UNIVERSAL CITY STUDIOS, INC. v. ERIC CORLEY

273 F.3d 429 (2nd Cir. 2001)

20 Jon O. Newman, Circuit Judge.

21 When the Framers of the First Amendment prohibited Congress from making any law "abridging the freedom of speech," they were not thinking about computers, computer programs, or the Internet. But neither were they thinking about radio, television, or movies. Just as the inventions at the beginning and middle of the 20th century presented new First Amendment issues, so does the cyber revolution at the end of that century. This appeal raises significant First Amendment issues concerning one aspect of computer technology—encryption to protect materials in digital form from unauthorized access. The appeal challenges the constitutionality of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 et seq. (Supp. V 1999) and the validity of an injunction entered to enforce the DMCA.

22 Defendant-Appellant Eric C. Corley and his company, 2600 Enterprises, Inc., (collectively "Corley," "the Defendants," or "the Appellants") appeal from the amended final judgment of the United States District Court for the Southern District of New York (Lewis A. Kaplan, District Judge), entered August 23, 2000, enjoining them from various actions concerning a decryption program known as "DeCSS." Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000) ("Universal II"). The injunction primarily bars the Appellants from posting DeCSS on their web site and from knowingly linking [435] their web site to any other web site on which DeCSS is posted. Id. at 346-47. We affirm.

Introduction

24 Understanding the pending appeal and the issues it raises requires some familiarity with technical aspects of computers and computer software, especially software called "digital versatile disks" or "DVDs," which are optical media storage devices currently designed to contain movies.[1] Those lacking such familiarity will be greatly aided by reading Judge Kaplan's extremely lucid opinion, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) ("Universal I"), beginning with his helpful section "The Vocabulary of this Case," [...]

25 This appeal concerns the anti-trafficking provisions of the DMCA, which Congress enacted in 1998 to strengthen copyright protection in the digital age. Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied. The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections. In so doing, Congress targeted not only those pirates who would circumvent these digital walls (the "anti-circumvention provisions," contained in 17 U.S.C. § 1201(a)(1)), but also anyone who would traffic in a technology primarily designed to circumvent a digital wall (the "anti-trafficking provisions," contained in 17 U.S.C. § 1201(a)(2), (b)(1)).

26 Corley publishes a print magazine and maintains an affiliated web site geared towards "hackers," a digital-era term often applied to those interested in techniques for circumventing protections of computers and computer data from unauthorized access. The so-called hacker community includes serious computer-science scholars conducting research on protection techniques, computer buffs intrigued by the challenge of trying to circumvent access-limiting devices or perhaps hoping to promote security by exposing flaws in protection techniques, mischief-makers interested in disrupting computer operations, and thieves, including copyright infringers who want to acquire copyrighted material (for personal use or resale) without paying for it.

27 In November 1999, Corley posted a copy of the decryption computer program "DeCSS" on his web site, http://www.2600.com ("2600.com").[2] DeCSS is designed to circumvent "CSS," the encryption technology [436] that motion picture studios place on DVDs to prevent the unauthorized viewing and copying of motion pictures. Corley also posted on his web site links to other web sites where DeCSS could be found.

28 Plaintiffs-Appellees are eight motion picture studios that brought an action in the Southern District of New York seeking injunctive relief against Corley under the DMCA. Following a full non-jury trial, the District Court entered a permanent injunction barring Corley from posting DeCSS on his web site or from knowingly linking via a hyperlink to any other web site containing DeCSS. [...]The District Court rejected Corley's constitutional attacks on the statute and the injunction.[...]

29 Corley renews his constitutional challenges on appeal. Specifically, he argues primarily that: (1) the DMCA oversteps limits in the Copyright Clause on the duration of copyright protection; (2) the DMCA as applied to his dissemination of DeCSS violates the First Amendment because computer code is "speech" entitled to full First Amendment protection and the DMCA fails to survive the exacting scrutiny accorded statutes that regulate "speech"; and (3) the DMCA violates the First Amendment and the Copyright Clause by unduly obstructing the "fair use" of copyrighted materials. Corley also argues that the statute is susceptible to, and should therefore be given, a narrow interpretation that avoids alleged constitutional objections.

Background

31 For decades, motion picture studios have made movies available for viewing at home in what is called "analog" format. Movies in this format are placed on videotapes, which can be played on a video cassette recorder ("VCR"). In the early 1990s, the studios began to consider the possibility of distributing movies in digital form as well. Movies in digital form are placed on disks, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, i.e., one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. This case arises out of the movie industry's efforts to respond to this risk by invoking the anti-trafficking provisions of the DMCA.

I. CSS

33 The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula. Decryption in the case of CSS requires a set of "player keys" [437] contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

34 The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

35 With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997, and DVDs quickly gained in popularity, becoming a significant source of studio revenue.[3] In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

II. DeCSS

37 In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system.[...] That program was called, appropriately enough, "DeCSS."

38 If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS

will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-CSS-compliant player and copied, manipulated, and transferred just like any [438] other computer file.[5] DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. Universal I, 111 F. Supp. 2d at 308, 313. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).[6]

39 Johansen posted the executable object code, but not the source code, for DeCSS on his web site. The distinction between source code and object code is relevant to this case, so a brief explanation is warranted. A computer responds to electrical charges, the presence or absence of which [439] is represented by strings of 1's and 0's. Strictly speaking, "object code" consists of those 1's and 0's.[...]While some people can read and program in object code, "it would be inconvenient, inefficient and, for most people, probably impossible to do so."[...]Computer languages have been written to facilitate program writing and reading. A program in such a computer language—BASIC, C, and Java are examples—is said to be written in "source code." Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. This task is usually performed by a program called a compiler. Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans.[...] Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code. [...]

40 In November 1999, Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, 2600: The Hacker Quarterly, which Corley has been publishing since 1984.[7] As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users—such as threats to online privacy—the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems. Representative articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express.[...]

41 Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, . . . [y]ou have to show your evidence . . . and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence . . . we have" that there is in fact technology that circumvents CSS.[...]Writing about DeCSS without including the DeCSS code would have

been, to Corley, "analogous to printing a story about a picture and not printing the picture."[...]Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.[...]

42 2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to many of these sites. These efforts met with only partial success; a number of sites refused to remove [440] DeCSS. In January 2000, the studios filed this lawsuit.[8]

III. The DMCA

44 The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty"), which requires contracting parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law." [...]Even before the treaty, Congress had been devoting attention to the problems faced by copyright enforcement in the digital age. Hearings on the topic have spanned several years. See, e.g., WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. (1997); NII Copyright Protection Act of 1995: Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 104th Cong. (1996); NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary and the Senate Comm. on the Judiciary, 104th Cong. (1995); H.R. Rep. No. 105-551 (1998); S. Rep. No. 105-190 (1998). This legislative effort resulted in the DMCA.

45 The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision.[9] This provision prohibits a person from "circumvent[ing] a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]." The Librarian of Congress is required to promulgate regulations every three years exempting from this subsection individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses." 17 U.S.C. § 1201(a)(1)(B)-(E).

46 The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides:

47 > 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 [441] that effectively controls access to a work protected under this title.

48 Id. § 1201(a)(2). To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work . . . or otherwise to . . . bypass . . . a technological measure, without the authority of the copyright owner." Id. § 1201(a)(3)(A).

49 Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure that effectively controls access to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who traffic in technology that can circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner under" Title 17.[...] In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to prevent access to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to permit access to a work but prevent copying of the work or some other act that infringes a copyright.[...]Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

50 The DMCA contains exceptions for schools and libraries that want to use circumvention technologies to determine whether to purchase a copyrighted product, 17 U.S.C. § 1201(d); individuals using circumvention technology "for the sole purpose" of trying to achieve "interoperability" of computer programs through reverse-engineering, id. § 1201(f); encryption research aimed at identifying flaws in encryption technology, if the research is conducted to advance the state of knowledge in the field, id. § 1201(g); and several other exceptions not relevant here.

51 The DMCA creates civil remedies, id. § 1203, and criminal sanctions, id. § 1204. It specifically authorizes a court to "grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation." Id. § 1203(b)(1).

IV. Procedural History

53 Invoking subsection 1203(b)(1), the Plaintiffs sought an injunction against the Defendants, alleging that the Defendants violated the anti-trafficking provisions of the statute. On January 20, 2000, after a hearing, the District Court issued a preliminary injunction barring the Defendants from posting DeCSS.[...]

54 The Defendants complied with the preliminary injunction, but continued to post links to other web sites carrying DeCSS, an action they termed "electronic civil disobedience."[...]Under the heading "Stop the MPAA [(Motion Picture Association of

America)]," Corley urged other web sites to post DeCSS lest "we . . . be forced into submission."[...]

55 The Plaintiffs then sought a permanent injunction barring the Defendants from both posting DeCSS and linking to sites containing DeCSS. After a trial on the merits, the Court issued a comprehensive opinion, Universal I, and granted a permanent injunction, Universal II.

56 The Court explained that the Defendants' posting of DeCSS on their web site clearly falls within section 1201(a)(2)(A) of the DMCA, rejecting as spurious their claim that CSS is not a technological measure that "effectively controls access to a [442] work" because it was so easily penetrated by Johansen, [...]and as irrelevant their contention that DeCSS was designed to create a Linux-platform DVD player, [...] The Court also held that the Defendants cannot avail themselves of any of the DMCA's exceptions, [...] and that the alleged importance of DeCSS to certain fair uses of encrypted copyrighted material was immaterial to their statutory liability,[...] The Court went on to hold that when the Defendants "proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks" on their site, they were trafficking in DeCSS, and therefore liable for their linking as well as their posting.[...]

57 Turning to the Defendants' numerous constitutional arguments, the Court first held that computer code like DeCSS is "speech" that is "protected" (in the sense of "covered") by the First Amendment,[...]but that because the DMCA is targeting the "functional" aspect of that speech,[...] it is "content neutral,"[...] and the intermediate scrutiny of United States v. O'Brien, 391 U.S. 367, 377 (1968), applies, [...] The Court concluded that the DMCA survives this scrutiny, id. at 330-33, and also rejected prior restraint, overbreadth, and vagueness challenges,[...]

58 The Court upheld the constitutionality of the DMCA's application to linking on similar grounds: linking, the Court concluded, is "speech," but the DMCA is content-neutral, targeting only the functional components of that speech. Therefore, its application to linking is also evaluated under O'Brien, and, thus evaluated, survives intermediate scrutiny. However, the Court concluded that a blanket proscription on linking would create a risk of chilling legitimate linking on the web. The Court therefore crafted a restrictive test for linking liability (discussed below) that it believed sufficiently mitigated that risk. The Court then found its test satisfied in this case. [...]

59 Finally, the Court concluded that an injunction was highly appropriate in this case. The Court observed that DeCSS was harming the Plaintiffs, not only because they were now exposed to the possibility of piracy and therefore were obliged to develop costly new safeguards for DVDs, but also because, even if there was only indirect evidence that DeCSS availability actually facilitated DVD piracy,[11] the threat of piracy was very real, particularly as Internet transmission speeds continue to increase.[...]Acknowledging that DeCSS was (and still is) widely available on the Internet, the Court expressed confidence in

60 > the likelihood . . . that this decision will serve notice on others that "the strong right arm of equity" may be brought to bear against them absent a change in their

> conduct and thus contribute to a climate of appropriate respect for intellectual property rights in an age in which the excitement of ready access to [443] untold quantities of information has blurred in some minds the fact that taking what is not yours and not freely offered to you is stealing.[...]

62 The Court's injunction barred the Defendants from: "posting on any Internet web site" DeCSS; "in any other way . . . offering to the public, providing, or otherwise trafficking in DeCSS"; violating the anti-trafficking provisions of the DMCA in any other manner, and finally "knowingly linking any Internet web site operated by them to any other web site containing DeCSS, or knowingly maintaining any such link, for the purpose of disseminating DeCSS."[...]

63 The Appellants have appealed from the permanent injunction. The United States has intervened in support of the constitutionality of the DMCA. We have also had the benefit of a number of amicus curiae briefs, supporting and opposing the District Court's judgment. After oral argument, we invited the parties to submit responses to a series of specific questions, and we have received helpful responses.

Discussion

I. Narrow Construction to Avoid Constitutional Doubt

66 The Appellants first argue that, because their constitutional arguments are at least substantial, we should interpret the statute narrowly so as to avoid constitutional problems. They identify three different instances of alleged ambiguity in the statute that they claim provide an opportunity for such a narrow interpretation.

67 First, they contend that subsection 1201(c)(1), which provides that "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title," can be read to allow the circumvention of encryption technology protecting copyrighted material when the material will be put to "fair uses" exempt from copyright liability.[12] We disagree that subsection 1201(c)(1) permits such a reading. Instead, it[...]simply clarifies that the DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred. Subsection 1201(c)(1) ensures that the DMCA is not read to prohibit the "fair use" of information just because that information was obtained in a manner made illegal by the DMCA. The Appellants' much more expansive interpretation of subsection 1201(c)(1) is not only outside the range of plausible readings of the provision, but is also clearly refuted by the statute's legislative history.[13] [...]

68 Second, the Appellants urge a narrow construction of the DMCA because of subsection 1201(c)(4), which provides 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." This language is clearly precatory: Congress could not "diminish" constitutional rights of free speech even if it wished to, and the fact that Congress also expressed a reluctance to "enlarge" those rights cuts against the Appellants' effort to infer a narrowing construction of the Act from this

provision.

69 Third, the Appellants argue that an individual who buys a DVD has the "authority of the copyright owner" to view the DVD, and therefore is exempted from the DMCA pursuant to subsection 1201(a)(3)(A) when the buyer circumvents an encryption technology in order to view the DVD on a competing platform (such as Linux). The basic flaw in this argument is that it misreads subsection 1201(a)(3)(A). That provision exempts from liability those who would "decrypt" an encrypted DVD with the authority of a copyright owner, not those who would "view" a DVD with the authority of a copyright owner.[14] In any event, the Defendants offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms.[15]

70 We conclude that the anti-trafficking and anti-circumvention provisions of the DMCA are not susceptible to the narrow interpretations urged by the Appellants. We therefore proceed to consider the Appellants' constitutional claims.

II. Constitutional Challenge Based on the Copyright Clause

72 In a footnote to their brief, the Appellants appear to contend that the DMCA, as construed by the District Court, exceeds the constitutional authority [445] of Congress to grant authors copyrights for a "limited time," U.S. Const. art. I, § 8, cl. 8, because it "empower[s] copyright owners to effectively secure perpetual protection by mixing public domain works with copyrighted materials, then locking both up with technological protection measures."[...]This argument is elaborated in the amici curiae brief filed by Prof. Julie E. Cohen on behalf of herself and 45 other intellectual property law professors.[...] For two reasons, the argument provides no basis for disturbing the judgment of the District Court.

73 First, we have repeatedly ruled that arguments presented to us only in a footnote are not entitled to appellate consideration.[...]Although an amicus brief can be helpful in elaborating issues properly presented by the parties, it is normally not a method for injecting new issues into an appeal, at least in cases where the parties are competently represented by counsel.[...]

74 Second, to whatever extent the argument might have merit at some future time in a case with a properly developed record, the argument is entirely premature and speculative at this time on this record. There is not even a claim, much less evidence, that any Plaintiff has sought to prevent copying of public domain works, or that the injunction prevents the Defendants from copying such works. As Judge Kaplan noted, the possibility that encryption would preclude access to public domain works "does not yet appear to be a problem, although it may emerge as one in the future."[...]

III. Constitutional Challenges Based on the First Amendment

A. Applicable Principles

77 Last year, in one of our Court's first forays into First Amendment law in the digital age, we took an "evolutionary" approach to the task of tailoring familiar constitutional rules to

novel technological circumstances, favoring "narrow" holdings that would permit the law to mature on a "case-by-case" basis. See Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 584 n.11 (2d Cir. 2000). In that spirit, we proceed, with appropriate caution, to consider the Appellants' First Amendment challenges by analyzing a series of preliminary issues the resolution of which provides a basis for adjudicating the specific objections to the DMCA and its application to DeCSS. These issues, which we consider only to the extent necessary to resolve the pending appeal, are whether computer code is speech, whether computer programs are speech, the scope of First Amendment protection for computer code, and the scope of First Amendment protection for decryption code. Based on our analysis of these issues, we then consider the Appellants' challenge to the injunction's provisions concerning posting and linking.

78 **1. Code as Speech**

79 Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," i.e., symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone [446] chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. [...] Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language.[...]

80 **2. Computer Programs as Speech**

81 Of course, computer code is not likely to be the language in which a work of literature is written. Instead, it is primarily the language for programs executable by a computer. These programs are essentially instructions to a computer. In general, programs may give instructions either to perform a task or series of tasks when initiated by a single (or double) click of a mouse or, once a program is operational ("launched"), to manipulate data that the user enters into the computer.[16] Whether computer code that gives a computer instructions is "speech" within the meaning of the First Amendment requires consideration of the scope of the Constitution's protection of speech.

82 The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech. . . ." U.S. Const. amend. I. "Speech" is an elusive term, and judges and scholars have debated its bounds for two centuries. Some would confine First Amendment protection to political speech.[...]Others would extend it further to artistic expression.[...]

83 Whatever might be the merits of these and other approaches, the law has not been so

limited. Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection. [...]

84 Thus, for example, courts have subjected to First Amendment scrutiny restrictions on the dissemination of technical scientific information, [...]and scientific research,[...]and attempts to regulate the publication of instructions[...]

85 Computer programs are not exempted from the category of First Amendment speech simply because their instructions require use of a computer. A recipe is no less "speech" because it calls for the use of an oven, and a musical score is no less "speech" because it specifies performance on an electric guitar. Arguably distinguishing computer programs from conventional language instructions is the fact that programs are executable on a computer. But the fact that a program has the capacity to direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions "speech" for purposes of the First Amendment.[19] The information [448] conveyed by most "instructions" is how to perform a task.

86 Instructions such as computer code, which are intended to be executable by a computer, will often convey information capable of comprehension and assessment by a human being.[20] A programmer reading a program learns information about instructing a computer, and might use this information to improve personal programming skills and perhaps the craft of programming. Moreover, programmers communicating ideas to one another almost inevitably communicate in code, much as musicians use notes.[21] Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars,[22] just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).[...]

90 For all of these reasons, we join the other courts that have concluded that computer code, and computer programs constructed from code can merit First Amendment protection,[...]

91 **3. The Scope of First Amendment Protection for Computer Code**

92 Having concluded that computer code conveying information is "speech" [450] within the meaning of the First Amendment, we next consider, to a limited extent, the scope of the protection that code enjoys. As the District Court recognized, Universal I, 111 F. Supp. 2d at 327, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available.[...] A content-neutral restriction is permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored, which "in this context requires . . . that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" [...]

93 "[G]overnment regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech."[...]"The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others."[...]The Supreme Court's approach to determining content-neutrality appears to be applicable whether what is regulated is expression,[...]conduct, [...] or any "activity" that can be said to combine speech and non-speech elements,[...]

94 To determine whether regulation of computer code is content-neutral, the initial inquiry must be whether the regulated activity is "sufficiently imbued with elements of communication to fall within the scope of the First . . . Amendment[]." [...]Computer code, as we have noted, often conveys information comprehensible to human beings, even as it also directs a computer to perform various functions. Once a speech component [451] is identified, the inquiry then proceeds to whether the regulation is "justified without reference to the content of regulated speech." [...]

95 The Appellants vigorously reject the idea that computer code can be regulated according to any different standard than that applicable to pure speech, i.e., speech that lacks a nonspeech component. Although recognizing that code is a series of instructions to a computer, they argue that code is no different, for First Amendment purposes, than blueprints that instruct an engineer or recipes that instruct a cook.[...] We disagree. Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements.[...]

96 We recognize, as did Judge Kaplan, that the functional capability of computer code cannot yield a result until a human being decides to insert the disk containing the code into a computer and causes it to perform its function (or programs a computer to cause the code to perform its function). Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe. Judge Kaplan, in a passage that merits extensive quotation, cogently explained why this is especially so with respect to decryption code:

97 > [T]he focus on functionality in order to determine the level of scrutiny is not an inevitable consequence of the speech-conduct distinction. Conduct has immediate effects on the environment. Computer code, on the other hand, no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really "a proxy for effects or harm" and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.

> The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.
>
> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass security measures, [452] some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used. And that is not all.
>
> There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source.
>
> In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.. . . . .
>
> These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Causation in the law ultimately involves practical policy judgments. Here, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

98 [...]The functionality of computer code properly affects the scope of its First Amendment protection.

99 **4. The Scope of First Amendment Protection for Decryption Code**

100 In considering the scope of First Amendment protection for a decryption program like DeCSS, we must recognize that the essential purpose of encryption code is to prevent unauthorized access. Owners of all property rights are entitled to prohibit access to their property by unauthorized persons. Homeowners can install locks on the doors of their

houses. Custodians of valuables can place them in safes. Stores can attach to products security devices that will activate alarms if the products are taken away without purchase. These and similar security devices can be circumvented. Burglars can use skeleton keys to open door locks. Thieves can obtain the combinations to safes. Product security devices can be neutralized.

101 Our case concerns a security device, CSS computer code, that prevents access by unauthorized persons to DVD movies. The CSS code is embedded in the DVD movie. Access to the movie cannot be obtained unless a person has a device, a licensed DVD player, equipped with computer code capable of decrypting the CSS encryption code. In its basic function, [453] CSS is like a lock on a homeowner's door, a combination of a safe, or a security device attached to a store's products.

102 DeCSS is computer code that can decrypt CSS. In its basic function, it is like a skeleton key that can open a locked door, a combination that can open a safe, or a device that can neutralize the security device attached to a store's products.[27] DeCSS enables anyone to gain access to a DVD movie without using a DVD player.

103 The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD. However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales. The advent of the Internet creates the potential for instantaneous worldwide distribution of the copied material.

104 At first glance, one might think that Congress has as much authority to regulate the distribution of computer code to decrypt DVD movies as it has to regulate distribution of skeleton keys, combinations to safes, or devices to neutralize store product security devices. However, despite the evident legitimacy of protection against unauthorized access to DVD movies, just like any other property, regulation of decryption code like DeCSS is challenged in this case because DeCSS differs from a skeleton key in one important respect: it not only is capable of performing the function of unlocking the encrypted DVD movie, it also is a form of communication, albeit written in a language not understood by the general public. As a communication, the DeCSS code has a claim to being "speech," and as "speech," it has a claim to being protected by the First Amendment. But just as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized—indeed, unlawful—access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its First Amendment protection.[...]

105 With all of the foregoing considerations in mind, we next consider the Appellants' First Amendment challenge to the DMCA as applied in the specific prohibitions that have been imposed by the District Court's injunction.

B. First Amendment Challenge

107 The District Court's injunction applies the DMCA to the Defendants by imposing two types of prohibition, both grounded on the anti-trafficking provisions of the DMCA. The first prohibits posting DeCSS or any other technology for circumventing CSS on any Internet web site.[...]The second prohibits knowingly linking any Internet web site to any other web site containing DeCSS. [...]The validity of the posting and linking prohibitions must be considered separately.

108 1. Posting

109 The initial issue is whether the posting prohibition is content-neutral, since, as we have explained, this classification [454] determines the applicable constitutional standard. The Appellants contend that the anti-trafficking provisions of the DMCA and their application by means of the posting prohibition of the injunction are content-based. They argue that the provisions "specifically target . . . scientific expression based on the particular topic addressed by that expression—namely, techniques for circumventing CSS."[...]. We disagree. The Appellants' argument fails to recognize that the target of the posting provisions of the injunction—DeCSS—has both a nonspeech and a speech component, and that the DMCA, as applied to the Appellants, and the posting prohibition of the injunction target only the nonspeech component. Neither the DMCA nor the posting prohibition is concerned with whatever capacity DeCSS might have for conveying information to a human being, and that capacity, as previously explained, is what arguably creates a speech component of the decryption code. The DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional capability is not speech within the meaning of the First Amendment. The Government seeks to "justif[y],"[...]both the application of the DMCA and the posting prohibition to the Appellants solely on the basis of the functional capability of DeCSS to instruct a computer to decrypt CSS, i.e., "without reference to the content of the regulated speech," id. This type of regulation is therefore content-neutral, just as would be a restriction on trafficking in skeleton keys identified because of their capacity to unlock jail cells, even though some of the keys happened to bear a slogan or other legend that qualified as a speech component.

110 As a content-neutral regulation with an incidental effect on a speech component, the regulation must serve a substantial governmental interest, the interest must be unrelated to the suppression of free expression, and the incidental restriction on speech must not burden substantially more speech than is necessary to further that interest.[...]The Government's interest in preventing unauthorized access to encrypted copyrighted material is unquestionably substantial, and the regulation of DeCSS by the posting prohibition plainly serves that interest. Moreover, that interest is unrelated to the suppression of free expression. The injunction regulates the posting of DeCSS, regardless of whether DeCSS code contains any information comprehensible by human beings that would qualify as speech. Whether the incidental regulation on speech burdens substantially more speech than is necessary to further the interest in preventing unauthorized access to copyrighted materials requires some elaboration.

111 Posting DeCSS on the Appellants' web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet, and such person can then instantly transmit DeCSS to anyone else with Internet access. Although the prohibition on posting prevents the Appellants from conveying to others the speech component of DeCSS, the Appellants have not suggested, much less shown, any technique for barring them from making this instantaneous worldwide distribution of a decryption code that makes a lesser restriction on the code's speech component.[28] It is true that the [455] Government has alternative means of prohibiting unauthorized access to copyrighted materials. For example, it can create criminal and civil liability for those who gain unauthorized access, and thus it can be argued that the restriction on posting DeCSS is not absolutely necessary to preventing unauthorized access to copyrighted materials. But a content-neutral regulation need not employ the least restrictive means of accomplishing the governmental objective. Id. It need only avoid burdening "substantially more speech than is necessary to further the government's legitimate interests."[...]The prohibition on the Defendants' posting of DeCSS satisfies that standard.[29]

112 **2. Linking**

113 In considering linking, we need to clarify the sense in which the injunction prohibits such activity. Although the injunction defines several terms, it does not define "linking." Nevertheless, it is evident from the District Court's opinion that it is concerned with "hyperlinks," [...] A hyperlink is a cross-reference (in a distinctive font or color) appearing on one web page that, when activated by the point-and-click of a mouse, brings onto the computer screen another web page. The hyperlink can appear on a screen (window) as text, such as the Internet address ("URL") of the web page being called up or a word or phrase that identifies the web page to be called up, for example, "DeCSS web site." Or the hyperlink can appear as an image, for example, an icon depicting a person sitting at a computer watching a DVD movie and text stating "click here to access DeCSS and see DVD movies for free!" The code for the web page containing the hyperlink contains a computer instruction that associates the link with the URL of the web page to be accessed, such that clicking on the hyperlink instructs the computer to enter the URL of the desired web page and thereby access that page. With a hyperlink on a web page, the linked web site is just one click away.[31]

114 [456] In applying the DMCA to linking (via hyperlinks), Judge Kaplan recognized, as he had with DeCSS code, that a hyperlink has both a speech and a nonspeech component. It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user's computer screen (or, as Judge Kaplan put it, to "take one almost instantaneously to the desired destination." [...]As he had ruled with respect to DeCSS code, he ruled that application of the DMCA to the Defendants' linking to web sites containing DeCSS is content-neutral because it is justified without regard to the speech component of the hyperlink. Id. The linking prohibition applies whether or not the hyperlink contains any information, comprehensible to a human being, as to the Internet address of the web page being accessed. The linking prohibition is justified solely by the functional capability of the hyperlink.

115 Applying the O'Brien/Ward/Turner Broadcasting requirements for content-neutral regulation, Judge Kaplan then ruled that the DMCA, as applied to the Defendants' linking, served substantial governmental interests and was unrelated to the suppression of free expression.[...]We agree. He then carefully considered the "closer call," id., as to whether a linking prohibition would satisfy the narrow tailoring requirement. In an especially carefully considered portion of his opinion, he observed that strict liability for linking to web sites containing DeCSS would risk two impairments of free expression. Web site operators would be inhibited from displaying links to various web pages for fear that a linked page might contain DeCSS, and a prohibition on linking to a web site containing DeCSS would curtail access to whatever other information was contained at the accessed site.[...]

116 To avoid applying the DMCA in a manner that would "burden substantially more speech than is necessary to further the government's legitimate interests," [...]Judge Kaplan adapted the standards of New York Times Co. v. Sullivan, 376 U.S. 254, 283 (1964), to fashion a limited prohibition against linking to web sites containing DeCSS. He required clear and convincing evidence

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

118 [...]He then found that the evidence satisfied his three-part test by his required standard of proof.[...]

119 In response to our post-argument request for the parties' views on various issues, including specifically Judge Kaplan's test for a linking prohibition, the Appellants replied that his test was deficient for not requiring proof of intent to cause, or aid or abet, harm, and that the only valid test for a linking prohibition would be one that could validly apply to the publication in a print medium of an address for obtaining prohibited material. [...]The Appellees and the Government accepted [457] Judge Kaplan's criteria for purposes of asserting the validity of the injunction as applied to the Appellants, with the Government expressing reservations as to the standard of clear and convincing evidence.[...]

120 Mindful of the cautious approach to First Amendment claims involving computer technology expressed in Name.Space, 202 F.3d at 584 n.11, we see no need on this appeal to determine whether a test as rigorous as Judge Kaplan's is required to respond to First Amendment objections to the linking provision of the injunction that he issued. It suffices to reject the Appellants' contention that an intent to cause harm is required and that linking can be enjoined only under circumstances applicable to a print medium. As they have throughout their arguments, the Appellants ignore the reality of the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Under the circumstances amply shown by the record, the injunction's linking prohibition validly regulates the Appellants' opportunity instantly to enable anyone anywhere to gain unauthorized access to copyrighted movies on DVDs.[32]

121 At oral argument, we asked the Government whether its undoubted power to punish the distribution of obscene materials would permit an injunction prohibiting a newspaper from printing addresses of bookstore locations carrying such materials. In a properly cautious response, the Government stated that the answer would depend on the circumstances of the publication. The Appellants' supplemental papers enthusiastically embraced the arguable analogy between printing bookstore addresses and displaying on a web page links to web sites at which DeCSS may be accessed.[...]They confidently asserted that publication of bookstore locations carrying obscene material cannot be enjoined consistent with the First Amendment, and that a prohibition against linking to web sites containing DeCSS is similarly invalid.[...]

122 Like many analogies posited to illuminate legal issues, the bookstore analogy is helpful primarily in identifying characteristics that distinguish it from the context of the pending dispute. If a bookstore proprietor is knowingly selling obscene materials, the evil of distributing such materials can be prevented by injunctive relief against the unlawful distribution (and similar distribution by others can be deterred by punishment of the distributor). And if others publish the location of the bookstore, preventive relief against a distributor can be effective before any significant distribution of the prohibited materials has occurred. The digital world, however, creates a very different problem. If obscene materials are posted on one web site and other sites post hyperlinks to the first site, the materials are available for instantaneous worldwide distribution before any preventive measures can be effectively taken.

123 This reality obliges courts considering First Amendment claims in the context of the pending case to choose between two unattractive alternatives: either tolerate some impairment of communication in order [458] to permit Congress to prohibit decryption that may lawfully be prevented, or tolerate some decryption in order to avoid some impairment of communication. Although the parties dispute the extent of impairment of communication if the injunction is upheld and the extent of decryption if it is vacated, and differ on the availability and effectiveness of techniques for minimizing both consequences, the fundamental choice between impairing some communication and tolerating decryption cannot be entirely avoided.

124 In facing this choice, we are mindful that it is not for us to resolve the issues of public policy implicated by the choice we have identified. Those issues are for Congress. Our task is to determine whether the legislative solution adopted by Congress, as applied to the Appellants by the District Court's injunction, is consistent with the limitations of the First Amendment, and we are satisfied that it is.

IV. Constitutional Challenge Based on Claimed Restriction of Fair Use

126 Asserting that fair use "is rooted in and required by both the Copyright Clause and the First Amendment," [...]he Appellants contend that the DMCA, as applied by the District Court, unconstitutionally "eliminates fair use" of copyrighted materials,[...]We reject this extravagant claim.

127 Preliminarily, we note that the Supreme Court has never held that fair use is constitutionally required, although some isolated statements in its opinions might

arguably be enlisted for such a requirement. In Stewart v. Abend, 495 U.S. 207 (1990), cited by the Appellants, the Court merely noted that fair use "'permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster,'"[...]In Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994), the Court observed, "From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, '[t]o promote the Progress of Science and useful Arts. . . .'"[33] [...]

128 We need not explore the extent to which fair use might have constitutional protection, grounded on either the First Amendment or the Copyright Clause, because whatever validity a constitutional claim might have as to an application of the DMCA that impairs fair use of copyrighted materials, such matters are far beyond the [459] scope of this lawsuit for several reasons. In the first place, the Appellants do not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits them from making such fair use. They are barred from trafficking in a decryption code that enables unauthorized access to copyrighted materials.

129 Second, as the District Court properly noted, to whatever extent the anti-trafficking provisions of the DMCA might prevent others from copying portions of DVD movies in order to make fair use of them, "the evidence as to the impact of the anti-trafficking provision[s] of the DMCA on prospective fair users is scanty and fails adequately to address the issues." [...]

130 Third, the Appellants have provided no support for their premise that fair use of DVD movies is constitutionally required to be made by copying the original work in its original format.[34] Their examples of the fair uses that they believe others will be prevented from making all involve copying in a digital format those portions of a DVD movie amenable to fair use, a copying that would enable the fair user to manipulate the digitally copied portions. One example is that of a school child who wishes to copy images from a DVD movie to insert into the student's documentary film. We know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original. Although the Appellants insisted at oral argument that they should not be relegated to a "horse and buggy" technique in making fair use of DVD movies,[35] the DMCA does not impose even an arguable limitation on the opportunity to make a variety of traditional fair uses of DVD movies, such as commenting on their content, quoting excerpts from their screenplays, and even recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie. The fact that the resulting copy will not be as perfect or as manipulable as a digital copy obtained by having direct access to the DVD movie in its digital form, provides no basis for a claim of unconstitutional limitation of fair use. A film critic making fair use of a movie by quoting selected lines of dialogue has no constitutionally valid claim that the review (in print or on television) would be technologically superior if the reviewer had not been prevented from using a movie camera in the theater, nor has an art student a valid constitutional claim to fair use of a painting by photographing it in a museum. Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique

or in the format of the original.

Conclusion

132 We have considered all the other arguments of the Appellants and conclude that [460] they provide no basis for disturbing the District Court's judgment. Accordingly, the judgment is affirmed.[...]

[Notes:]

135 [2] "2600" has special significance to the hacker community. It is the hertz frequency ("a unit of frequency of a periodic process equal to one cycle per second," Webster's Third New International Dictionary 1061 (1993)) of a signal that some hackers formerly used to explore the entire telephone system from "operator mode," which was triggered by the transmission of a 2600 hertz tone across a telephone line, [...]or to place telephone calls without incurring long-distance toll charges, [...]One such user reportedly discovered that the sound of a toy whistle from a box of Cap'n Crunch cereal matched the telephone company's 2600 hertz tone perfectly.[...]

136 [3] By the end of 1997, most if not all DVDs that were released were encrypted with CSS. [...] Moreover, DVD players were projected to be in ten percent of United States homes by the end of 2000.[...]In fact, as of 2000, about thirty-five percent of one studio's worldwide revenues from movie distribution was attributable to DVD sales and rentals.[...]

138 [5] An item of some controversy, both in this litigation and elsewhere, is the extent to which CSS-encrypted DVDs can be copied even without DeCSS. The record leaves largely unclear how CSS protects against the copying of a DVD, as contrasted with the playing of a DVD on an unlicensed player. The Defendants' experts insisted that there is nothing about the way CSS operates that prevents the copying of a DVD. [...]Some of the Plaintiffs' experts countered simply that "copying to a hard drive is something that compliant DVD players are not allowed to do," without explaining why. [...]Another expert indicated that while a DVD movie can be copied to a computer's hard drive in encrypted form, the movie cannot be played without a DVD actually present in the DVD drive. [...] This expert did not identify the mechanism that prevents someone from copying encrypted DVDs to a hard drive in the absence of a DVD in the disk drive. However, none of this detracts from these undisputed findings: some feature of either CSS itself, or another (unidentified) safeguard implemented by DVD manufacturers pursuant to their obligations under the CSS licensing scheme, makes it difficult to copy a CSS-encrypted DVD to a hard drive and then compress that DVD to the point where transmission over the Internet is practical. [...] Conversely, a DVD movie file without CSS encryption is easily copied, manipulated, and transferred. [...]In other words, it might very well be that copying is not blocked by CSS itself, but by some other protection implemented by the DVD player manufacturers. Nonetheless, in decrypting CSS, the DeCSS program (perhaps incidentally) sidesteps whatever it is that blocks copying of the files. While there may be alternative means of extracting a non-encrypted, copyable movie from a DVD—for example, by copying the movie along with its encryption "bit-by-bit,"

or "ripping" a DVD by siphoning movie file data after CSS has already been decrypted by a licensed player—DeCSS is the superior means of acquiring easily copyable movies, see id. at 342, and in fact, is recommended by a DVD compression web site as the preferred tool for obtaining a decrypted DVD suitable for compression and transmission over the Internet,[...]We acknowledge the complexity and the rapidly changing nature of the technology involved in this case, but it is clear that the Defendants have presented no evidence to refute any of these carefully considered findings by the District Court.

139 [6] The District Court determined that even at high speeds, typical of university networks, transmission times ranged from three minutes to six hours. The Court noted, however, that "the availability of high speed network connections in many businesses and institutions, and their growing availability in homes, make Internet and other network traffic in pirated copies a growing threat."[...]

140 [7] Defendant 2600 Enterprises, Inc., is the company Corley incorporated to run the magazine, maintain the web site, and manage related endeavors like merchandising.[...]

146 [13] The legislative history of the enacted bill makes quite clear that Congress intended to adopt a "balanced" approach to accommodating both piracy and fair use concerns, eschewing the quick fix of simply exempting from the statute all circumventions for fair use.[...]It sought to achieve this goal principally through the use of what it called a "fail-safe" provision in the statute, authorizing the Librarian of Congress to exempt certain users from the anti-circumvention provision when it becomes evident that in practice, the statute is adversely affecting certain kinds of fair use. [...] Congress also sought to implement a balanced approach through statutory provisions that leave limited areas of breathing space for fair use. A good example is subsection 1201(d), which allows a library or educational institution to circumvent a digital wall in order to determine whether it wishes legitimately to obtain the material behind the wall. [...]It would be strange for Congress to open small, carefully limited windows for circumvention to permit fair use in subsection 1201(d) if it then meant to exempt in subsection 1201(c)(1) any circumvention necessary for fair use.[...]

166 [33] Although we have recognized that the First Amendment provides no entitlement to use copyrighted materials beyond that accorded by the privilege of fair use, except in "an extraordinary case," Twin Peaks Productions, Inc. v. Publications International, Ltd., 996 F.2d 1366, 1378 (2d Cir. 1993), we have not ruled that the Constitution guarantees any particular formulation or minimum availability of the fair use defense.

167 [34] As expressed in their supplemental papers, the position of the Appellants is that "fair use extends to works in whatever form they are offered to the public," Supplemental Brief for Appellants at 20, by which we understand the Appellants to contend not merely that fair use may be made of DVD movies but that the fair user must be permitted access to the digital version of the DVD in order to directly copy excerpts for fair use in a digital format.

168 [35] In their supplemental papers, the Appellants contend, rather hyperbolically, that a prohibition on using copying machines to assist in making fair use of texts could not validly be upheld by the availability of "monks to scribe the relevant passages."[...]