The DMCA and Researchers' First Amendment Rights
Amy E. McCall*

Introduction

The Digital Millennium Copyright Act, or DMCA, was enacted by Congress in October of 1998.1 Section 1201(a)(1) of the Act, known as the "anti-circumvention" provision, states that "[n]o person shall circumvent a technological measure that effectively controls access to a [digital] work protected under this title.".2 Sections 1201(a)(2) and 1201(b) combine to form the "anti-trafficking" provisions, which provide that no one shall distribute technology that can accomplish this circumvention.3 Congress constructed a two-year delay in implementation of these provisions, thus, on October 28, 2000, circumvention of effective technological controls became punishable by both civil and criminal actions.4 Unfortunately, the presence of these provisions, along with courts refusal to recognize traditional copyright privileges and defenses in this area of "paracopyright,"5 chills programmers' speech.

Long before the enactment of the DMCA, commentators worried that the passage of this proposed legislation would adversely affect the First Amendment rights of citizens.6 These First Amendment worries ranged from a generalized concern about the "right to read anonymously," implied in the First Amendment to the free speech rights of researchers and programmers whose business it is to create and analyze technological measures that effectively control access to a digital work.7

This paper will focus on two current civil actions under the DMCA in which programmers are asserting that enforcement of the DMCA violates their First Amendment rights; *Universal City Studios, Inc. v. Reimerdes*8 and *Felten v. RIAA*.9 Before discussing these significant cases, Part I of this paper provides a sufficient history of copyright to understand the circumstances that brought about the DMCA. Part II provides a brief introduction to the concepts and terminology necessary to understand the cases. Part III introduces the two cases mentioned above which are currently before the courts. Although both cases directly implicated the DMCA, they reached that point in different ways. In *Reimerdes*, Universal City Studios used the DMCA to effectively challenge Internet posting of decryption software capable of decrypting DVDs, while in *Felten*, researchers sought reassurances that they would be permitted by creators of protection techniques for music CDs, to publish information on their successful decryption. Both suits additionally sought to have the anti-circumvention and anti-trafficking provisions of the DMCA declared unconstitutional as to unacceptable restrictions on researchers' First Amendment Rights. Part IV lays out several of the leading alternatives to the current anti-circumvention provisions, ranging

from elimination of the provisions entirely, to stringent encryption techniques controlled by trusted third parties charged with protecting the public interest in the digital copyright world. Although eliminating these provisions and placing digital copyright back within the realm of traditional copyright might be the best solution, it is most likely not a politically acceptable alternative. Thus, one of the measures permitting some amount of special protection for digital works, while allowing traditional copyright defenses, is probably the optimal solution. Part V is a brief conclusion that outlines the disposition of the discussed cases under the proposed alternatives.

Part 1-History of the DMCA

Copyright, as it is known in the United States, came into existence in response to the history of censorship in England. As early as 1557, Queen Mary granted a single publishing guild the right to publish books in England in return for its promise to obtain pre-approval for all publishing.10 This led to a system where publishers had great power over authors and their works. Many consider that copyright had its true beginnings in 1710, when the Statute of Anne was enacted in Britain.11 The Statute of Anne was necessary to stop publishers' oppression of authors and the public under the previous regime, and begin a system where authors had control of their own works.12

When the Constitution was drafted, the members of the Constitutional Convention believed strongly that a healthy dialogue was necessary to protect the democracy they had envisioned. To promote this healthy dialogue, James Madison proposed a clause in Article I of that document, that authorized Congress to enact copyright legislation. Article I, §8, cl. 8, stated, "The Congress shall have Power… To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."13 It is important to note that the Constitution expressly authorized that the copyright protections are to be for a "*limited* time" and are designed to promote "the *Progress* of Science and Arts."14 The Framers believed, and rightly so, that the healthiest democracies require a public dialogue. Thus, there is no protection given to ideas. And protected works were to be protected only long enough to provide incentive for the creators of the work to create more. At that point, such works would go into the public domain, where they could best support the healthy debate necessary for our democracy. As this article will demonstrate, provisions of the DMCA ignored these constitutional notions. In the legislators' zeal to protect those who believe their copyright privileges should be infinite, they have undercut the very purpose of the constitutional clause empowering their action.

By the beginning of the twentieth century, copyright law had become too complicated for the average citizen to understand.15 It had also become too complicated for many of the legislators responsible for creating copyright law.16 The Congressional solution to this dilemma in the beginning of the twentieth century was to require all "interested parties" to propose legislation that they would deem acceptable.17 This complicated process brought many familiar names into the process,

as content holders such as Samuel Clemens (Mark Twain), testified before Congress in 1906 as to their reasons for believing that extended copyright protection should be available to them.18 There were multiple problems with this process of allowing currently interested parties to determine copyright legislation. Two of the most significant were: 1) Only powerful parties were represented-emerging technologies or yet-to-emerge technologies had no representation in this process; and 2) no one represented the public in this process. Since the public had no lobbying group and there were strong interests represented by the content-holders, the legislature abdicated its responsibility to protect the public interest. The result was a system in which current content holders-authors, publishers, etc.--were granted more expansive rights, while emerging technologies, such as motion pictures, were left out of the process. Copyright legislation has followed this path for most of the past century and much of the process is similar today.

For generations, the United States was a net copyright importer, i.e. it imported more copyrighted material than it exported. Therefore, when the United States was approached with the first Berne Convention in 1886, to create international recognition of copyrights, the existing powers refused to sign that treaty.19 Although the United States eventually signed a reciprocal copyright agreement with England, it refused to sign the Berne Convention until 1988, over one hundred years after the first opportunity.20 By this time, the United States had become a net copyright exporter, and therefore, the burden required on this country to recognize other signatories' copyright was far outweighed by the benefit of having other countries recognize United States copyright. Also in the late 1980's, at approximately the same time as the United States became a signer of the Berne Convention, the United Nations World Intellectual Property Organization (WIPO), created in 1970, began to focus its attentions on copyright.21 Although the term "Intellectual Property" appeared in legal writings once or twice before 1900, the creation of WIPO spurred a massive growth in the use of the term and in case law depending on intellectual property as the basis of those actions.22 This organization drew up a treaty that the United States did sign.23 The WIPO treaty, among other things, required recognition of copyright for digital media and protections for the anti-circumvention technologies used to protect that media.24 There were individuals who believed that the then existing United States copyright law adequately covered the terms of the treaty or required only minimal modification.25 However, the Clinton administration authorized a group to determine the best possible way to protect information available on what they labeled the National Information Infrastructure, or NII (commonly known as the Internet).26 Bruce Lehman headed up this effort, and offended many people by protecting what were perceived to be the rights of big business, but not the civil rights of the general citizenry.27 The "Green Paper" (or proposal) that was created by the group caused a negative stir among many concerned parties.28 When the final White Paper was released, some of the offending language had been cleaned up to make it seem as if concessions were being made, but the results were much the same as under the Green Paper.29 The White Paper, which was the basis for the DMCA, was all about protecting the interest of the current content holders, and little or no thought was given to emerging businesses or to the public interest.30

This article focuses on the anti-circumvention provisions of the DMCA which had wide ranging implications which deserve more careful legislative consideration. Because a content owner could mix a little of his own work with work already in the public domain, and then protect the whole work with a technological protection-- which would be protected by the anti-circumvention provisions, the statute is overbroad. Under traditional First Amendment doctrine, overbreadth of a statute is reason for striking that statute down even when the statute is not overbroad as to a particular plaintiff.31 The statute offers language which looks like it may protect some traditional copyright privileges and defenses, stating that "nothing here should expand or restrict any First Amendment rights." However, the Second Circuit has labeled this language "clearly precatory," which in effect removes those traditional features of copyright law from application to the anti-circumvention and anti-trafficking provisions.32 When one considers the Constitutional mandate requiring that copyright be *limited* and intended only to *promote* progress, it is clear that at least the anti-circumvention provisions of the DMCA are overbroad. The question of whether these same provisions of the DMCA also violate First Amendment rights will be addressed in a later section.

I. INTRODUCTION OF CONCEPTS AND TERMS
A. Technical

Public awareness of the serious danger to citizens' First Amendment and privacy rights from the provisions of the DMCA is very low, largely because of the complexities of the issues involved. One of the first court decisions concerning the anti-circumvention provisions of the DMCA, *Universal City Studios, Inc. v. Reimerdes*, was almost one hundred pages long and contained two hundred seventy-nine footnotes.33 Judge Kaplan, District Judge from the Southern District of New York, even provided a table of contents for the decision.34 Although the legal issues are somewhat complicated, the initial barrier for many citizens is the language relating to technology and copyright.

First of all, it is important to note that the DMCA only protects digital media. Digital media, as the name implies, is any media that is stored in digital form, e.g., music on a compact disc (CD), word processing documents on the hard drive of a computer, movies on a digital virtual disk (DVD), or books in electronic, or eBook, form. The reason for this deferential treatment of digital media is that, compared to more traditional media, digital works are cheap and easy to copy. Furthermore, unlike traditional media, a copy of a digital work may be indistinguishable from the original, thus enabling an individual other than the copyright holder to create as many "perfect" copies as he or she desires.35

The anti-circumvention provisions of the DMCA are aimed at computer programs and other devices designed to circumvent technological protections installed by the copyright holder or his or her authorized distributor. Many of these protections involve some sort of encryption. Cryptography is the science of hidden writing.36 Encryption is the process of using cryptography to protect information, in this case to prevent the end-user of the copyrighted material from making any unauthorized use of

that material.37 Just as a lock that protects a safety deposit box requires a key to access the contents, an encrypted message requires a key to decrypt and view its contents. In the cryptographic sense of the word, a key is a string of characters and generally the longer the key, the more secure the encryption.

"Breaking" a cipher, or "cracking" an encryption scheme means getting around the encryption and returning the information to its unencrypted form. This can be accomplished in many ways-sometimes by determining the key, sometimes by devising a way around the encryption. Encryption is not the only method of protecting digital information, but it is one of the most discussed. Because it is easier to "crack" the encryption if one knows the content of the encrypted message, encryption alone is not the ideal method for perfect protection of known text such as a CD or a DVD. The DMCA makes clear that one can only be prosecuted for "circumvent[ing] a technological measure that *effectively* controls access to a work."38 Although this gave some researchers hope that their actions would be outside the scope of the DMCA, thus far, effective control has been found to mean any attempt to control access, no matter how weak the attempted control.39

Encryption programs, like all computer programs, are normally written by humans in *source code*, i.e., in a high level language with particularized grammar and syntax. This source code is then compiled or interpreted into object code, which is essentially a long string of 1's and 0's which can be read by a computer. As courts concur more frequently that all computer code is speech,40 the differences between these two types, or levels of code becomes less important. However, it is necessary to note these differences in order to understand the analysis contained in this note.

B. Copyright

In addition to the above technical items, there are some broad copyright terms and some specific DMCA provisions that are used in discussing these issues. In copyright, one significant defense or privilege to charges of copyright infringement is known as "fair use." Fair use is embodied in Title 17, Chapter 1, §107 of the traditional copyright law.41 Fair use is sometimes difficult to define precisely, but a few examples may help. If one owns a music CD and makes a copy of that CD for one's car, that is considered to be a "fair use" of something that you own. If one is a teacher and wishes to copy five pages of a several hundred page work for distribution to a class, that is considered to be "fair use." If one is reviewing a copyrighted work, quotes from that work may be included in the review without the author's permission, and that is considered to be "fair use."42 If one is parodying a work, and it is true parody, courts will generally consider that to be fair use as well.43 Fair use is "fair" even though the copyright holder does *not* grant any permission.44 Fair use is considered a constitutional requirement in that it balances the rights of the copyright owner with the citizens' interest in the free flow of information through the First Amendment. Although the DMCA specifically refers to the copyright code and says that doctrines such as fair use will remain, these exceptions generally have been read not to apply to violations of these anti-circumvention provisions.45

Another traditional copyright privilege is the doctrine of first sale.46 This doctrine provides that after buying a copyrighted product, (e.g., a book), one has the right to do with that book as one wishes-loan it to a friend, read it to a child, give it to the library or sell it to a used book store. The copyright holder has no control over the product after that "first sale." Once again, the DMCA has no provision for allowing the doctrine of first sale to continue in situations involving anti-circumvention devices. At least one commentator has referred to the fair use and first sale doctrines as "taxes" on the copyright holder.47

Because the DMCA creates such strict rules about the use of copyrighted digital media, in particular regarding that media which is protected by a technological anti-circumvention device, Congress realized that certain exceptions to the anti-circumvention provisions were required. However, these exceptions are extremely narrow and limited.48 There are several expressly stated exceptions to the anti-circumvention provisions that are available to the general public. The most significant exceptions for this discussion are: 1) Reverse engineering is excepted for the purpose of creating a compatible product;49 2) Encryption research is an exception;50 and 3) Security testing a system you own is also an exception.51

Although these exceptions have been asserted by programmers to apply in the cases below, courts have thus far refused to find that the defendants met the rigid qualifications of any of these exceptions. In *Reimerdes*, Eric Corley attempted to claim the reverse engineering and encryption research exception applied to his actions.52 The court concluded that Corley, as a publisher, did not meet the very narrow requirements.53 Although Edward Felten may have met the requirements for the encryption research exception, his case was different as shall be shown in the next section, in that Felten was the plaintiff, charging that his speech had been chilled by the threat of action under the DMCA.54

II. CASES
A. Universal City Studios, Inc. et al. v. Shawn C. Reimerdes, et al.55
i. Facts

Universal City Studios, Inc. (Universal), along with most distributors of motion pictures, distributes some movies in DVD (digital virtual disk) format.56 These DVDs are protected by an encryption system known as CSS.57 DVDs encrypted using CSS can only be viewed on players, either stand-alone players or computer drives, equipped with licensed decryption devices that allow for the user to play those DVDs.58

In 1999, Jon Johansen, a fifteen year old computer hacker from Norway, reverse engineered59 a licensed DVD player and successfully "broke" the CSS encryption scheme.60 Johansen and others have claimed that this was done as part of the international effort to make it possible to use DVDs in computers using the Linux operating system.61 At the time this case was brought, there was no licensed DVD player for the Linux operating system. This claim, however, was not very plausible.62 The decryption scheme created by Johansen, called DeCSS, was posted on multiple

websites, including co-defendant Eric Corley's hacker website, or "e-zine,"63 2600 ("Corley's website").64 When the motion picture industry became aware of the DeCSS presence on the Internet, it sent cease-and-desist letters to web sites posting the code.65 Some of those site operators complied.66 Corley's website, for example, removed the actual DeCSS code from its web site after the court granted plaintiff's uncontested preliminary injunction motion.67 However, in what was termed an act of "electronic civil disobedience," Eric Corley posted links on his website to other web sites that continued to offer DeCSS code.68

The district court decision in *Reimerdes* contained a fairly clear statement of the facts.69 Since the Second Circuit relied heavily on the district court opinion in its affirmation, a thorough review of the opinion is important to the understanding of the case and issues at hand.

The district court found Eric Corley to be an unsympathetic figure.70 With his long hair, tattered sports coat and sneakers, the court saw everything that it feared in a "hacker."71 It is obvious that, in the district court's view, defendant's act of posting the source and object code for DeCSS on his website was just another in a string of anti-establishment, quasi-illegal (or illegal) acts perpetrated by defendant.72 Nevertheless, the court engaged in a careful analysis of the issues raised in the case. As a threshold issue, the court was required to determine whether computer code is speech and thus deserving of First Amendment protection.

ii. Code as Speech
Universal requested that the court issue a permanent injunction against Corley's website to prevent it from posting DeCSS.73 The defendants argued that an injunction for this purpose would violate the Constitution's protection of free speech.74 Universal claimed that computer programs were not speech. Rather, it argued that DeCSS was the equivalent of a burglary tool-a "virtual crowbar" for breaking and entering onto its property, and was thus deserving of no more protection than any other burglary tool.75 Until recently, this argument might have prevailed. In *Bernstein v. U.S. Dept. of State*, the Ninth Circuit recognized that source code was speech.76 However, that opinion also stated that it was doubtful that object code was speech. Initially, in *Reimerdes*, the district court was prepared to side with plaintiffs on this issue and agree that computer programs were not speech, but David Touretzky, Carnegie Mellon Computer Science Professor, free speech advocate, and expert witness for the defense, claimed that "after I taught him to read a hex dump of a C program, he changed his mind."77 The district court stated that all computer programs are speech, whether stated in source code or object code.78 The court next needed to determine the level of protection to which this type of speech was entitled.

Defendants maintained that because code is expressive, it is entitled to strict scrutiny-the required level of judicial review of any challenge imposing a restriction on speech.79 Strict scrutiny requires a compelling government interest and a statute narrowly tailored to accomplish that government interest. Plaintiffs claimed that even if code is speech, it is also functional and that functionality requires that intermediate

scrutiny be used to test the DMCA.80 Intermediate scrutiny requires an "important" government interest and a "close" relationship between the means selected and the end achieved. This is a lower hurdle for the DMCA to overcome than strict scrutiny.

The district court found that, in a computer program, the functional element of the code outweighs any expressive element.81 While this is an interesting argument, it is ultimately unpersuasive. It could lead to the conclusion that if a program is not functional, it is not a threat, and deserves full expressive speech protection (for example, strict scrutiny applied to the DMCA's effect on speech).82 It is hard to believe (particularly for programmers) that liability would change based on whether the code is immediately functional or not, although this seems to be the test. Courts have determined that speech imminently leading to illegal action is unprotected.83 According to the district court, the fact that a program can be executed so quickly to create illegal action is sufficient for the court to deny that code the protection of strict scrutiny.84 However, this leads to absurd results (for example, instructions to make an illegal drug are not an illegal drug, and a picture of an automatic weapon is not an automatic weapon, they are both protected speech). But what about a listing of code? So far, courts seem to be saying that a picture of code is code. However, this is the whole point of David Touretzky's Gallery of DeCSS.85 At what point does this information become illegal under the DMCA as unprotected speech? How many mouse clicks or keystrokes away from functionality must the code be to no longer be code capable of imminent harm? The district court's reasoning does not explain where this line should be drawn, rather it merely finds that Corley's postings of DeCSS are too close to functionality, i.e. within too few mouse clicks of functionality to be protected speech.

Another First Amendment issue, largely ignored by both the plaintiffs and the court in this case, is that Corley is a media defendant. Corley had been publishing his website for 16 years.86 The original article listing the source and object code of DeCSS was just another article in Corley's magazine. That fact should have triggered the heightened First Amendment protection owed to the press. Corley's act of publishing the article on the Internet was no different from publishing in the brick and mortar world.87

iii. Content-Based vs. Content-Neutral Restrictions

In determining whether the statute should be analyzed under strict or intermediate scrutiny, one must refer to the purpose of the regulation. One must ask whether the regulation is content-based or content-neutral. A content-based regulation is evaluated under strict scrutiny because it is assumed that the government is attempting to restrict a certain message.88 This is viewed as antithetical to the free exchange of ideas necessary for a healthy democracy. A content-neutral regulation, however, is one that is applied to all speech without regard to the message. Content-neutral regulations of speech are often time, place and manner regulations (e.g., a regulation against using loudspeakers on residential streets). These content-neutral regulations are evaluated using an intermediate form of scrutiny as set forth in *United*

States v. O'Brien.89 This is not to say that the same message cannot be expressed, rather it must be expressed in a different manner. According to the district court in *Reimerdes*, "[g]iven the fact that DeCSS code is expressive, defendants would have the Court leap immediately to the conclusion that Section 1201(a)(2)'s prohibition on providing DeCSS necessarily is content based regulation of speech because it suppresses dissemination of a *particular kind of speech*."90 The court rejects defendants' argument and finds that the DMCA is content-neutral.91

The court was mistaken in finding that the content-neutral standard applied in Reimerdes. The DeCSS code is definitely expressive, and in many contexts, code is speech. Code can be used to state the existence of a fact. For example, "I have cracked the CSS protections on DVD's." That statement, without the code to back it up, proves nothing. It lacks the information necessary for others to determine whether there really was a crack, whether it was an effective crack, and how the crack occurred. Code can also be used to communicate a statement more effectively. For example, the statement "I have improved this encryption system by shortening the code to three lines in Perl" without the code offers very little information. However, with the code to provide proof and clarity, the statement can be tested and the improvement seen and judged.92 Since the code is expressive, a particular type of speech was being repressed by the statute, thus violating the strictures of the First Amendment.

iv. Traditional Copyright Defense-Fair Use.

As mentioned in Part II, fair use is a copyright term that has been interpreted in the past to be both a privilege and a defense. These interpretations differ in that a privilege can be exercised without much concern about court action, but a defense is only available after one has been charged with a violation. Fair use has been found to be a balancing element between the First Amendment and the copyright clause, both of which may be at odds with one another.93 In balancing these two constitutional provisions, it is important to recall that the copyright clause is the only clause granting legislative power that states its purpose and provides a built-in limitation. The framers were well aware of the abuses that could occur with government powers of copyright94 and therefore noted that the purpose of this grant of power was "to promote science and the useful arts."95 However, the copyright grants must be valid only "for a limited time."96 This language limiting purpose and time frame in the grant of exclusive rights must be balanced against the First Amendment. The First Amendment contains no such limitations, stating simply and eloquently that "[c]ongress shall make no law…abridging the freedom of speech."97 When the legislature starts ignoring the purposes and the limitations that were constitutionally mandated for copyright, it is imperative that the courts intervene to remind the legislature that the First Amendment protects certain basic values in our society, and trumps laws to the contrary.98

In *Reimerdes*, the defendants validly argued that without products such as DeCSS, those who wished to make what would otherwise be termed a fair use of the content of a legally purchased DVD cannot use the product in that way. The specific example argued most often in this case was that the DMCA makes it illegal for an

individual to purchase a DVD and then play that DVD on a computer running an open-source operating system in his or her own home.99 The court claims that DeCSS is not required to make a fair use of the work.100 Although there may exist a fair use privilege or defense for a professor to excerpt short scenes from a movie to show to her cinematography class, that privilege does not require that she be allowed to use the best, that is, digital, version of the work.101 Thus, shooting a video image of a television on which the DVD is playing is sufficient.102 Of course, if one thinks about the use here, it seems odd, since a cinematography class may learn little from the quality of print that would be available using this process. Defendants argue that this would require the user to go back to the "horse and buggy" version while the world moves rapidly ahead.103 However, the court in *Reimerdes* evidently found this to be a sufficient use.104

       v. Hyperlinks

       Aside from the regulation of the computer code, the other major First Amendment issue in *Reimerdes* was the injunction preventing the defendant from providing "hyperlinks" to sites providing DeCSS.105 Hyperlinks are embedded in the html106 code of web pages and by clicking on that hyperlink, a user may jump directly to another web site. These hyperlinks were provided so that the user could jump directly to the web sites of others who were providing DeCSS for download, often with just a click of a mouse to start downloading.107 Consequently, DeCSS is just one mouse click further away than if the code were posted for download on Corley's website itself. The court found that this did nothing to reduce the imminent harm presented by DeCSS.108 Corley's response was to change all the links that were listed on Corley's website to plain text statements of the address information for pages purporting to make DeCSS available.109

       Hyperlinks created a much more difficult problem for the court than the code itself. A link might lead to a web page that contains extensive information, which might just have a link to another page that only provides DeCSS. At what point is it sufficient to find the defendant liable for "trafficking?"

       The district court found that hyperlinks were also illegal under the DMCA and were not protected under the First Amendment. Hyperlinks were too close to operational, but in finding these links unprotected, the district court ignored the traditional "right to cite." It has been argued that a hypertext link is merely a citation to another source for the material.110 Thus, as a citation, a hypertext link is just another traditional piece of the First Amendment freedoms of speech and press, and should have been protected as a fair use. The court's failure to recognize this fair use opens a pandora's box of potential litigation involving online journalists who have cited to locations offering potentially illegal material. The court limits liability to those for whom clear and convincing evidence exists that 1) defendant knew "at the relevant time that the offending material" was on the linked-to site, 2) defendant knew that it was "a circumvention technology that may not lawfully be offered" and 3) the link was created or maintained "for the purpose of dissemination of that technology."111 These

limitations help limit the implications of the holding that hypertext links are not protected by the First Amendment, but leave a chilling effect on journalists, who must consider before every Internet publication whether their work will violate this test.

vi. Trial Court Holding

Consequently, the district court found that although computer programs are speech, they were deserving of the lower protections of intermediate scrutiny. Under that scrutiny, the court found that the government's important purpose in this instance was protecting copyrighted works stored on digital media from the vastly expanded risk of piracy in this electronic age.112 Judge Kaplan also found that the statute was narrowly tailored to achieve that interest and there was no violation of Corley's First Amendment rights.

The opinion yielded a mixed result for Corley's defense team. The opinion contained a strong statement that computer code was speech:

> It cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine. The path from idea to human language to source code to object code is a continuum. As one moves from one to the other, the levels of precision and, arguably, abstraction increase, as does the level of training necessary to discern the idea from the expression. … But each form expresses the same idea, albeit in different ways.113

This was a significant victory in the long fought battle to have computer code be declared speech.114 However that victory was severely tempered by the fact that Judge Kalan went on to find that as speech, code deserves very little protection.

vii. On Appeal - Corley v. Universal

The saga continued as defendants appealed and the Second Circuit heard oral arguments on May 1, 2001. Shortly after oral arguments, in what was viewed as a promising sign by advocates of free-speech on the Internet, the circuit submitted a list of questions to both parties that were directed at the free speech issues in the case.115 Both sides submitted reply briefs and the court issued its decision, written by Judge Newman, on November 28, 2001. The circuit court affirmed the district court's decision with many quotes from and praises for its reasoning.116 It must first be said that there are many affirmations of programmers' free speech rights in the Second Circuit's decision. The fact that code is assumed to be speech is definitely a positive development. Since the courts both highlight the fact that the target of the DMCA is not the expressive element of the speech, but the functional element of the speech, many (including plaintiff's expert Michael Shamos) believe that if the functional element was removed, then speech would be protected.117

The circuit court also recognized that a serious balancing had to be engaged in, weighing the copyright clause and the First Amendment when regulating hypertext links.118 The court went on to state that when courts are "considering First Amendment claims in the context of the pending case" they are obliged "to choose between two unattractive alternatives: either tolerate some impairment of communication in order to permit Congress to prohibit decryption that may lawfully be prevented, or tolerate some decryption in order to avoid some impairment of communication."119

At the same time, programmers' free speech rights took a blow when the appellate court declared that the language in 17 U.S.C. 1201(c)(4) is clearly prefatory, stating that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products" is clearly precatory, and thus did nothing to apply these traditional defenses and privileges to the anti-circumvention provisions.120

Eric Corley is not a sympathetic figure - there was an obvious lack of veracity in his dealings with the court. This led to reluctance on the courts' part in granting that his purposes might validly be protected. This in turn resulted in a case where both the district and circuit courts have said very favorable things concerning computer code as speech and yet found that that speech is not deserving of any real protection. Many advocates in the field believed that what was needed for free speech rights to prevail in this cyber world was a sympathetic figure with unquestionable motives to challenge the constitutionality of the anti-circumvention provisions of the DMCA. That figure soon appeared.

B. Edward Felten, et al. v. Recording Industry Association of America.121
i. Facts

On September 5, 2000, the Secure Digital Music Initiative (SDMI) issued a challenge to the computer community at large - crack the SDMI's proposed encryption schemes that were designed to protect music CDs.122 Princeton computer science professor Edward Felten and a group of colleagues did just that.123 The invitation allowed the user to access music protected with these proposed schemes after passing through a click-through agreement which provided that a successful cracker could be compensated up to $10,000 if he or she agreed to further terms.124 Those further terms included a requirement that the successful cracker would "not be permitted to disclose any information about the details of the attack to any other party," in other words, the paid successful cracker would lose his or her intellectual property rights.125 This portion of the click-through agreement also provided, importantly, that if the cracker elected "not to receive compensation" he or she would not be required to assign any of his or her intellectual property rights to the RIAA, "although [they were] still encouraged to submit details of [their] attack."126

Felten and his team of researchers successfully cracked five of the six technologies that were included in the challenge.127 They did not choose to collect any

compensation and entered no agreement to assign their rights to their work to the RIAA.128 Instead, they did what academic researchers do in furtherance of the scientific method: they attempted to publish a paper describing their research and their successful attacks and subject their findings to a peer review.129

In February, 2001, plaintiffs received word that their paper detailing these cracks of the SDMI information had been accepted for presentation at the Information Hiding Workshop (IHW) in Pittsburgh, Pennsylvania.130 The previous November, Professor Felten had been contacted by an executive at Verance, a defendant company which had created at least one of the protective technologies cracked by Felten's team.131 Felten discussed the paper with this executive, but did not send a copy of the paper until March 31, 2001, when a pre-publication copy was available.132 Felten specifically asked that the paper not be circulated outside of the company.133

Shortly thereafter, Felten received a letter from the Secretary of the SDMI Foundation and Senior Vice President of Business and Legal Affairs of the RIAA, Matthew Oppenheim, Esq., that discussed many issues. However, the pertinent fact was that unless the SDMI group had pre-publication review with veto power, the Foundation would sue under the DMCA.134 This condition was demanded despite the fact that the click-through agreement had specifically stated that the cracking-party would maintain his or her own intellectual property rights unless he or she accepted compensation for the feat.135 Although the RIAA would later claim that Dr. Felten's suit against it and the SDMI was inexplicable as "[the RIAA has] unequivocally and repeatedly stated that [RIAA has] no intention of bringing a lawsuit against Professor Felten or his colleagues,"136 the letter's threat to bring action in federal court clearly revealed a previous intent to at least use the threat of a suit under the DMCA to chill Professor Felten's speech. As a matter of fact, the IHW authorities and Professor Felten eventually decided to withdraw the SDMI paper from the proceedings to avoid litigation.137 On April 26, 2001, the date the SDMI paper was to have been presented, the RIAA and the SDMI issued a joint public statement that they had no intent to sue Professor Felten and his colleagues over the paper. Of course, at this point, the threat of the suit had already accomplished its purpose, *i.e.* Professor Felten's team had withdrawn their paper from the IHW conference and there was thus no need for the threat to be maintained.

On June 6, 2001, Felten and his fellow researchers, with the support of the Electronic Frontier Foundation (EFF),138 filed a law suit in the United States District Court for the District of New Jersey requesting an injunction enjoining the defendants from initiating any action against Felten and others for publishing the paper.139 At this point, the paper, with some improvements, had been accepted for the USENIX conference in Washington, D.C.140 Plaintiffs were seeking reassurance that they would not again be threatened with legal action for sharing their research results.

ii. Motion to Dismiss
Defendants, both the private defendants and the government, submitted motions to dismiss.141 They expressly avoided using mootness as a reason for this dismissal

because that would require that there had been a controversy at some point, which defendants deny. Instead, defendants contended that Felten's suit contained no adversity of interests and that plaintiffs lacked standing. The private defendants alleged that their threat of action was not action-they disregarded the chilling effect that the threat of action could have on researchers' speech. Essentially, the private defendants claimed that since they had provided assurances that they would not sue based on the specific papers involved in this suit (as long as there were no material changes in the content of those papers), there was no longer a controversy between the plaintiffs and the private defendants. However, in First Amendment cases, "an actual and well-founded *fear* that the law will be enforced against" plaintiffs is sufficient for the court to grant relief.142

iii. Standing
The classic case that describes the requirements for standing is *Lujan v. Defenders of Wildlife*.143 Based on Lujan, the three requirements to establish standing are 1) an injury in fact, 2) that is caused by the defendant, 3) which can be redressed by a favorable court decision.144 Standing requirements are relaxed in First Amendment cases where the threat of self-censorship creates harm without actual prosecution.145 In this case, plaintiffs correctly claimed that the necessary conditions are met for a finding of injury in fact.146

In First Amendment cases, a credible threat of litigation can serve as the injury in fact.147 Here, where the Felten team self-censored their research paper because the letter from the SDMI contained an explicit threat of prosecution under the DMCA, this prong of the test is met. Defendants claim that because they withdrew this particular threat, plaintiffs lacked standing.148 But since it is reasonable for plaintiffs to infer a continued threat from the existence of the defendant's prior threats149 as well as from defendant's unwillingness to disavow future litigation, this claim seems meritless. Because defendants refuse to waive future DMCA claims against Felten and his research team, there is continued adversity of the parties.

iv. No Adversity of Interests
The government's motion to dismiss focused on claims that the parties lacked adverse interests and that the court could not grant relief.150 The adverse interest claims were similar to those of the private defendants, but the courts' inability to grant relief was different. If the court could not grant relief, then the third prong of the *Lujan* test fails and the plaintiffs would lack standing.151 The government claimed that because the activities for which plaintiffs sought protective assurances were far too vague, the court would be unable to grant relief.152 The government also contended that because plaintiffs had not established that an injunction or lack thereof would alter their plans with respect to their future projects, "addressing Pintiff's [sic] claims would be of little practical utility to the parties."153

In response to the government's motion to dismiss, Felten's legal team countered that "[i]n this action, Plaintiffs raise three major claims against the Defendants: that DMCA violates the First Amendment on its face; that, as applied, DMCA violates Plaintiffs' First Amendment rights; and that Congress exceeded its constitutional

powers in enacting the DMCA. None of these requires significant further factual development."154 In particular, plaintiffs asserted that several of the projects that were either not being carried out or were on hold pending a ruling in this matter had been described in detail sufficient to satisfy a "live controversy" under the First Amendment.155 Plaintiffs further argued that the documents already before the court described with concrete detail the ways in which their plans for immediate and near-future projects would be affected by the court's ruling, thereby rejecting defendant's claim to the contrary.156

v. Hearing

On Wednesday, November 28, 2001, Judge Garrett Brown of the Federal District Court in Trenton, New Jersey held a hearing on defendants' motions to dismiss.157Although Judge Brown allowed some very brief oral comments on the motions, he appeared prepared to grant both RIAA's and the government's motions, which he did orally from prepared notes.158 He agreed with defendants that because the threat of litigation did not remain throughout the process, there was no threat at all.159 EFF has since stated that it intends to appeal the decision.160

Essentially, this ruling means that a large organization with equally large legal resources can censor a researcher by using the threat of a law suit under the DMCA and, after the researcher has relented, claim that it no longer wishes to prosecute. Under these circumstances, the court's decision in *Felten* leaves the researcher without the ability to seek redress.

C. Summary of Cases

Both *Felten* and *Reimerdes* bring to light troubling issues regarding the constitutionality of the DMCA's anti-circumvention and anti-trafficking provisions. These provisions, without any exceptions or exclusions to permit the traditional balancing between copyright law and the First Amendment, have a clear chilling effect on free speech and are unjustifiably broad. Both of these constitutional infirmities traditionally weigh in favor of rejecting a statute on First Amendment grounds.

The remaining problem is to determine an appropriate balance between the legislative desire to protect the interests of copyright holders and the national interest in maintaining the strength of the First Amendment which forms the cornerstone of the democratic freedoms enjoyed in the United States. Various approaches have been proposed for striking this balance; the following section considers several.

Part IV - Alternatives to the DMCA.

Because the anti-circumvention and anti-trafficking provisions of the DMCA can spawn such varied cases, it is difficult to tailor a comprehensive solution that addresses the issues arising in each case to the satisfaction of all parties involved. As the cases discussed above make clear, however, these provisions are chilling free speech and thus should be held to be unconstitutional. Although such a ruling might be criticized as creating a hole in the fabric of copyright protections that clothe content

owners, the reality is that these content owners are attempting to use their political influence to broaden their privileges under copyright law. Unfortunately, they are succeeding.

It is possible that the DMCA could be saved by broadening existing exceptions and allowing the traditional copyright privileges and defenses to apply to the anti-circumvention and anti-trafficking provisions. Although perhaps not the most ideal solution, this may be a politically feasible approach for balancing the interests involved. Many scholars have proposed interesting changes to copyright law that could be used to provide protection to digital works. Several of these changes are discussed briefly below.

As Lawrence Lessig points out in his seminal work, Code and Other Laws of Cyberspace, the technological controls that are implemented in the digital world can take the place of legislative action.161 However, to the extent these controls really take the place of legislative action, it must be realized that constitutional restraints may not be applied to the creators of such controls without modification of the traditional state action doctrine.162 As two commentators recently noted:

> Where technological constraints substitute for legal constraints, control over the design of information rights is shifted into the hands of private parties, who may or may not honor the public policies that animate public access doctrines such as fair use. Rights-holders can effectively write their own intellectual property statute in computer code. Moreover, to the extent that the DMCA appears to legitimate technological controls over copyrighted works, without regard to their effect on public policy, the statute effectively grants rubber-stamp approval to such private legislation.163

Noted digital copyright scholar Pamela Samuelson suggests that the DMCA should be interpreted only as an extension of current copyright law, *i.e.*, as a copyright infringement statute punishing only infringing activities.164 In particular, Samuelson observes that

> [a]n overly strict, technical reading of the DMCA would seriously threaten freedom of speech. It does so not only by ignoring the communicative aspects of writing and sharing computer code per se, but also by restricting activities [such as citations to encrypted works or to locations known to include illicit material] which … involve traditional forms of expressive activity.165

Samuelson also proposes that a broad "general purpose, 'or other legitimate purposes'" exception should be added to the DMCA to allow judicial interpretation of legitimate interests.166

In *Digital Copyright*, one of the first detailed works on the DMCA intended for the general public, copyright scholar and Wayne State University Law Professor Jessica Litman reminds readers that copyright was intended to be a bargain between the public

and a content-creator that would encourage the content-creator to generate more works.167 Litman proposes a radical change to copyright law - throw out the current law and replace it with a simple and easily understood statute that "recast[s] copyright as an exclusive right of commercial exploitation."168 Under this statute, making money from another's work or substantially interfering with a copyright holder's ability to make money would be actionable.169 However, neither the defeat of digital protections on a work for purposes of personal use nor the creation of tools for enabling others to make traditional fair use of a work would constitute a violation under the statute.

Professors Julie Cohen and Dan Burk propose a fascinating alternative that incorporates an expansion of copyright management systems to include default fair use rights, along with a key escrow mechanism.170 Under this approach, the default fair use rights would be governed by a set of rules that define what uses automatically constitute fair use.171 The key escrow mechanism would serve to address more difficult cases in which a desired use exceeds that permitted by the default rules. In these instances, a potential fair user would apply to a trusted third party who retains an alternate key to the protected work, such as the Library of Congress, and request permission to use the work in a specified manner.172 The trusted third party would then determine if the requested use was permissible and, if so, provide the escrowed key to unlock the protected work.173 Although Burk and Cohen identify several problems with this approach, it appears to provide a reasonable alternative for both sides of the bargain - greater protection is afforded to the content holder than he would otherwise realize with traditional media, and reasonable fair use rights for the individual citizen are preserved.174

David Touretzky, a Carnegie Mellon computer science professor and free speech advocate, suggests that the anti-circumvention and anti-trafficking provisions should simply be removed from the DMCA so that publishers can resort to traditional suits against the actual infringer (as opposed to the person providing a tool that may make it possible to infringe) for redress.175 Although this approach may prove difficult in a digital world where information travels quickly, Touretzky validly maintains that the loss of a few dollars by content holders is preferable to the loss of long-standing constitutional rights by citizens.

Conclusion

Although several of Corley's defenses asserted in *Reimerdes* may appear reasonable on their surface, it is unlikely that a court will entertain arguments of overbreadth and vagueness on behalf of such unappealing defendants. Furthermore, although it may be argued that Corley's posting allowed fair use - users of the Linux operating system could now use DVDs on their computers - the fact that DeCSS was originally created and distributed in the Windows operating system diminishes the forcefulness of this argument. Corley's freedom of the press argument was largely ignored by both courts, and once again, the courts may well be falling victim to prejudice. A more sympathetic defendant may be key to a finding of traditional press privileges.

The chilling effect that the DMCA had on Professor Felten's exercise of free speech could be lessened by adopting one of the alternatives discussed above. The same things that made Felten a good plaintiff in a law suit against the DMCA - the fact that he was engaged in legitimate research and was dissuaded from dispersing the results of that research by an outside threat - also made it easier for the court to find no controversy in that case. Professor Felten was engaged in legitimate research that provided a societal benefit: making digital media protections stronger and more protective of their content. The recording industry quickly realized that the threat of a lawsuit against Felten was a mistake, since a court would be more likely to find that the anti-circumvention and anti-trafficking provisions of the DMCA were unconstitutional when confronted with a sympathetic plaintiff rather than a quasi-criminal figure like Eric Corley. The recording industry did their best to claim that there was never any controversy between themselves and Professor Felten so that the court would not rule adversely to the DMCA, a statute which they had lobbied long and hard to achieve and was extraordinarily protective of their intellectual property rights. Although Judge Brown sided with defendants, it seems likely that a reviewing court will recognize the error of this reasoning and rule purely on the constitutionality of the DMCA. It is hoped that in reaching their decision, the court will refute the arguments of defendants who attempt to reap more protection from the copyright bargain than the constitutional grant was intended to provide.

There is a criminal case working its way through the system that demonstrates the dangers of the anti-trafficking provisions. In July 2001, Adobe Systems tipped off the FBI that Dmitry Sklyarov, a Russian citizen, was guilty of violating the anti-trafficking provision of the DMCA in the course of his employment with ElcomSoft.176 Sklyarov had found a way to circumvent the protections on Adobe's eBook technology.177 This circumvention would allow an authorized user to make a copy, or to have the book read aloud if that option had been turned off on a particular eBook.178 Russian copyright law allows for a legitimate owner to make a back-up copy of a digital work.179 Sklyarov came to the United States to deliver a talk at a convention regarding the weaknesses of the eBook format.180 He was arrested before he was given the opportunity to give that presentation.181

After protests and public pressure began to mount, Adobe chose to drop the charges.182 However, the federal government continued to keep Sklyarov in this country, although they released him on bail on the condition that he remain in Northern California.183 In December, 2001, charges against Sklyarov were dropped as he served as a focus for protests against the Justice Department in this action.184 Charges have not been dropped against Elcomsoft, Sklyarov's employer.185 The prosecution is continuing, with hearings on various motions scheduled for March and April 2002.186

The fact that the DMCA gives United States officials the ability to jail a foreign citizen for coming to this country to give a *lecture* demonstrates a flaw in the system. Freedom of speech is a cornerstone of democracy and Sklyarov had broken no laws in Russia. Enforcement of this strict interpretation of provisions originally designed to extend copyright rules has led to international warnings for technical programmers to

avoid the United States and to technical conferences moving to other countries for the safety of their members.187 Either courts need to recognize that the chilling effect of these anti-circumvention and anti-trafficking provisions far outweighs any societal benefit they may have or Congress needs to address the issue with amendments or revisions to the DMCA. In either case, the current situation is an intolerable twisting of law into the form of copyright and First Amendment law, which has ignored the constitutional restrictions on both.

*Amy E. McCall, J.D. Expected 2003, Duquesne University

FN1 Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998), (codified in Title 17).

FN2 17 U.S.C. § 1201(a) (2000).

FN3 17 U.S.C. § 1201(a)(2) (2000).
No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-
(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
(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 this title; or
(C) is marketed by that person, or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.
17 U.S.C. § 1201(b) (2000).
ADDITIONAL VIOLATIONS.-(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof. (2) As used in this subsection-(A) "to circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and (B) a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a copyright owner under this title.

FN4 The statute provides for civil remedies in 17 U.S.C. § 1203, which states that "any person injured by a violation of § 1201… may bring a civil action" in which the judge

may award actual or statutory damages as well as attorney fees and may impound any "device or product" that the court reasonably believes was used in the violation. 17 U.S.C. § 1203. Criminal offenses are handled in 17 U.S.C. § 1204 which provides that willful violations of 1201 are subject to a fine of not more than $500,000 and a prison term of not more than 5 years, or both for the first offense and double that for subsequent offenses. 17 U.S.C. § 1204(a)-(c) (2000).

FN5 Because this area of legislation is really beyond copyright, some commentators have called this "paracopyright." The Hon. Tom Bliley (R-VA, now retired) noted in extended remarks for the record:
      As proposed by the Clinton Administration, however, the anti-circumvention provisions to implement the WIPO treaties would have represented a radical departure from this tradition. In a September 16, 1997 letter to Congress, 62 distinguished law professors expressed their concern about the implications of regulating devices through proposed section 1201. They said in relevant part: `[E]nactment of Section 1201 would represent an unprecedented departure into the zone of what might be called *paracopyright*--an uncharted new domain of legislative provisions designed to strengthen copyright protection by regulating conduct which traditionally has fallen outside the regulatory sphere of intellectual property law.
      The Hon. Tom Bliley, Excerpt from Comment made October 12, 1998, Digital Future Coalition, at http://www.dfc.org/dfc1/Archives/wipo/bliley_full_comments.html [emphasis added].

FN6 *See* JESSICA LITMAN, DIGITAL COPYRIGHT 91-95 (2001).

FN7 *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981 (1996); ACM (Association for Computer Machinery), *Computer Professionals concerned DMCA stifles Academic Freedom And Speech*, at http://www.acm.org/usacm/IP/DMCA-release.html.

FN8 Universal City Studios, Inc. v. Remierdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000), *aff'd by* Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001).

FN9 Felten v. RIAA, No. CV-01-2669 (D.N.J. 2001), *available at* http://www.eff.org/legal/Cases/Felten_v_RIAA.

FN10 SIVA VAIDHYANATHAN, COPYRIGHTS AND COPYWRONGS: THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY 37, (2001).

FN11 Litman, *supra* note 6, at 15.

FN12 Pamela Samuelson, *Copyright Grab*, Wired Archive 4.01, 36 (Jan. 1996), at http://www.wired.com/wired/archive/4.01/white.paper_pr.html.

FN13 U.S. CONST. art. I, § 8, cl. 8.

FN14 *Id.* (emphasis added).

FN15 LITMAN, *supra* note 6, at 13.

FN16 *Id.* at 23.

FN17 *Id.*

FN18 VAIDHYANATHAN, *supra* note 10, at 35.

FN19 Timeline: A History of Copyright in the U.S., at
http://arl.cni.org/info/frn/copy/timeline.html (last modified Aug. 2, 2002).

FN20 *Id.*

FN21 About WIPO: The Beginning, (visited 1/3/02), *at* http://www.wipo.int/about-
wipo/en/gib.htm.

FN22 LAWRENCE LESSIG, THE FUTURE OF IDEAS n.26, ch. 6, 293-94 (Random
House) (2001).

FN23 The United States signed the WIPO treaty on April 12, 1997 and the treaty was
ratified on October 28, 1998. WIPO Copyright Treat, S. Treaty Doc. No. 105-17, 105th
Cong., 1st Sess. (1997), 1997 WL 447232.

FN24 In terms of anti-circumvention, the treaty requires party-states to "provide
adequate legal protection and effective legal remedies against the circumvention of
effective technological measures… that restrict acts … which are not authorized by the
authors concerned or permitted by law." *Id.*

FN25 See Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the
Anti-Circumvention Regulations Need to be Revised*, 14 BERKELY TECH. L.J. 519,
529-533 (1999).

FN26 LITMAN, *supra* note 6, at 90.

FN27 See Samuelson, *supra* note 12.

FN28 LITMAN, *supra* note 6, at 91.

FN29 See *Id.* at 94-96.

FN30 See Samuelson, *supra* note 25 at 530-31.

FN31 GEOFFREY R. STONE, ET AL., CONSTITUTIONAL LAW 1176 (3d ed.
1996), *citing* U.S. v. Raines, 362 U.S. 17 (1960); Barrows v. Jackson, 346 U.S. 249

(1953); and *Note: Standing to Assert Constitutional Jus Tertii*, 88 HARV. L. REV. 423 (1974).

FN32 Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001).

FN33 111 F. Supp. 2d. 294 (S.D.N.Y. 2000).

FN34 *Id.*

FN35 Compare a cassette tape of an LP record to a song in MP3 format. The cassette will not be of the quality that the original recording was, and each successive copy will be degraded even more. Also, there is a transaction, or media, cost for each copy. The song in MP3 format (or translated into MP3 format from a CD) can be sent across the Internet to a friend without any degradation in quality and with little or no realized cost (there are costs associated with the internet connection and with the storage space, but since these costs are often considered fixed, the additional use for this purpose may not add cost in the users mind). Additionally, successive copies can be made in that same method with no degradation in quality.

FN36 SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY, QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY 6 (1999).

FN37 *See* SSH Communications Security, *Introduction to Cryptography*, *at* http://www.ssh.fi/tech/crypto/intro.html. This is a very simplified explanation of the protection methods used - encryption was only a small piece of the picture.

FN38 17 U.S.C. § 1201(a) (2000) (emphasis added).

FN39 Note that Jon Johanson, who first cracked CSS was 15 at the time and not an experienced cryptoanalyst. *Reimerdes*, 111 F. Supp. 2d at 311.

FN40 *See* Bernstein v. U.S. Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996) *rev'd sub nom.* Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999); DVD Copy Control Ass'n v. Bunner, 113 Cal. Rptr. 2d 338 (2001); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000); Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

FN41 17 U.S.C. § 107 (2002). Limitations on exclusive rights: Fair use Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies of phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include-
(A) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(B) the nature of the copyrighted work;
(C) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
(D) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

FN42 LESSIG, *supra* note 22, at 181.

FN43 *See* Campbell v. Acuff Rose Music, Inc., 510 U.S. 569 (1994).

FN44LESSIG, *supra* note 22, at 105.

FN4517 U.S.C. § 1201(c)(1) (2000) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.").

FN46 17 U.S.C. § 109(a) (2002) ("Notwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.").

FN47 Keith Aoki, Symposium: *Sovereignty and the Globalization of Intellectual Property: Neocolonialism, Anticommons Property, and Biopiracy in the (Not-So-Brave) New World Order of International Intellectual Property Protection*, 6 Ind. J. Global Leg. Stud. 11, 15 (1998).

FN48 17 U.S.C. § 1201(e) (provides an exception for law enforcement and government activities, but not for the general public).

FN49 17 U.S.C. § 1201(f) (2000).

FN50 17 U.S.C. § 1201(g) (2000).

FN51 17 U.S.C. § 1201(j) (2000).

FN52 *Reimerdes*, 111 F. Supp. 2d at 319-20.

FN53 *Id.* at 320.

FN54 Plaintiffs' Complaint, Felten, No. CV-01-2669 (D.N.J. filed June 6, 2001), *available at* http://www.eff.org/legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

FN55 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

FN56 *Id.* at 303.

FN57 *Id.*

FN58 *Id.*

FN59 Software reverse engineering involves reversing a program's machine code (the string of 0s and 1s that are sent to the logic processor) back into the source code that it was written in, using program language statements. Software reverse engineering is done to retrieve the source code of a program because the source code was lost, to study how the program performs certain operations, to improve the performance of a program, to fix a bug (correct an error in the program when the source code is not available), to identify malicious content in a program such as a virus, or to adapt a program written for use with one microprocessor for use with a differently-designed microprocessor.
IT Encyclopedia at Whatis.com, *at*
http://whatis.techtarget.com/definition/0,,sid9_gci507015,00.html. (last visited Nov. 9, 2002).

FN60 *Reimerdes*, 111 F. Supp. 2d at 311.

FN61 Linux is an operating system (based on AT&T's Unix operating system) that was developed as part of what is known as the open source movement. Open source means that the source code for Linux and all Linux derivatives must be available. It does not have to be free, but the source code will be available for any end user to modify. Those modifications must also be available for the open source community. Jon Johansen claimed to be part of a group called MoRE (Masters of Reverse Engineering), which "is/was a group of individuals in Norway and Germany who were directly responsible for the 'cracking' of the CSS scrambling algorithm. To this date the only member of the group identified by name is Jon Johansen, the author of DeCSS." The Openlaw DVD/DeCSS Forum Frequently Asked Questions (FAQ) List 1.4.4. *at*
http://eon.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html. (last modified May 3, 2000).

FN62 *See Id.* § 1.2.1. According to the FAQ at the Harvard openlaw site (operated by a community which is cosponsoring Johansen's defense) there is no evidence that this was accomplished as part of the organized effort to crack the CSS scheme and create the ability for a Linux player. Johansen did contribute this code to the Linux "LiViD" effort after it was complete.

FN63 This term refers to an electronic magazine.

FN64 *Reimerdes*, 111 F. Supp. 2d at 312. 2600 can be found on the web at http://www.2600.com/.

FN65 *Id.*

FN66 *Id.*

FN67 Universal Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

FN68 *Reimerdes*, 111 F. Supp. 2d at 303-04.

FN69 *Id.*

FN70 Lisa M. Bowman, *Putting a kind face on copyright battles*, CNET (5/2/01) *at* http://news.com.com/2100-1023-256912.html?legacy=cnet.

FN71 *Id.* The court goes to great lengths to describe Corley's previous acts that make him a bad character - his magazine has published articles on how to steal an Internet domain name, how to break into computer systems and a guide to the criminal justice system for readers charged with computer hacking. *Reimerdes*, 111 F. Supp. 2d at 308-09.

FN72 Defendant Eric Corley is viewed as a leader of the computer hacker community and goes by the name Emmanuel Goldstein, after the leader of the underground in George Orwell's classic, 1984. He and his company, defendant 2600 Enterprises, Inc., together publish a magazine called 2600: The Hacker Quarterly, which Corley founded in 1984, and which is something of a bible to the hacker community. The name "2600" was derived from the fact that hackers in the 1960's found that the transmission of a 2600 hertz tone over a long distance trunk connection gained access to "operator mode" and allowed the user to explore aspects of the telephone system that were not otherwise accessible. Mr. Corley chose the name because he regarded it as a 'mystical thing,' commemorating something that he evidently admired. Not surprisingly, 2600: *The Hacker Quarterly* has included articles on such topics as how to steal an Internet domain name, access other people's e-mail, intercept cellular phone calls, and break into the computer systems at Costco stores and Federal Express. One issue contains a guide to the federal criminal justice system for readers charged with computer hacking…
Reimerdes, 111 F. Supp. 2d at 308-09. The listing of these issues in the body of the opinion seems to indicate that the character of the defendant affected the outcome of the opinion.
Professor Dan Burk of the University of Minnesota School of Law commented, "As soon as the judge says 'hacker,' you know you've lost." Bowman, *supra* note 70.

FN73 *Reimerdes*, 111 F. Supp. 2d at 343.

FN74 *Id.* at 325-26.

FN75 Brief for Intervenor United States at 19, *Reimerdes* 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (00-9185).

FN76 Bernstein v. United States Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997) *vacated, scheduled for reh'g en banc, then in light of new regulations, remanded back to district court*.

FN77 David Touretzky, Remarks at A Great Debate: Are Computer Programs Protected Speech? Computer Immigration Series at Carnegie Mellon University School of Computer Science (Nov. 30, 2001). "C" is a computer programming language and a "hex dump" is a listing of numbers in base-16 (hexidecimal) that tells what was in all the computer registers, the stack and other selected information at the time of an error. David Touretzky is a Principal Scientist at the School of Computer Science at Carnegie Mellon University and a long-time advocate of free-speech rights on the Internet. His web gallery of DeCSS has subjected him to legal challenges of his own. He notes that that web gallery is mentioned in both court opinions in this case (the District Court and the Circuit Court) but that both refused to comment on the legal issues involved because "they realize that it's a tar pit and they don't wish to get pulled into it. But I'm going to pull them in." *Id.* Touretzky, DS (2000) Gallery of CSS Descramblers, *available at* http://www.cs.cmu.edu/~dst/DeCSS/Gallery (Jan. 3, 2002).

FN78 Additionally, the assumption that defendants are making should not be overlooked here. There is an implicit assumption in their argument (and since some of this argument prevailed it is worth some serious worry) that the DVD remains theirs to do with as they wish even after a consumer has purchased it. If DeCSS is a "crowbar" even if it's not used to do anything illegal, then we must assume that the thing being pried open belongs to the complainant.

FN79 *Reimerdes*, 111 F. Supp. 2d at 327.

FN80 Appellate Reply Brief of Movie Industry Plaintiffs-Appellee, Universal v. Reimerdes, 111.F. Supp. 2d 294 (S.D.N.Y. 2000) (No. 00-9185).

FN81 Judge Kaplan notes that "[g]iven the fact that DeCSS code is expressive, defendants would have the Court leap immediately to the conclusion that Section 1201(a)(2)'s prohibition on providing DeCSS necessarily is content based regulation of speech because it suppresses dissemination of a particular kind of expression." *See* 111 F. Supp. 2d at 328 (citing portions of Defendant's Post-Trial Memorandum).

FN82 Plaintiff's expert, Micheal Shamos Ph.D., J.D., who serves as Co-Director for Carnegie Mellon University's Institution for eCommerce and as Special counsel for Reed Smith, L.L.P., has stated that if the computer code is not functional, or if the code is described in words, even words that the audience could then turn into effective DeCSS code, that would be protected speech and the DMCA could not reach that. Michael I. Shamos, Remarks at A Great Debate: Are Computer Programs Protected Speech? Computer Immigration Series at Carnegie Mellon University School of Computer Science (Nov. 30, 2001).

FN83 Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

FN84 111 F. Supp. 2d at 332-33. The District Court further made note of the fact that the only human interaction required to perform the illegal act was a single mouse click. That single mouse click was not sufficient insulation from the imminent harm to provide protection for the speech. *See id.* at 331-34.

FN85 *See supra* note 75.

FN86 Declaration of Emmanuel Goldstein, Universal Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001) (00-0277).

FN87 *See* Banco Nacionale de Mexico v. Narco News et al., Index No. 603429/00 (N.Y. App. Div. Dec. 5, 2001) *available at* http://www.eff.org/Cases/BNM_v_Narco_News/20011205_decision.html (applied higher standard for proof of defamation from New York Times v. Sullivan to online journalists). "Brick and mortar world" is the term commonly used by those who function in both the online world and that "brick and mortar world" to differentiate between the two.

FN88 *See* Yates v. United States, 354 U.S. 298 (1957).

FN89 United States v. O'Brien, 391 U.S. 367 (1968). The court will uphold a content-neutral regulation of speech if "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." *Turner quoting O'Brien as stated in Reimerdes.*

FN90 (emphasis added).

FN91 *Reimerdes*, 111 F. Supp. 2d at 329. A literal reading of the Constitution shows this dichotomy, the copyright clause provides that Congress must make laws to protect authors which will limit speech of others while the First Amendment provides that Congress shall make NO law restricting the freedom of speech. U.S. CONST. art. I, §8, cl. 8; U.S. CONST. amend. I.

FN92 Programmers have worked for a number of years to create the shortest version of a workable form of the RSA encryption algorithm (one of the strongest encryption systems currently available). The current winner is the following 3-line Perl script which fits simply on a business card and can be entered into any computer that can interpret the programming language Perl:
```
#!/bin/perl -sp0777i<X+d*1Mla^*1N%0]dsXx++1M1N/dsM0<j]dsj
$/=unpack('H*',$_);$_='echo 16dio\U$k"SK$/SM$n\EsN0p[1N*1
1K[d2%Sa2/d0$^Ixp"|dc`;s/\W//g;$_=pack('H*',/((..)*)$/)
```
The quest for the most diminutive munitions program, at http://www.cypherspace.org/~adam/rsa/story.html. RSA has been declared to be

ammunitions by the federal government, although that status is not necessarily applicable any longer. The distribution of this code is still arguably illegal.

FN93 "[C]opyright's idea/expression dichotomy [and thus fair use] '[strikes] a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression.'" Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1984).

FN94 VAIDHYANATHAN, *supra* note 10, at 37.
Thomas Jefferson was an outspoken proponent of limiting terms of absolute monopoly for ideas. In what may be the most famous example of this, he said:
If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea, which an individual may exclusively possess as long as he keeps it to himself; but the moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it. he who receives an idea from me, receives instruction himself without lessening min; as he who lites his taper at mine, receives light without darkening me. That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation.
Letter from Thomas Jefferson to Isaac McPherson (August 13, 1813), in *The Writings of Thomas Jefferson* 6 (H. A. Washington, ed., 1861), 175, 180.

FN95 U.S. CONST. art. I, §8, cl. 8.

FN96 *Id.*

FN97 U.S. CONST. amend. 1.

FN98 LESSIG, *supra* note 21, at 188:
If copyright law must protect fair use-meaning the law cannot protect copyrighted material without leaving space for fair use-then laws protecting code protecting copyrighted material should also leave room for fair use. You can't do indirectly (protect fair-use-denying-code protecting copyright) what you can't do directly (protect copyright without protecting fair use.
Id.
On the other hand, on the House floor, Sonny Bono's widow (and replacement in the U.S. House of Representatives) said:
Copyright term extension is a very fitting memorial for Sonny. This is not only because of his experience as a pioneer in the music and television industries. The most important reason for me was that he was a legislator who understood the delicate balance of the constitutional interests at stake. Last year he sponsored the term

extension bill, H.R. 1621, in conjunction with Sen. Hatch. He was active on intellectual property issues because he truly understood the goals of Framers of the Constitution: that by maximizing the incentives for original creation, we help expand the public store-house of art, films music, books and now also, software. It is said that "it all starts with a song," and these works have defined our culture to audiences world-wide. Actually, Sonny wanted the term of copyright protection to last forever. I am informed by staff that such a change would violate the Constitution. I invite all of you to work with me to strengthen our copyright laws in all of the ways available to us. As you know, there is also Jack Valenti's proposal for term to last forever less one day. Perhaps the Committee may look at that next Congress.

Statement of Mary Bono, (R-Cal), 144 Cong Rec H 9946, 9951 (1998).

As Lawerence Lessig has pointed out, forever is forever, even if it is minus one day or five days, or five years. (The reason for the Mickey Mouse moniker is that some commentators have pointed out that every time the copyright is about to run out on Mickey Mouse, Congress lengthens the copyright term.).

LESSIG, *supra* note 22, at 107.

FN99 An open-source operating system (the most prevalent example is Linux) is an operating system for which the code is provided. There is no secret as to how these operating systems run, it is shared knowledge and anyone can update their own system and offer those systems to others. As a matter of fact, in some versions of open source licensing, if you make a change to the operating system, you are required by the license to provide those changes to the open-source community. Although DVD players were available for the Windows and Macintosh operating systems, at the time of this case, there was no licensed DVD player for Linux.

FN100 *Reimerdes*, 111 F. Supp 2d at 337-338. The court also notes that had Congress intended for the fair use exception to apply to the anti-circumvention provisions, that would have been clear in the statute. *Id.* at 324.

FN101 *Id.* at 337.

FN102 *Id.* at 338.

FN103 *Id.*

FN104 *Id.* at 321-323.

FN105 *Reimerdes*, 111 F. Supp. 2d at 340.

FN106 "Html" stands for hyper text markup language which is the programming language used for World Wide Web applications.

FN107 *Id.* at 325.

FN108 The basic argument here is that a program is somehow different from instructions to make LSD because the program can be executed with too little human effort. Somehow the courts seem to be saying that the fact that there is little human effort involved in running a program makes it somehow so that the humans are not responsible. This seems spurious at best-the mantra of programmers has become much like the mantra of the NRA, "Guns don't kill people, people kill people." That is, "Programs don't infringe copyrights, people infringe copyright." Just because little human effort is required to run the program that may infringe someone's copyright does not mean that the computer can run the program by itself. And programmers are talking about speech-something which enjoys a clearly preferential status under the United States Constitution.

FN109 One of the examples used by the court is what if a newspaper article had a link to a site that provided DeCSS as part of a story about this issue? Could that be enjoined from being printed? See Banco Nacional de Mexico, S.A. v. Mario Renato Menèndez Rodriques, Al Giordano and The Narco News Bulletin (N.Y. Sup. Ct. Dec. 5, 2001) *available at* http://www.eff.org/Cases/BNM_v_Narco_News/20011205_decision.html.

FN110 See LITMAN, *supra* note 6, at 183.

FN111 *Reimerdes*, 111 F. Supp. 2d at 341.

FN112 *Id.* at 329.

FN113 *Id.* at 326.

FN114 Cindy Cohn, who began her battle with this issue with the Daniel Bernstein case in 1995, was also involved in this case for the EFF. This has been a long battle for some.

FN115 Those questions were:
1. Are the anti-trafficking provisions of the Digital Millennium Copyright Act content-neutral? See 111 F. Supp. 2d 294, 328-29 (S.D.N.Y. 2000).
2. Does DeCSS have both speech and non-speech elements?
3. Does the dissemination of DeCSS have both speech and non-speech elements?
4. Does the use of DeCSS to decrypt an encrypted DVD have both speech and non-speech elements?
5. Does the existence of non-speech elements, along with speech elements, in an activity sought to be regulated alone justify intermediate level scrutiny?
6. If DeCSS or its dissemination or its use to decrypt has both speech and non-speech elements and is not subject to intermediate level scrutiny simply because of the non-speech elements, is intermediate level scrutiny appropriate because of the close causal link between dissemination of DeCSS and its improper use? See 111 F. Supp. 2d at 331-32.
7. If the District Court is correct that the dissemination of DeCSS "carries very substantial risk of imminent harm" 111 F. Supp. 2d at 332, does that risk alone justify

the injunction? In other words, does that risk satisfy the requirements for regulating speech under Brandenburg v. Ohio, 395 U.S. 444 (1969), thereby rendering unnecessary an inquiry as to whether non-speech elements of DeCSS or its dissemination or its use (if such exists) may be regulated under *United States v. O'Brien*, 391 U.S. 367 (1968)?

8. Are the three criteria identified at 111 P. Supp. 2d 333 the correct criteria for determining the validity, under intermediate level scrutiny, of the use of DeCSS that has been enjoined?

9. If not, what modification or supplementation would be required to conform to First Amendment requirements?

10. Are the three criteria identified in 111 F. Supp. 2d 341 and the "clear and convincing evidence" standard the correct criteria and the correct standard of proof for testing the validity of the injunction's prohibition of posting on the defendant's website and of linking?

If not, what modification or supplementation would be required to conform to First Amendment requirements?

available at
http://www.eff.org/IP/Video/MPAA_DVD_cases/20010508_ny_augment_order.html.

FN116 Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

FN117 Micheal Shamos, Remarks at A Great Debate: Are Computer Programs Protected Speech? at the Computer Immigration Series at Carnegie Mellon University School of Computer Science (Nov. 30, 2001). Also note - there are programs that now can take computer code and turn it into simple English and vice versa. It will not be long before computers can read English, at that point, may we suppress all language on the view that it is functional? There are even t-shirt versions of DeCSS which are definitely non-functional. (See http://www.copyleft.net - Copyleft has been named as a defendant in DVD Copy Control Ass'n v. Bunner, 93 Cal. App. 4th 648, (2001), charging infringement of trade secrets).

FN118 Corley, 273 F.3d 429, 458 (2d Cir. 2001).

FN119 *Id.*

FN120 *Id.* at 32.

FN121 Civil Action No. CV-01-2669 (D.N.J. filed June 6, 2001), *available at* http://www.eff.org/legal/Cases/Felten_v_RIAA.

FN122 The invitation said, in part:
Here's an invitation to show off your skills, make some money, and help shape the future of the online digital music economy.
The Secure Digital Music Initiative [SDMI] is a multi-industry initiative working to develop a secure framework for the digital distribution of music. SDMI protected

content will be embedded with an inaudible, robust watermark or use other technology that is designed to prevent the unauthorized copying, sharing, and use of digital music. We are now in the process of testing the technologies that will allow these protections. The proposed technologies must pass several stringent tests: they must be inaudible, robust, and run efficiently on various platforms, including PCs. They should also be tested by you.
So here's the invitation: Attack the proposed technologies. Crack them.
By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt.
Plaintiff's Complaint at 32, Felten v. RIAA (No. CV-01-2669) *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

FN123 Professor Felten's research includes analyzing and improving various Internet security protocols. Felten testified as an expert witness for the defendant in the *Reimerdes* case and for the government in the anti-trust case against Microsoft. Frequently Asked Questions about Felten & USENIX v. RIAA Legal Case, *at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/faq_felten.html.

FN124 Plaintiff's Complaint at 32, Felten v. RIAA (No. CV-01-2669) *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

FN125 *Id.*

FN126 *Id.*

FN127 *Id.* at item 37.

FN128 *Id.*

FN129 *Id.*

FN130 *Id.* at item 38.

FN131 *Id.* at item 39.

FN132 *Id.*

FN133 *Id.* at 40.

FN134 RIAA/SDMI Legal Threat Letter, *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html. In pertinent part, the letter stated:
In addition, because the public disclosure of your research would be outside the limited authorization of the Agreement [the click-through agreement discussed above], you could be *subject to enforcement actions under federal law, including the DMCA*. The Agreement specifically preserves any rights that proponents of the technology being

attacked may have "under any applicable law including, without limitation, the U.S. Digital Millennium Copyright Act, for any acts not expressly authorized by this Agreement." The Agreement simply does not "expressly authorize" participants to disclose information and research developed through participation in the Public Challenge and thus such disclosure could be the subject of a DMCA action. (emphasis added).

FN135 Plaintiff's Complaint at 32, Felten v. RIAA (No. CV-01-2669).

FN136 Statement by RIAA's Cary Sherman on Felten Lawsuit (June 6, 2001), *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_riaa_statement.html.

FN137 Plaintiff's Complaint at 2, Felten v. RIAA (No. CV-01-2669).

FN138 The Electronic Frontier Foundation (EFF) was founded in 1990 to "protect our fundamental rights regardless of technology, to educate the press, policymakers, and the general public about civil liberties issues related to technology…" EFF web site, *available at* http://www.eff.org/abouteff.html.

FN139 Plaintiff's Complaint at G, Felten v. RIAA (No. CV-01-2669).

FN140 *Id.* at 50.
USENIX is the Advanced Computing Systems Association. Since 1975 the USENIX Association has brought together the community of engineers, system administrators, scientists, and technicians working on the cutting edge of the computing world. The USENIX conferences have become the essential meeting grounds for the presentation and discussion of the most advanced information on the developments of all aspects of computing systems. The USENIX Association and its members are dedicated to:
" problem-solving with a practical bias,
" fostering innovation and research that works,
" communicating rapidly the results of both research and innovation,
" providing a neutral forum for the exercise of critical thought and the airing of technical issues.
from the USENIX web site, *available at* http://www.usenix.org/.

FN141 Defendant RIAA's Memorandum in Support of Motion to Dismiss, Felten v. RIAA, No. CV-01-2669 (July 12, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010712_riaa_mtd_memo.html. Defendant John Ashcroft's memorandum in Support of Motion to Dismiss, Felten v. RIAA, No. CV-01-2669 (Sept. 25, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010925_doj_dismiss_motion_memo. html.

Fn142 *Virginia v. American Booksellers Ass'n, Inc*., 484 U.S. 383, 393 (1988) (emphasis added).

FN143 504 U.S. 555, 560-561 (1992).

FN144 *Id.*

FN145 *ACLU v. Miller*, 977 F.Supp. 1228, 1231 (N.D. Ga. 1997); *Virginia v. American Booksellers*, 484 U.S. 383 (1988); *Waters v. Barry*, 711 F.Supp. 1125 (D.C.D.C. 1989).

FN146 Plaintiffs' Brief in Opposition to RIAA's Motion to Dismiss at 19, *Felten v. RIAA,* No. CV-01-2669 (Aug. 13, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_eff_felten_brief.html.

FN147 *American Booksellers Ass'n*, 484 U.S. at 393; Babbitt v. United Farm Workers, 442 U.S. 289, 298 (1979); New Hampshire Right to Life Political Action Comm. v. Gardner, 99 F.3d 8, 13 (1st Cir. 1996).

FN148 Defendant RIAA's Memorandum in Support of Motion to Dismiss at 20-23, *Felten v. RIAA,* No. CV-01-2669 (July 12, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010712_riaa_mtd_memo.html.

FN149 "Past threats of enforcement are evidence 'bearing on whether there is a real and immediate threat of repeated injury.'" Opposition Brief, *Felten v. RIAA*, No. CV-01-2669 (Aug. 13, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011025_eff_felten_opp_brief.rtf (quoting O'Shea v. Littleton, 414 U.S. 488, 496 (1974)).

FN150 Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss at 1, *Felten*, (No. CV-01-2669).

FN151 *Id.* at 18.

FN152 *Id.* at 20-23.

FN153 *Id.* at 23.

FN154 Plaintiff's Brief in Opposition to Defendant John Ashcroft's Motion to Dismiss at 17-18 (footnote omitted), *Felten* (No. CV-01-2669 (GEB)).

FN155 Id. at 19-20.

FN156 Id. at 21-22.

FN157 Transcript of Motions Before Honorable Garrett E. Brown, United States District Court Judge, *Felten v. RIAA*, No. CV-01-2669 (Nov. 28, 2001) *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011128_hearing_transcript.html.

FN158 *Id.*

FN159 *Id.* at 30.

FN160 Judge Denies Scientists' Free Speech Rights, EFF Press Release (Nov. 28, 2001) *at* http://www.eff.org/effector/HTML/effect14.37/html.

FN161 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 135 (1999).

FN162 For an interesting discussion of reasons for removing the state action doctrine because of these technological actions, see, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. Rev. 354 (1999).

FN163 Dan L. Burk and Julie Cohen, *Fair Use Infrastructure for Copyright Management Systems*, 15 HARV. J.L. & TECH. 41 (2001). Key escrow is a system often discussed with encryption systems. The basic tenet is that the key for particular works would be provided to a trusted party. That party would hold the key until it had reason to provide it to another. For an excellent explanation of the subject, *see*, Michael Froomkin, *It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 1996 U. CHI. LEGAL F. 15 (1995).

FN164 Declaration of Pamela Samuelson at 7, *Corley* (No.Civ. 00-0277).

FN165 *Id.* at 15. *See also*, Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, SCIENCE, Sept. 14, 2001, at 1018.

FN166 Samuelson, *supra* note 25, at 524.

FN167 LITMAN, *supra* note 6.

FN168 *Id.* at 180.

FN169 *Id.*

FN170 Burk & Cohen, *supra* note 160, at 65.

FN171 *Id.*

FN172 *Id.* at 66.

FN173 *Id.*

FN174 *Id.* at 68.

FN175 David Touretzky, Remarks at A Great Debate: Are Computer Programs Protected Speech, *supra* note 77.

FN176 Criminal Complaint, United States v. Sklyarov, No. 5-02-257 (N.D. Ca. filed June 26, 2001).

FN177 *Id.*

FN178 Lawrence Lessig, *Jail Time in the Digital Age at* http://www.eff.org/IP/DMCA/US_v_Sklyarov/20010730_lessig_oped.html (July 30, 2001).

FN179 *Id.*; *See also* Associated Press, Adobe Hacker off Hook in Russia, Wired News *at* http://www.wired.com/news/politics/0,1283,45966,00.html (Aug. 9, 2001).

FN180 *See* Jennifer Lee, *Russian in Digital Copyright Case Is Released on Bail*, N.Y. TIMES, Aug. 7, 2001, at C4, *available at* http://www.nytimes.com/2001/08/07/technology/07HACK.html.

FN181 *Id.*

FN182 *See* Declan McCullagh, Sklyarov Release in Feds Hands, WIRED NEWS July 24, 2001, *at* http://www.wired.com/news/politics/0,1283,45484,00.html.

FN183 *See* Lee, *supra* note 177.

FN184 *See* Jennifer Lee, In Digital Copyright Case, Programmer Can Go Home, December 14, 2001, N.Y. TIMES, *available at* http://www.nytimes.com/2001/12/14/technology/14HACK.html

FN185 *Id.*

FN186 *See* Press Release, U.S. Attorney (N.D. Cal.) On Dropping of Charges Against Dmitry Sklyarov (Dec. 13, 2001), *available at* http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20011213_usatty_pr.html.

FN187 *See* Press Release, Electronic Frontier Foundation, Judge Denies Scientists' Free Speech Rights (Nov. 28, 2001) *available at* http://www.eff.org/effector/HTML/effect14.37.html#I.