*, at: http://www.cnn.com/tech/computing/9805/19/encryption (last visited: December 1, 2000).

8 K. Nice, *How DVDs and DVD Players Work*, at:http://www.howstuffworks.com/dvd14.htm (last visited: November 30, 2000).

9 *Id.*

10 *Id.*

11 International Intellectual Property Alliance, Press Release 202-833-4198, "New Study Reveals Copyright Industries Are Driving the U.S. Economy – Copyright Industries Lead the Economy in Contribution to GDP, Jobs and Foreign Sales" (December 16, 1999) at: http://www.iipa.com/html/121699_press_release.html (last visited: December 2, 2000).

12 *Reimerdes*, at 310 n.69.

13 *Id.*, 310 n.70.

14 World Intellectual Property Organization Copyright Treaty, Apr. 12, 1997, Art. 11, S. Treaty Doc. No. 105-17 (1997), 1997 WL 447232.

15 *Reimerdes,* at 316.

16 17 U.S.C. § 1201(a)(1)(A).

17 H.R. REP. NO. 105-551(I), 105th Cong., 2d Sess. ("JUDICIARY COMM.REP."), at 18 (1998) at cited in Reimerdes, at 316 n.132.

18 See Tr. (Johansen) at 622-23, 638; Ex. 9 at SCH-000846, noted at *Reimerdes*, 311 n.73.

19 See Tr. (Johansen) at 635, noted at *Reimerdes*, 311 n.73.

20 See Tr. (Johansen) at 622-23, 638; Ex. 9 at SCH-000846, noted at *Reimerdes,* 311 n.73.

continued on page 10

[21] The legal issues and factual circumstances surrounding Mr. Johansen's arrest are beyond the scope of this paper and therefore will not be discussed herein.

[22] The MPAA membership includes Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Metro-Goldwyn-Mayer Studios, Inc., Paramount Pictures Corporation, Time Warner Entertainment Co., L.P., Tristar Pictures, Inc., Twentieth Century Film Fox Film Corporation and Universal City Studios, Inc.

[23] *DVD Copy Control Association, Inc*. v. *McLaughlin*, 2000 WL 48512 (Cal.Superior) at 1.

[24] As an interesting footnote, Corley has dubbed himself "Emmanuel Goldstein" after the main character in Orwell's 1984. (See *Reimerdes* at 308). This serves to give the reader some insight into the mindset of Corley and how he likes to view himself vis-a-vis the mainstream computer establishment.

[25] See Tr. (Corley) at 791; Ex. 28, noted in *Reimerdes* at 312 n. 83.

[26] Preliminary Injunction, January 20, 2000 (DI 6) *Universal City Studios, Inc.*, v. *Reimerdes*, 82 F.Supp.2d 211. [hereinafter *Reimerdes Injunction*].

[27] See Tr., Jan. 20, 2000 (DI 17) at 85, noted in *Reimerdes*, at 312 n.93.

[28] *Reimerdes*, at 312 n.93.

[29] *Id.* at 313.

[30] In fact, post-decision, the defendant Corley, posted a comment on his website stating that he felt the court was biased against his cause. He even pointed to the language used by the judge in the decision suggesting it was evidence of the judge's hostility toward the defendants. See E. Corley, "Analysis of the Decision Against 2600" (August 21, 2000) online: 2600: The Hacker Quarterly - News Archive, at http://www.2600.com/news/2000/0821.html (last visited: November 22, 2000) [hereinafter Corley].

[31] 17 U.S.C. § 1201(a)(2).

[32] *Reimerdes*, at 318.

[33] *Id*.

[34] *Id.* at 319.

[35] *Id.* at 318.

[36] See Tr. (Johansen) at 619; (Corley) 833-34, noted at *Reimerdes*, at 319.

[37] *Reimerdes*, at 319.

[38] 17 U.S.C. §§ 1201(f)(1), (2).

[39] 17 U.S.C. § 1201(f)(3).

[40] *Reimerdes*, at 320.

[41] *Id*.

[42] See Commerce Comm. Rep. at 43, noted in *Reimerdes* , at 320.

[43] *Reimerdes*, at 320.

[44] *Id*., at 321.

[45] Ex. 96 (Corley Dep.) at 33, noted in *Reimerdes*, at 321.

[46] 17 U.S.C. § 1201(j).

[47] See Ex. 1.2 - R. Crim, *How Domains Are Stolen*, 2600: THE HACKER QUARTERLY, Summer 2000, at 43, noted at *Reimerdes*, at 308 n.41.

[48] See Ex. 1.16 - Schlork, *Snooping via MS-Mail*, 2600: THE HACKER QUARTERLY, Winter 1996-97, at 28, noted at *Reimerdes,* at 308 n.42.

[49] See Ex. 1.16 - T. Icom, *Cellular Interception Techniques*, 2600: THE HACKER QUARTERLY, Spring 1995, at 23, noted at *Reimerdes*, at308 n.43.

[50] See Ex. 1.12 - nux, *Fun at Costco*, 2600: THE HACKER QUARTERLY, Summer 1999, at 12, noted at *Reimerdes* fn44 at 12.

[51] See Ex. 1.19 - PhranSys Drak3, *Hacking FedEx*, 2600: THE HACKER QUARTERLY, Autumn1997, at 14, noted at *Reimerdes*, at 309 n.45.

[52] See Corley, *supra* note 20.

[53] *Reimerdes*, at 321.

[54] 17 U.S.C. § 107.

[55] *Reimerdes*, at 321.

[56] *Id*.

[57] *Id*.

[58] *Id*.

[59] *Id*., at 323.

[60] 17 U.S.C.A. § 1201(a)(1).

[61] *Reimerdes* at 323. See 17 U.S.C.A. § 1201(d),(f),(g),(j).

[62] 464 U.S. 417, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984) [hereinafter *Sony*].

[63] *Reimerdes* at 323.

[64] *Id*.

[65] *Id*., at 324.

[66] *Id*., at 326.

[67] *Id*., at 328.

[68] *Id*., at 329.

[69] See *Turner Broadcasting System, Inc*., 512 U.S. at 662.

[70] *Reimerdes*, at 330, quoting *United States* v. *Albertini*, 472 U.S. 675, 689, 105 S.Ct. 2897, 86 L.Ed.2d 536 (1985).

[71] *Reimerdes*, at 332.

[72] *Id*.

[73] *Reimerdes*, at 335, here the court noted Lemley & Volokh, 48 DUKE L.J. at 211-12, 215 (which acknowledged that a high likelihood of success diminishes the risk of erroneous suppression of protected speech).

[74] *Reimerdes*, at 337

[75] *Id*.

[76] *Id*., at 338, n245.

[77] *Id*., at 338, n.246.

[78] *Id*., at 338

[79] See *United States* v. *O'Brien*, 391 U.S. 367, 377, 88 S.Ct. 1673, 20 L.Ed.2d 672 (1968).

[80] *Reimerdes*, at 339.

[81] *Id*., at 341.

[82] *Id*., at 341n.260, Def. Post-trial Mem. at 27, 28.

[83] *Id.* at 342 n.262, Def. Post-trial Mem. at 28.

[84] *Id.* at 342 n.263, Def. Post-trial Mem. At 28, 29.

[85] 33 Cal. 2d 80, 199 P.2d 1 (1948).

[86] *Id*., at 342 n.267.

[87] *Id*., at 342 n.267.

[88] *Id*., at 344.

[89] *Id*., at 345.

[90] *Id*., at 345.

[91] *Id*., at 346.

Meijer Wins Internet Domain Name Dispute

Chadwick C. Busk
Meijer Senior Counsel
www.ccbatcyberlaw.com

What does the Meijer Legal Department do when a disgruntled customer decides to register domain names containing Meijer's trademarks, as in *meijerphoto.com* and *meijerphotolab.com*? First, we contacted him and explained the law of trademarks in relation to Internet domain names. We even offered him a reasonable sum for his ruined film and to register domain names that didn't infringe on the Meijer marks, not even demanding that he remove the content of his web site, which unfairly criticized Meijer's in-store photo lab. When the customer did not respond to our generous offer, we initiated an arbitration action with the National Arbitration Forum under the ICANN Rules for Uniform Domain Name Dispute Resolution Policy. Thus, the case of *Meijer, Inc. v. Porksandwich Web Services* was born.

On July 6, 2001, the Arbitration Panel ruled that Porksandwich ("Respondent") had to relinquish the two disputed domain names and transfer them to Meijer. First, the Panel found that confusion would likely arise as a result of the Respondent's current use of each of the contested domain names, which contained both registered and common law Meijer trademarks:

> **"There can be no question here that each of the contested domain names, by virtue of its inclusion of the term 'MEIJER', as currently used by the Respondent or by a third party to which the Respondent might transfer that name, will likely cause user confusion."**

Internet users would be misled by Respondent's use of the domain names**,** thinking that they identified web sites created by Meijer to promote its photo lab operations**.**

Second, the Panel determined that Respondent's use of the domain names was illegitimate. After discussing legal authority, which compares the rights of trademark holders to a person's First Amendment rights to criticize the businesses represented by the trademarks, the Panel noted that Respondent refused Meijer's suggestion to register a new domain name to include a pejorative term, such as *sucks*. Respondent failed to prove that he could **not** have registered a domain name containing a pejorative term as part of the name and thus receive free speech protection.

Finally, the Panel found that Respondent's actions constituted bad faith registration and use of both of the contested domain names:

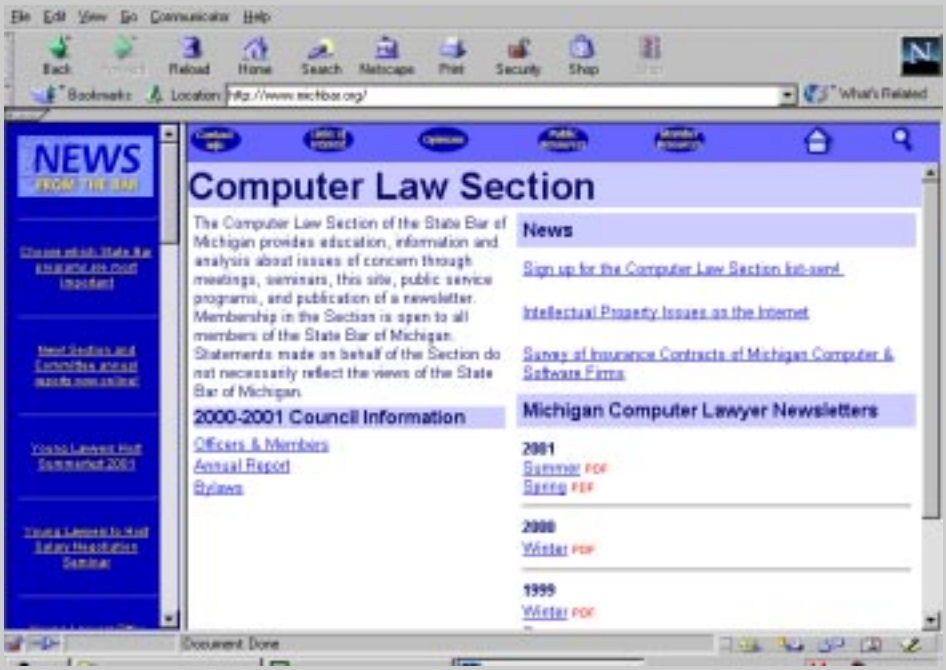
> **"There can be no doubt, particularly after the Respondent chose to register the second contested domain name [meijerphotolab.com], of its calculated intent to cause user confusion and, by doing so, injure the Complainant's photofinishing and film processing business by diverting those users away from doing business with the Complainant, either through its web site or even its traditional stores."**

The Panel noted that the Respondent's conduct indicated a pattern, which effectively prevented Meijer from using its trademarks in either domain name, and this was also proof of bad faith registration and use of both domain names.

The opinion of the Panel can be found on the Web at: *ww.arbforum.com/domains/decisions/97186.htm*.

Visit our Section Website

www.michbar.org



Computer Law Section
State Bar of Michigan
Michael Franck Building
306 Townsend Street
Lansing, MI 48933-2083

PRESORTED
FIRST CLASS MAIL
U.S. POSTAGE PAID
LANSING, MI
PERMIT NO. 191