6 DeCSS Continued: The Hacker Ethic and the Reimerdes Case

The Reimerdes case, like the Bunner case, is important in the DeCSS history in that it showcases important frames for the movement. Furthermore, it is particularly illustrative of the dissonance between hacker practices, academic freedom, and user concepts of freedom of speech and legal/industry interpretations of those concepts. It shows how wider publics such as academics in the fields of cryptology and engineering can be drawn into a debate that starts off as a question of copyright policy. In that sense, the case demonstrates the power of movement frames to touch on the everyday technological practices of users with technological expertise and transcend into professional practices such as online journalism.

The Fight for a Preliminary Injunction

On January 15, 2000, a little more than two weeks after the DVD CCA filed suit against Andrew Bunner and others in California, the MPAA filed for an injunction on three individuals in New York State: (1) Shawn Reimerdes, who operated a Web site called dvd-copy.com, distributed the DeCSS program, and linked to other sites that also distributed the application; (2) Roman Kazan, who operated the Web site krackdown.com/decss, which also distributed the DeCSS source and application; and (3) Eric Corley, perhaps the most important for our discussion, who operated the *2600: The Hacker Quarterly* Web site. The print publication and Web site for *2600* magazine are edited by Eric Corley under the pseudonym "Emmanuel Goldstein" (the name of a character in George Orwell's *1984*).

Founded in 1984, the magazine is at the center of hacker subculture. The name of the publication itself is a reference to one of the most infamous instances in computer hacking known as "phreaking." *Phreaking* is a hacker term melding the words *phone* and *freak* and used to describe

hackers who study and exploit weaknesses in telephone communication architectures. Phreakers are generally considered to be a subgroup within the broader hacker community and are usually minors younger than seventeen. The legal ramifications for hacking into the telephone system can be quite severe, and most leave the practice when the costs become potentially too high. In the 1960s, hackers discovered that a telephone user could access the operator mode in telephones and make free long-distance telephone calls if they whistled a tone with a frequency of 2600 hertz into the receiver of any telephone. The magazine title is thus a direct reference to one of the earliest of hacker practices, and when Universal named *2600*'s Eric Corley as a defendant in its lawsuit, it attacked a mainstay in hacker culture. Corley had also been named in the DVD CCA case, but in this instance he took a central role.

In both the Bunner and Reimerdes cases, the movie industry wanted to enjoin the defendants from distributing and linking to the DeCSS application and source code, but in the Reimerdes case the MPAA used the DMCA and copyright law as its basis for enjoining the defendants. Learning from the DVD CCA case, in which by this time the DVD CCA had been denied a temporary injunction by the California Superior Court, the MPAA presented its case from the perspective of the constitutionally important intellectual-property clause.

In its arguments for granting an injunction, the MPAA was affected by earlier failures in California. When the Superior Court chose to deny the DVD CCA a preliminary injunction in Bunner, DeCSS proponents interpreted this decision as an affirmation of their free-speech rights and so increased their efforts to distribute the code as widely as possible. Corley had actually been trying to do so ever since the code had been released in November 1999 (a month before he was named in either the Bunner case or the Reimerdes case). On his Web site, Corley noted that "there have been numerous reports of movie industry lawyers shutting down sites offering information about DeCSS. *2600* feels that any such suppression of information is a very dangerous precedent. That is why we feel it's necessary to preserve this information. . . . People with original copies of pages that have now been censored or removed are encouraged to send us copies for mirroring as well as links to additional information" ("DVD Encryption Cracked" 1999).

By the time the MPAA brought suit in New York, there was a concerted effort to distribute DeCSS on the Internet. Fritz Attaway, senior vice president for government relations and general counsel for the MPAA in Washington, DC, explained to the New York court that

> When . . . the court [in California] declined to issue a temporary restraining order, members of the hacker community took this as a vindication of their actions. Displaying an "in your face" attitude, hackers taunted CCA and the MPAA by stepping up their efforts to distribute DeCSS to the widest possible worldwide audience. I am informed that one enterprising individual even announced a contest with prizes (copies of DVDs) for the greatest number of copies distributed, for the most elegant distribution method, and for the "lowest tech" method. (Universal v. Reimerdes et al., US District Court [SD NY 2000], Declaration of Fritz Attaway in Support of Plaintiffs)

Much like in the Bunner case, the EFF played a key role, providing legal defense for Shawn Reimerdes and the others. However, the EFF was much less successful with the Reimerdes case than it was with the Bunner case. Transcripts of the hearing for the petition to the court to enjoin Reimerdes show that the EFF lawyers had a very bad day in court. They failed to present supporting affidavits, had not really thought their arguments through, and failed to convince an openly antagonistic judge[1] that their defendants ought not to be enjoined. Unlike in the Bunner case, the EFF did not make cogent arguments regarding the issues of prior restraint and, it seems, could not navigate the DMCA in a fashion that convinced the judge that the defendants were acting within exemptions in the statute. Part of the problem was that the judge read the complaint quite narrowly and pressed the EFF to show how the defendants had in fact not violated the DMCA's anticircumvention and antidistribution provisions. Even though the EFF tried to argue that there may be some conflicts with fair use or even that some of the defendants might be protected by the DMCA's safe-harbor provisions, the court was interested only in knowing how exactly DeCSS was not a circumvention device outlawed by section 1201, which of course it plainly was.

Furthermore, the brazen statements made by many hackers distributing the DeCSS software—posting comments such as "Yes, you can trade DVD movie files over the Internet. . . . [T]he DVD Copy Control Association . . . are [*sic*] cocksuckers"—made a sympathetic interpretation of hacker motives almost impossible.[2] Posters of DeCSS technology came across as the work of nihilistic scofflaws, and without affidavits from computer scientists and other cryptographers the EFF could not give DeCSS any legitimacy. In contrast, the MPAA had significant evidence showing that the hacker and broader Internet community was engaged in an all-out campaign to distribute DeCSS as widely as possible. Comments from Fritz Attaway and Web pages calling for wide distribution made a damaging case against those distributing DeCSS.

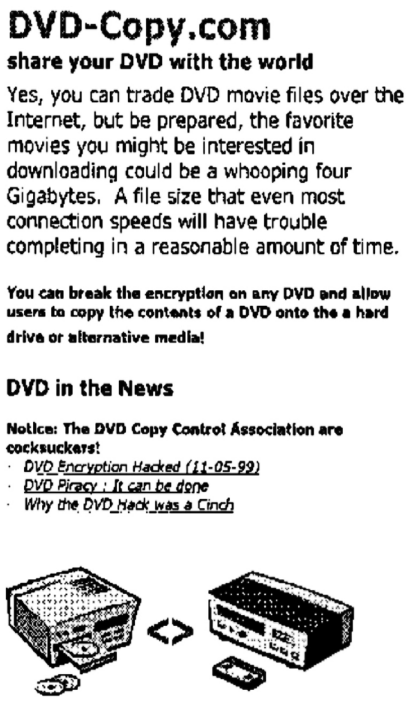


Figure 6.1
Screen capture of the home page of defendant Shawn Reimerdes's Web site dvd-copy .com. Note the text under its title. Image used with permission of site owner.

Even though some of the posts were indeed inflammatory (see figure 6.1), others had a more political bent. There was, in fact, a contest to see who could come up with the most creative way to distribute the DeCSS source code, and the distribution was couched in political, not nihilistic, terms. One contest flyer sarcastically read: "Winners of the contest will receive a copy of a DVD movie of their choice about an evil totalitarian society such as '1984' or 'Brazil' so they can watch the movie and thank God for their freedom," and another noted, "This is about the freedom of information, the right we all still have to learn how technology works—once this is gone there is no end to the kind of information that could be restricted because some conglomerate somewhere decides that its dissemination could cause them some grief" (quoted in Universal City Studios, Inc. v. Corley, US Court of Appeals [2nd Cir. 2001]).

The court was not interested in how hackers and users would define rights of access and use; as mentioned previously, the central question was

whether DeCSS was indeed a circumvention technology in violation of the DMCA. With this question in mind, one cannot fault the court for pursuing the issue narrowly. The task of redefining those rights would fall on activists themselves as they set out to ignore the commands of Judge Lewis Kaplan and the Second Circuit Court of southern New York.

Defining the Issues

During the initial hearing on the case, the MPAA prevailed in court and got its preliminary injunction on Reimerdes and the others. During this hearing, the EFF tried to argue some of the more important issues pertaining to the digital rights movement. On the issue of code as speech, the EFF sought to point out the expressive aspects of code, in particular the part of the source code that contains programmer comments on the importance or rationale behind some lines of code. Second, the EFF noted that because the code was of interest to cryptographers, it must be available to be referenced and looked at by other members of the programming community. Enjoining the defendants from posting the code would interfere with this socially important action. The EFF argued that enjoining Reimerdes and the others from posting DeCSS before it had been determined to what extent DeCSS was expressive should be considered prior restraint. Therefore, the court was compelled to preserve the defendant's free speech and not issue the injunction.

Furthermore, the EFF claimed that DeCSS was protected under the exemptions in the DMCA for reverse engineering. Under these exemptions, an owner of a legally bought program can reverse engineer a copy-protection measure for the purposes of interoperability. The EFF told the court that DeCSS was such a program because it allowed for the design of DVD players for Linux.

The court rejected all of these assertions, viewing DeCSS as primarily a functional tool and not expressive in the way that analysis of prior restraint would require. The judge argued that the public good achieved by posting and distributing DeCSS was minimal. Even if there was some expressive element to the code, harm from its curtailment could not be compared to the harm done to the film industry, whose copyright was also a constitutionally important goal. Furthermore, the judge noted that curtailment of the code was not curtailment of the notes in the code, which could be posted.

As stated earlier, these arguments appear disingenuous. On the issue of reverse engineering, the judge read the statute quite narrowly. The statute

explicitly notes that circumvention is for a program and that it has to be done for the sole purpose of interoperability. In its analysis, the court noted:

> First, defendants have offered no evidence to support this assertion.
>
> Second, even assuming that DeCSS runs under Linux, it concededly runs under Windows—a far more widely used operating system—as well. It therefore cannot reasonably be said that DeCSS was developed "for the sole purpose" of achieving interoperability between Linux and DVDs.
>
> Finally, and most important, the legislative history makes it abundantly clear that Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works, such as movies. In consequence, the reverse engineering exception does not apply. (Universal v. Reimerdes et al. [2000], Memorandum Order)

The statute appears inconsistent in its attitude toward reverse engineering of computer programs. What if, for example, the computer program is an anticircumvention measure? Does this imply that this program must not be reverse engineered? What if copy control is part of a larger program, and reverse engineering of the whole implies reverse engineering copy-protection devices?

The defendants' case was damaged early on by their inability to show evidence at the preliminary hearing that some of the activities in designing DeCSS were legitimately important to cryptography. They were also harmed by the court's perception that DeCSS was not designed in good faith. The judge wrote, "There is no evidence that any of them is engaged in encryption research, let alone good faith encryption research. It appears that DeCSS is being distributed in a manner specifically intended to facilitate copyright infringement. There is no evidence that [the] defendants have made any effort to provide the results of the DeCSS effort to the copyright owners" (Universal v. Reimerdes et al. [2000], Memorandum Order).

Expanding the Injunction and Continuing the Defense

Following the preliminary injunction, Reimerdes and Kazan dropped out of the case, choosing to discontinue distributing DeCSS. However, Corley stayed on and stepped up his efforts to distribute DeCSS on his 2600.com Web site, stating, "Help us fight the MPAA by leafleting and mirroring DeCSS" (as quoted in Reply Memorandum of Law in Further Support of Plaintiffs' Motion to Modify the January 20, 2000, Order of Preliminary Injunction, Universal v. Reimerdes, IS District Court [SD NY 2000]). Although

he was enjoined from actively distributing the code, he linked to it heavily, providing more than four hundred links to the DeCSS application and source code on his own site, with some of those linked sites providing even more links (Universal v. Corley, US District Court [SD NY 2000], Supplemental Declaration of Robert W. Schumann). This act prompted the MPAA to request a modification to the injunction, asking the court to prohibit Corley not only from distributing the code, but also from linking to it.

In an initial declaration in opposition to expanding the injunction, Corley attempted to educate the court on the nature of hacker culture, hoping to the correct the pejorative meaning typically associated with the term. He noted:

> It is important to understand that the terms "hacker" and "hacking" as used by and about *2600* are not pejorative, but refer to the original sense of the term "hacker" as a person experienced or expert with computers and Internet navigation who is imbued with a spirit of imagination, innovation and exploration. In the traditional sense of the word, for example, "hackers" include professional security experts used by major corporations and governments to test the security of systems. (Universal v. Corley [2000], Declaration of Emmanuel Goldstein in Opposition to Plaintiffs' Motion to Modify the Preliminary Injunction)

Corley went on to point out how hacker practices have been misunderstood by society. He explained that the role of *2600* magazine was not only to instruct hackers, but also to "instill a sense of reality into the mainstream so that the actions of such people are judged in a more even-handed way and so that people aren't sent to prison for relatively minor offenses" (Universal v. Corley [2000], Declaration of Emmanuel Goldstein).

Corley's reason for posting DeCSS was entirely consistent with the hacker subcultural ethic and with many of the goals of the digital rights movement. Explaining why he chose to distribute DeCSS, Corley wrote, "When [DeCSS] was posted to the Internet, I recognized the importance of such a program to a variety of disciplines, including reverse engineering and open-source DVD player, cryptography, and in aid of legal consumer fair use. I was quick to show support for its existence and to condemn the attempts at forcibly quashing such knowledge" (Universal v. Corley [2000], Declaration of Emmanuel Goldstein). Finally, Corley complained bitterly about the court's inability to see legitimate alternative purposes for DeCSS and about the MPAA's bullying tactics toward other DeCSS distributors whom the court order had not enjoined. He noted:

> It is important to note that this entire issue is NOT about copying but rather about access. I believe it is entirely legal to use a DVD one has bought in a computer that one has bought. I oppose illegal copying but that has got nothing to do with DeCSS.

> . . . [The MPAA] has been sending cease-and-desist letters to some or all of the websites on our mirror list. The letters . . . are misleading and intimidating, since they suggest that the recipient "may" be subject to an injunction even though Plaintiffs know very well that the recipient is not. (Universal v. Corley [2000], Declaration of Emmanuel Goldstein).

An important development in this case was the EFF's recruitment of noted First Amendment lawyer Martin Garbus.[3] Garbus immediately filed to have the injunction vacated and began pressuring the MPAA to step up its discovery process. He made some important claims early on about the court's refusal to consider Corley's First Amendment rights properly. He noted, for example, that there was bias in the injunction against *2600* magazine because it was a hacker publication as opposed to a traditional news source. Garbus states that "had [the] plaintiff[s] sued *The San Jose Mercury News* or *The New York Times*, the resultant outcry would have been different" (Universal v. Corley [2000], Affidavit of Martin Garbus in Support of Defendant's Motion to Have Plaintiffs Post Security Bond). Richard Meislin, editor in chief of the *New York Times* digital edition, explained to the court that "the ability to refer readers to other Web sites that relate to a particular article is an integral part of the practice of journalism on the Web" (Universal v. Corley [2000], Declaration of Richard Meislin, Editor in Chief: *New York Times* Digital Edition).[4]

Garbus also argued that expanding the injunction to include hyperlinking would encounter some technological hurdles defined by Web browser technology. Linking involves annotating the text visible to the reader with some invisible HTML (hypertext markup language) commands; for example, one can type in the word *DeCSS* and have the word associated with an HTML code that calls for the specific Web address where DeCSS can be found. Or one can type out the Web address as part of the text and then tie the HTML to it. Some browsers are able to scan the text of a page looking for text that can double as an HTML command. Garbus noted that the browser can treat any Web address this way, even if not linked. Thus, even if hyperlinking were enjoined, the presence of the Web address in the text of an article would cause some browsers to treat it automatically as a live link. To prevent this, Garbus implied, the court would have to enjoin not only the conduct of linking, but also the very mention of any Web address that a browser may assume to be a live link (Universal v. Corley [2000], Brief Submitted by Media Defendant 2600 Enterprises).

Garbus also argued against the injunction on fair-use grounds and revisited many of the themes presented in the review of the formulation of the DMCA. As was done in the Sklyarov case, Garbus tied fair use to the First

Amendment. He explained that fair use strikes a balance against the monopoly on speech granted by copyright. He portrayed fair use as a right, an interpretation that had been heavily contested by copyright owners and the register of copyrights during formulation and review of the DMCA. Garbus wrote:

> CSS, which plaintiffs would have codified into law through its cramped reading of Section 1201, completely blocks access to the copyrighted material on a DVD, and prevents thereby any possibility that the right of fair use can be exercised with respect to that material. Congress did not anticipate or permit this . . . it is imperative to explode the favored analogy urged by plaintiffs, the MPAA and the DVD CCA, that no one has the right to break into a bookstore to make fair use of a book. In reality, the effect of CSS on fair use is to permit a publisher to prohibit a customer who has purchased one of its books from reading the work, except in a room constructed by a licensed builder, or under the lamp built by a licensed manufacturer. (Universal v. Corley [2000], Brief Submitted by Media Defendant 2600 Enterprises)

The notions of copy control and access control were central to this case. Deployment of the "breaking and entering" metaphor does not apply equally to both copy-control and access-control technologies. The exemptions that Congress made were for the first, not the second. Congress created an access right for copyright owners in the course of protecting access-control technologies. The digital rights movement argues that access rights, when under the protection of technological enforcement, preclude fair use.

Corley's Allies and Their Support of DeCSS

Besides the EFF's and Martin Garbus's involvement as defense counsel, Corley mustered an impressive array of support against the expansion of the preliminary injunction, with supporters coming from universities, law schools, and the computer industry (see table 6.1).

Many of Corley's supporters submitted statements to the court, and it became obvious how extensive resistance to the preliminary injunction had become. There were also close connections between the Bunner case in California and the Corley case in New York. Some defendants, for example, were named in both cases, and some of the people submitting statements of support for the defendants did so in both cases. Analysis of the court record in the Corley case shows an extensive network of activists coming together on the Internet to undermine the court's attempts at suppressing DeCSS. All of these activities were coordinated in an ad hoc fashion as participants took interest in the case and chose to "mirror"

Table 6.1
Corley's Supporters against Expansion of the Preliminary Injunction on DeCSS to Include Linking

Name of Supporter	Occupation/Affiliation
Pam Samuelson	Professor of law, Boalt Hall School of Law at the University of California at Berkeley
Richard J. Meislin	Editor in chief, *New York Times* digital edition
Charles R. Nesson	Professor of law, Berkman Center for Internet and Society at Harvard Law School
Chris DiBona	VA Linux Systems, Inc.
Bruce Fries	TeamCom New Media Consulting, LLC
John Gilmore	Founder, SunMicro Systems; EFF cofounder; founder, Cygnus Support/Affiliation with Red Hat Linux; cofounder, Cypherpunks, an informal educational and advocacy group devoted to advancement of privacy and security through greater knowledge and deployment of encryption
Lewis Kurlantzick	Professor of law, University of Connecticut Law School
Eben Moglen	Professor of law and legal history, Columbia University Law School
Matt Pavlovich	President, Media Driver, LLC, a consulting company that focuses on providing Linux video solutions to industry
Bruce Schneier	Chief technology officer, Counterpane Internet Security Inc., a cryptography consulting company, and author of one of the five encryption methods under consideration to become the US Advanced Encryption Standard
Barbara Simons	President, Association for Computing Machinery
Frank Stevenson	Computer research programmer, Funcom Oslo AS; first to publicly disclose cryptonalysis on the CSS ciphers
Dave Touretsky	Senior research scientist, Computer Science Department and Center for the Neural Basis of Cognition, Carnegie Mellon University
David Wagner	PhD candidate in computer science, University of California at Berkeley; cofounder, UC Berkeley's ISAAC Security Research Group
John Young	Operator, Cryptome.org Internet Library Archive

DeCSS or post the code themselves. The EFF played an important role in this regard by acting as a collection point of information and supplying defense counsel to those being sued by the movie industry. The defendants themselves were responsible for fomenting dissent against the injunction. The movement was coherently attacking the DMCA with both institutional and extrainstitutional tactics.[5]

Perhaps one instance above all others shows the determination to challenge the court's injunction: David Touretsky's Gallery of CSS

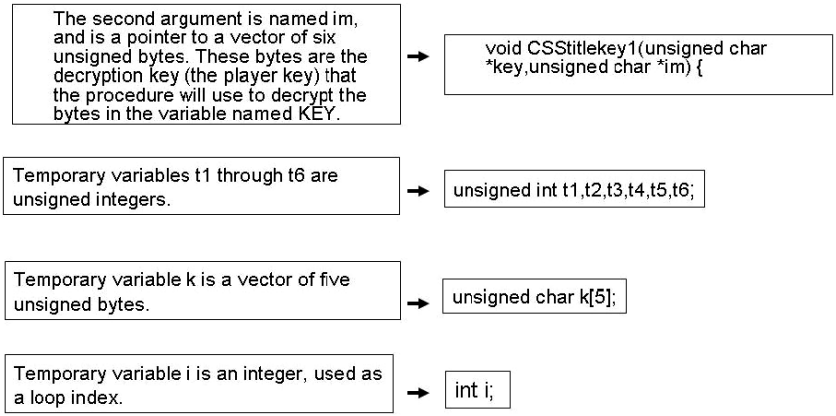


Figure 6.2
English to C translation of DeCSS. Adapted from David Touretsky's Gallery of CSS De-Scramblers (Touretsky n.d.).

De-Scramblers. Touretsky, a senior computer scientist at Carnegie Mellon's Center for the Neural Basis of Cognition, posted a collection of DeCSS variants to "point out the absurdity of Judge Kaplan's position that source code can be legally differentiated from other forms of written expression" (Universal v. Corley [2000], Deposition of Dr. David Touretsky).

On Touretsky's site, one could view DeCSS in various forms. For example, one could order T-shirts or ties with the DeCSS code inscribed on them, or one could view the DeCSS code translated into conversational English (see figure 6.2) with corresponding translations in the C programming language or in verse form (quoted in chapter 5).

Dr. Touretsky was very clear about the political nature of his gallery. In a written statement submitted to the court in support of Corley, he noted:

> I created the Gallery in response to the Preliminary Injunction issued by this Court. The Gallery consists of a set of files containing source code, textual descriptions of algorithms, and discussion of programs that can decrypt data that has been encrypted with CSS or that can recover the keys necessary for such decryption. . . . It is my belief that source code is expressive speech meriting the full protection of the First Amendment. This belief results in part from my experience as a computer science educator. . . . I am concerned that this Court issued an order prohibiting the defendants from posting source code for CSS decryption algorithms on the Internet. As a scientist, I feel it is imperative that anyone, not just academics, be allowed to participate in the ongoing analysis and improvement of encryption technologies. . . . My Gallery is a combination of scientific dialog and political statement. (Universal v. Corley [2000], Declaration of Dr. David Touretsky)

He also pointed out that many of the more than four hundred sites linking to DeCSS had a political bent. It was clear from his gallery and from other acts of support for Corley that the DeCSS case had inspired far more people than professional programmers. One high school graduate at the time posted DeCSS on his byline in his school's yearbook.

Besides subverting the court's order on linking and posting DeCSS, Touretsky made some incisive critiques of the injunction. Important among them was his assertion that it is impossible to have open discussion guaranteed by the First Amendment without being able to see and reference the DeCSS code. The court itself had said that its injunction was only on posting DeCSS and that the injunction was not meant to curtail its discussion. Touretsky pointed out the difficulty inherent in this distinction, telling the court, "My web site contains a copy of a textual description of the CSS decryption algorithm by the cryptographer Frank Stevenson. How is one to determine whether Stevenson's description is accurate? The only reliable way is to compare it with the source code for an implementation that is known to be correct because it has been compiled and run successfully" (Universal v. Corley [2000], Declaration of Dr. David Touretsky). The absurdity of an injunction on the "text" (the DeCSS source code) but not on discussion of the "text" was made clear during an exchange between Touretsky and the MPAA's lawyers during Touretsky's deposition.

MPAA: . . . How does Judge Kaplan's injunction affect the things that you express concern about in the sentences I just read?

Touretsky: Judge Kaplan has enjoined the publication of source code, and that will hinder the ability of people to discuss these algorithms. . . .

MPAA: Let's say you were interested in having a discussion with like-minded people about encryption technologies. You could do that through e-mail, couldn't you[?] . . . And you could, if you wanted to study source code in connection with the discussion of encryption technologies, you could send copies of the source code back and forth by e-mail, correct[?] . . . And, hypothetically, if like-minded people wished to discuss encryption technology and in the process study source code, at least hypothetically they could get together, form a private Web site and post the source code on that site, correct[?] . . . What is the difference between obtaining or studying the source code through that private Web site as opposed to obtaining it through the 2600 Web sites?

Touretsky: I think there are two differences. First of all, if discussion was [*sic*] restricted to this private Web site, people with a casual interest would not be able to obtain access to the material. And, secondly, if people were required to only discuss the source code on this private Web site, they would be denied their First Amendment rights.

MPAA: And how would that be, sir?

Touretsky: Because the First Amendment does not say that one can discuss things in private but not in public. (Universal v. Corley [2000], Deposition of Dr. David Touretsky)

Touretsky makes the point quite clear that when the court enjoined DeCSS but yet still claimed to protect speech, it was being inconsistent. A person with a casual interest in the topic would be completely excluded from discussing DeCSS, and those with significant interest would have to go to great lengths to be part of the discussion.

Themes in Statements by Corley's Supporters

As Corley's supporters submitted their declarations, it became clear that some themes consistent with the goals of the digital rights movement were continuously raised. First, they claimed that interpreting the DMCA's reverse engineering exemption[6] as narrowly as the court had done in Corley would have a chilling affect on innovation. David Wagner, a computer scientist at Berkeley, argued that without reverse engineering CSS, a DVD player for Linux would be difficult to build. He noted,

Reverse engineering is often tedious and time-consuming because computer programs are extremely verbose (by human standards), but it is not in principle difficult. . . . Based upon my experience and participation in and my observation of the academic and research communities at the University of California, Berkeley, reverse engineering is necessary, standard, and good for software and consumer electronic products containing encryption. . . . Reverse engineering CSS as part of this process was . . . a necessity: you cannot build a DVD player on which to play DVDs that are encrypted with CSS unless you know how CSS works and how to make the DVD play despite the presence of CSS. (Universal v. Corley [2000], Declaration of David Wagner)

Second, witnesses argued that there were other significant noninfringing uses for DeCSS, such as fair uses that had been shown to be permissible by the Supreme Court case Sony Corp. of America v. Universal City Studios, Inc. (464 US 417 [1984]). Noted legal scholar Pamela Samuelson, an early critic of the DMCA and a prominent figure in the network of activists and organizations that comprise the digital rights movement, pointed out that

the U.S. Supreme Court in *Sony Corp. of America, Inc. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) established the rule that copyright owners only have the right to control infringement-enabling technologies if they lack "substantial noninfringing uses." During the legislative struggle over the anti-circumvention provisions, Congress added a provision to the DMCA intended to preserve this standard by including section 1201(c)(2) in this law. Insofar as DeCSS has a substantial

noninfringing use, such as the enablement of platform conversion, it should be permissible under both *Sony* and the DMCA. (Universal v. Corley [2000], Declaration of Pamela Samuelson in Opposition to Plaintiffs)

Charles Nesson of Harvard Law School pointed out that CSS interfered with fair use in the course of his teaching. He explained:

I frequently use multimedia in my teaching, adding audio and video to my classroom presentations to help tell the full story of a case or question. For example, in my Evidence class I use clips from "The Verdict" to illustrate closing argument, from "The Accused" . . . and from "My Cousin Vinny" to raise a variety of trial and ethical issues. Currently, I can assemble a series of selections from videotape to present at the time and in the order most effective for my lesson. I can store other segments on a computer for quick access if they become relevant to a discussion. If new works are made available only in DVD format, access controls such as those the studios seek to enforce here will prevent me from using such works as an effective teaching tool. I believe this is only one example among many fair uses that would be extinguished if [the] plaintiffs' reading of anti-circumvention were adopted. (Universal v. Corley [2000], Brief of Professor Charles R. Nesson as Amicus Curiae in Support of Defendants)

As noted in chapter 2, both the WGIP and the registrar of copyrights had addressed this view of fair use, noting that so long as users had the ability to access content in formats not protected by technological enforcement, then the copyright owners and the law were under no obligation to provide access to digital formats. However, some of Corley's supporters increasingly saw the ability to manipulate the kinds of uses of digital media described by Professor Nesson as a political issue. Bruce Fries of TeamCom LLC, a new-media publishing company, was motivated to write a book on the issue, to be titled "Fair Use: The Fight for Consumer Rights." In his statement to the court, he explained:

I conceived this book as a result of the recent court cases initiated by the Entertainment Industry in response to the Internet publication of the DeCSS source code. Fair Use focuses on the issues surrounding the fair use of copyrighted materials by consumers and researchers. It explains various forms of encryption and copy protection schemes that assume consumer dishonesty and prevent or restrict duplication of copyrighted works for legitimate purposes such as fair use and reverse engineering. . . . The book includes tutorials and source code for programs—including the source code for DeCSS—that enable consumers and researchers to circumvent copy protection schemes for fair use purposes. Obviously, it is crucial to the book's accuracy and credibility that I am able to publish the source code for DeCSS and other CSS descramblers. (Universal v. Corley [2000], Declaration of Bruce Fries)

Third, some of Corley's supporters complained that CSS was also being used to force consumers to watch unsolicited advertisements by enforcing a "no-fast-forwarding" section on DVDs. Computer scientist Matt Pavlovich noted that "[n]ot only does [the] CSS license prevent a player from fast-forwarding through those certain portions of a DVD that are marked 'no fast-forwarding,' including entire blocks of unsolicited advertisements, but [it] also . . . explicitly forbids its licensees from making a DVD player with that capability" (Universal v. Corley [2000], Declaration of Matt Pavlovich).

Last, according to some of the respondents on Corley's behalf, the injunction was in conflict not only with scientific norms, but also with hacker norms of sharing information and the norms of the free-software movement. Matt Pavlovich, who also was a defendant in the Bunner case, explained that "the reverse engineering undertaken to develop a Linux DVD player is also directly applicable (and necessary) to the development of DVD players for use on other open-source operating systems, such as NetBSD, OpenBSD, and FreeBSD. . . . The Linux DVD player will be 'open-source' and free of charge to consumers, as with most Linux open-source products" (Universal v. Corley [2000], Declaration of Matt Pavlovich).

Thus, themes of reverse engineering, fair use, scientific norms, innovation, and consumer rights (topics consistent with the digital rights movement) surfaced within the context the DeCSS case. This case became emblematic of what had gone wrong with digital copyright, and Corley's supporters were quick to point that out.

Perhaps no other claim made by the MPAA instilled greater pressure on the court than the claim that DeCSS ease of use would lead to rampant copying. The MPAA expended considerable resources to prove this point in hopes that the program's alarming simplicity would compel the court to perceive an acute threat to the film industry's copyrights. A deconstruction of these technical claims is helpful in illustrating how the narrative of fear regarding technological consequences was deployed to convince the court of some yet unforeseen copyright disaster.

Deconstructing the Fear of Rampant Copying

During court proceedings, some commentators expressed frustration with the claims that CSS was a serious protection mechanism meant to safeguard copyright. Like supporters of Andrew Bunner in the DVD CCA case, they felt that CSS was actually meant to control markets in regions. John Gilmore, cofounder of the EFF, explained:

> Many published DVD discs [*sic*] can only be decoded by a subset of DVD players. Under the name "region coding," the DVD industry has used its capability to create subsets to divide the world into seven regions and contracted to restrict the DVD players sold in each region to only play DVD discs intended to be sold in that region. The region coding system is not inherent in or necessitated by the design of the encryption system at issue, but is created by how the secret keys are administered. I believe that the DVD industry designed and implemented the region coding system in order to restrain global trade in DVD discs, so they can charge differential prices in different regions, and so that the release of particular movies can be delayed in particular markets, for the benefit of theater owners and the companies who rent them movies. (Universal v. Corley [2000], Declaration of John Gilmore)

Corley's supporters argued that if the movie industry were serious about protecting its content, it would have used a strong encryption scheme, not one such as CSS, which was known to be weak. Furthermore, they noted that digital security experts soundly rejected a tactic used in the encryption scheme—to hide the keys in the data of a DVD or security by obfuscation—because any committed individual could scour the data on the DVD and actually find those keys. Barbara Simons, a noted computer scientist and president of the Association for Computing Machinery, argued that "CSS uses only a 40-bit key, a length known to be breakable in a few minutes. It also employs a proprietary algorithm, rather than one that has been extensively tested in the public domain. The copy protection system relies heavily on obfuscation which, together with the carelessness of at least one licensee, appears to have created additional opportunities to break the system" (Universal v. Corley [2000], Declaration of Barbara Simons).

And Bruce Schneier, chief technology officer of Counterpane Internet Security Inc., noted that

> [t]he entertainment industry knew this was a problem, but failed to come up with a viable solution. Instead, DVD software manufacturers were supposed to disguise the decryption program, and possibly the playing program, using some sort of software obfuscation techniques. This is a technique that has never worked: there is simply no way to obfuscate software because it has to be on the computer somewhere, and is thus accessible to researchers, people engaged in reverse engineering, and the like. (Universal v. Corley [2000], Declaration of Bruce Schneier)

Given such technological failure, the defendants argued, claims that the entertainment industry had taken extensive measures to safeguard its content were hyperbole. Although this reasoning alone cannot be seen as a rationale for breaking technological mechanisms, it goes hand-in-hand with claims that testing and sharing information on security systems of this sort makes the security technology better and is consistent with

scientific norms. In fact, every computer scientist who commented on the potential for expanding the injunction on Corley noted that such an action would curtail the free discourse of science. Andrew Appel, a computer scientist from Princeton, noted: "Based on my experience as a University professor and researcher, as a programmer, and as a serious participant on the internet [*sic*] since its birth, it is my opinion that scholarship and science, and the innovation that is so crucial to technological advancement and economic growth, will be seriously damaged by an interpretation of Section 1201 that would prohibit circumvention of security systems" (Universal v. Corley [2000], Declaration of Andrew Appel).

And, again, Bruce Schneier argued that "[DeCSS] is good research, illustrating how bad the encryption algorithm is and how poorly thought out the security model is, and must be available to cryptologists, programmers, and others as a research and intellectual tool through the normal channels—including, but not limited to, posting it on the internet [*sic*]. What is learned here can be applied to making future systems stronger" (Universal v. Corley [2000], Declaration of Bruce Schneier).

One important fact that came out during proceedings for expanding the injunction on Corley was that no cases of pirating commercial DVD movies by the use of DeCSS had been reported yet. Robin Gross of the EFF had met with Gregory Goeckner, MPAA vice president and deputy general counsel, at a panel discussion exploring litigation under the DCMA, "In the Trenches: Reports from the DMCA Battlefield," in New York. When asked if there was any evidence that DeCSS was being used for pirating, Mr. Goeckner had responded that "he was aware of no evidence of any actual piracy attributable to DeCSS" (Universal v. Corley [2000], Declaration of Robin Gross). Many speculated that there had been no pirating because DeCSS was actually too hard to use and because the technology was not yet available. Chris DiBona, a computer scientist for VA Linux, carried out an informal survey, asking members of his mailing list if they had been able to use DeCSS to copy a movie from a DVD. He reported:

> I posted general inquiries about DeCSS-related copying to the Linux, other open-source, and "hacker" (in the non-pejorative sense of individuals devoted to exploring the limits of the Internet) communities via a variety of mailing lists and websites, including but not limited to the SVLUG and DeCSS mailing lists and the opendvd .org website. These communities are made up of very skilled and technically capable people. None of the approximately 2000 people who responded to my e-mails and postings reported using DeCSS to make copies of DVDs. Indeed, only two people—both of whom insisted on strict anonymity as a condition of speaking with me because they feared reprisal from the MPAA—said that they were able to use DeCSS

to view DVDs they had purchased. However, both reported significant problems with playback. One experienced distorted video and both experienced stuttering sound. It's also worth noting that the individual who called the video "high quality" (although with bad sound) used a very expensive dual processing computer equipped with a great deal of random access memory. (Universal v. Corley [2000], Declaration of Chris DiBona)

Others showed that it would be uneconomical to pirate DVDs, calculating that,

[d]ue to the huge size of the files involved, making a verbatim copy of a DVD is impossible in essentially all easily transportable media commonly available today on personal computers. . . . Using the Internet to send or sell copies of stored movies is particularly unreasonable: uploading a single gigabyte over a 56K modem would take about 40 hours, so an entire DVD would take many days. The sheer bulk of the material makes it impractical for consumers to "pirate" DVDs using commonly available equipment. DVD-RAM has been out for a year, and its drives cost from $300–1000. But its discs only hold 2.6GB, cost $14 to $35, and are incompatible with everything else. . . . The available DVD-R recorder drives cost $3500–$5200. Blank recordable media for DVD-R are more expensive than buying pre-recorded DVDS. There is no incentive to copy a $15 DVD onto a $30–$60 blank DVD-R, rather than buying a second original at $15. (Universal v. Corley [2000], Declaration of John Gilmore)

Here it is important to point out an apparent inconsistency in the testimonies of many of Corley's allies, however. Computer scientists in particular made a point of noting that CSS was not good copy protection, that it was easy to break, and therefore posited that its primary purpose was to serve as the linchpin of a licensing mechanism that allowed for price control and regional distribution of content. But in statements such as those given previously, Corley's supporters said that copying was impractical and difficult because getting DeCSS to work required technical expertise and hardware with large storage capacity, which implies that CSS was at least creating a difficult enough barrier to copying. One might argue that these inconsistencies actually show that CSS was at least a "good enough" copy-protection system (good enough to stop the average consumer, who would have to incur costs to get DeCSS to work) as well as an effective price-control mechanism. But this argument conflates views that CSS is an objectively mediocre copy-protection scheme with arguments that it is practically effective. In the eyes of computer scientists noting that CSS was not sophisticated, the argument was necessary to show that the movie industry's claims to having made extraordinary efforts to protect content was exaggerated. Showing that it was practically effective was necessary to

counter arguments that DeCSS would lead to rampant copying. In a sense, Corley's supporters made the argument that DeCSS, when thought of as a copying tool, was theoretically effective but practically not that useful. This gap between theoretical effectiveness and practical effectiveness opened the door for the central functional point of the case: that all DeCSS was really practically good for was to help Linux users develop DVD players for their computers. Critiques of the legal backlash against DeCSS from free-speech, fair-use, and other movement perspectives were important to frame this otherwise very technical issue (designing DVD players) within the movement's broader issues.

There is, however, something valuable to be learned from thinking of the theoretical and practical effectiveness of CSS and DeCSS. CSS is only practically effective when mapped onto a sociotechnical network that involves laws, economies of cost, and technological limitations. This relationship suggests that practical effectiveness is contingent and subject to the network of social and technical forces that define the possibilities of an artifact's use.

In Court: Themes in Testimony

The review of documents and arguments given so far has centered on the hearing meant to stave off the preliminary injunction on Corley. The MPAA's case against Corley went to court, and in this section I review those proceedings. Many of the themes highlighted during Corley's fight against the preliminary injunction resurfaced in the court proceedings. This is important because it shows that the movement's themes remained consistent and its arguments solidified as the case wore on. Corley's and Touretsky's testimony continue to be of particular importance. It defined issues for activists and shaped movement constituencies, which were expanding to include not only hackers and technology companies, but also the open-source community in general, the Linux development community in particular, and educators such as university computer science professors.

Corley, *2600*, and the Hacker Ethic

Eric Corley's testimony made clear how hacker attitudes toward information positioned DeCSS as technology symbolizing hacker beliefs. The hacker subculture is, as much as any subculture, constructed in opposition to dominant trends and mores within broader society. It is in principle subversive and constituted as a response to trends in society that attempt

to establish legitimacy and ownership claims over information. Steven Levy first articulated the hacker ethic in his book *Hackers: Heroes of the Computer Revolution* (1984). He states that the hacker ethic is composed of six tenets: 1. "Access to computers—and anything that might teach you about the way the world works—should be unlimited and total. Always yield to the Hands-On Imperative," 2. "All information should be free," 3. "Mistrust Authority—Promote Decentralization," 4. "Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position," 5. "You can create art and beauty on a computer" and 6. "Computers can change your life for the better" (23–28). Because DeCSS was being suppressed, it became emblematic of the hacker ethic, and access to DeCSS became an end unto itself.

Corley, when asked why he founded *2600* magazine, noted:

> Well, I saw the need for information to be spread beyond computer nerds, people who are just simply calling into bulletin boards. . . . I thought it would be nice, because these people had so much to say, if there is a way, a forum for them to say it and actually read it on paper, and since nobody else was doing that, I figured why not. . . . We try and bring these people together, whether they are representatives of the government, people from different countries, 12-year-old kids who are just learning something, we try to bring them all together in the same room so they can share information and bring something out of that, and we find that many relationships are forged from this that last for a very long time. (Universal v. Corley [2000], Testimony of Eric Corley)

Consistent with other accounts of the hacker ethic, the information presented by *2600* has over the years had an element of playfulness with technology that illustrates an "I wonder if I can do this" attitude toward complex technological systems (see Raymond 2001 and Stallman 2002). For example, some articles have been instructive on how to explore or manipulate complex computer or communication systems. Titles of past articles in the magazine include "Snooping via MS Mail," "Cellular Interception Techniques," "Tips on Generating Fake ID," "AT&T's Gaping Hole," and "Cellular Network Detailed."

In his remarks, Corley showed a hacker's understanding of authority in information sources:

> What we mostly do [at *2600*] is print information. We have an editorial at the beginning of every issue where we expound on various thoughts, which is something that I write, and also in the replies to letters in the magazine, which is also printed every issue. If we give any kind of moral guidance or judgment, that's where it is, but in the actual articles themselves, it is more or less a compilation of material that is already out there, and we kind of present it to the people to show them this

is what people are saying, this is the information that's out there, this is how systems supposedly work or don't work. And people write in with corrections, they write in with additions, and we have a dialog going based on that. (Universal v. Corley [2000], Testimony of Eric Corley)

One of Corley's main points during the trial was that he was entitled to the same First Amendment protections allotted to journalists even though industry lawyers had suggested he was not. Importantly, Corley's view of journalism differed from the court's. A publication such as *2600* is rooted in a "see for yourself" practice that has become common in online reporting, where linking to original documents is part of the standard. Much like the hacker culture in which it is embedded, *2600* in its online version welcomes "crowd knowledge": the expertise of official contributors is parsed through the expertise of the contributing crowd. The authority is established when participants review claims and test or examine them. This is a marked shift in what would be considered typical journalistic approach to reporting facts and is in line with social computing practices that only recently have come into the mainstream in the forms of blogs and wikis.

The practice of letting a dialog establish the authority of knowledge claims runs against the practices and expectations of traditional journalistic reporting, where the tenets of journalistic methods often ensures that the "facts" of a story are related accurately. In fact, from developments in mass media, including scandals that have plagued prominent journalists such as Dan Rather in response to counterreporting by bloggers, such expectations of journalism have been shown to be unrealistic. Given ready access to primary material, readers and media consumers can make their own determinations of what is or is not fact or relevant to the accurate telling of a story. Therefore, the expectations of journalism in new media have shifted to where journalists are not only expected to present their version of the story, but also to "link" to the primary documentation that led them to their conclusions. This attitude is clearly informed by the hacker ethic, which calls for information transparency. Corley tried to illustrate this fact to the court and repeatedly noted that *2600* could not have presented a credible piece of journalism to its *particular* readership unless it also presented the DeCSS code.

The plaintiffs and the court never accepted this point, however, perceiving journalism in a traditional sense and not in the sense Corley was presenting it. The following exchange illustrates this difference:

Plaintiffs: You began posting DeCSS on your web site in November of 1999?
Corley: That's correct.

Plaintiffs: Is it your testimony that you did that as a journalist to write a story?
Corley: That's correct.
Plaintiffs: Could you have written the identical story without the posting, using the letters DeCSS as many times as you wanted in the story?
Corley: Not writing a story that would have been respected. . . . You have to show your evidence and in this particular case, we would be writing an evidence without showing what we were talking about and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to, what bit of technology that doesn't work, what new advancement, what evidence do we have and simply saying that somebody else said something just won't cut it. So in this particular case, we pointed to the evidence itself which was already firmly established out there in the Internet world. We just put it up on our site so we could write our perspective on it and show the world what it was all about.
Plaintiffs: Getting back to the question, in November of 1999, was it possible for you to write a story about DeCSS on your web site, using the letters DeCSS next to each other as many times as you wanted, without posting DeCSS?
Corley: I will take another shot at it. I—basically, the story would not hold any value to our readers if we simply printed allegations without showing evidence. (Universal v. Corley [2000], Testimony of Eric Corley)

Corley's testimony showed a consistency with the hacker subculture that the plaintiffs chose not to accept and that the court dismissed in its decision, stating:

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. (Universal v. Corley [2000], Opinion of Judge Lewis Kaplan)

Corley's testimony gave positive interpretations of hacker practices that the court saw as subversive to established regimes of authority and information ownership. Corley tried to frame his practices within accepted practices of journalism and freedom of information, but he apparently could not be understood by the establishment that he and his comrades were challenging.

Beyond proving consistent with the hacker ethic, Corley also saw posting and distributing DeCSS as a political act against censorship and called it an act of civil disobedience. He told his readers, "We have to face the possibility that we could be forced into submission. For that reason it's

especially important that as many of you as possible, all throughout the world, take a stand and mirror these files" (Universal v. Corley [2000], quoted in Opinion of Judge Lewis Kaplan). The idea that posting code and linking it can constitute an act of civil disobedience tied directly into activists' belief that code is indeed a form of speech and that DeCSS in particular was political in what it stood for as well as what it did functionally.

Touretsky, the Hacker Ethic, and the Futility of Banning DeCSS

Corley's other supporters also framed their defense of DeCSS with the hacker ethic. David Touretsky, for example, painstakingly described his rationale for his Gallery of CSS De-Scramblers, noting that it was meant to convey two important points: (1) that the distinction between functional and pure speech in code is a fallacy; and (2) that code and its publication are an important way in which computer science professionals communicate with each other. His remarks were also consistent with the hacker ethic of free-information flows and an aversion to proprietary claims over it. Specifically, Touretsky reiterated the logical inconsistencies of separating code into functional speech versus pure speech. He stated that an injunction against some iterations of DeCSS would be meaningless in light of the fact that the code could be presented in a number of ways. In other words, if the court wanted to abridge distribution of the DeCSS source code, it would have to engage in the onerous task of abridging all the various forms in which it could be conveyed.

Touretsky used one interesting example to make the point that the DeCSS code had now taken many forms. Andrea Gnesutta had won an online contest for the most ingenious way of distributing DeCSS. Her winning submission was the image shown in figure 6.3. Gnesutta embedded the DeCSS source code in the image, and users were instructed to look at the source code of the image (distributed online) to extract the DeCSS code, which was embedded in the graphic file. In typical hacker fashion, a recursive system was used to distribute the image; the image itself said it was distributing DeCSS, and the code of that image *was* DeCSS.

Pavlovich and Why DeCSS Mattered to the Linux Community

Last, Matt Pavlovich's testimony was important in this case as well. He was a named defendant in the DVD CCA case and was the founder of LiViD, the open-source Linux Video project. His group made the most use of the DeCSS algorithm and authored some important components of the decryption schema. Pavlovich made clear in his testimony how important the DeCSS code was to the continued development of a Linux DVD player, a

Figure 6.3
Winning entry in the Great International DVD Source Code Distribution Contest. From http://www.dvd.zgp.org.

significant and legitimate use for DeCSS. Much of the resistance to the early injunction in the MPAA case and to the DVD CCA case came from the Linux and open-source communities. They saw these cases as direct attacks on their way of socializing and doing business. Open-source development was a foreign concept to many at the trial, however. The content industry representatives opined that open source would not amount to much of a business model, and they marginalized the importance of Linux DVD endeavors. Also, the court made much of the fact that because DeCSS had been designed for Windows, the Linux community could not claim it was intended to help in Linux DVD development. In response, Pavlovich testified that Linux machines had no way of reading the file structure on DVDs. DeCSS had to be designed for the Windows system so that Linux developers could use it to access DVDs and understand the encryption. They could then use this knowledge to develop the player for Linux machines. In spite of these reasons, the court and the plaintiffs complained

that the cost of developing a Linux DVD application was too great. Windows was so widely available, the plaintiffs reasoned, that they could not risk having an application like DeCSS, which, even if it had legitimate uses, would give a great number of Windows users the ability to pirate DVDs. In this fashion, the Linux community's interests were marginalized and subsumed to the movie studios' interests.

The Corley Decision

It took only six days of trial for Judge Kaplan to find for the plaintiffs. In so doing, he issued a permanent injunction on Eric Corley with regard to the distribution and linking of DeCSS. As in the formulation of the DMCA, this decision was influenced not by actual data on personal pirating of movies or on data concerning damages, but rather on speculation of future losses.

Corley sought to appeal the injunction to the US Second Circuit Court and argued that the lower court had overrun his free-speech rights. Specifically, his defense noted

1. That the press can be enjoined from publishing truthful material because others, unrelated to the publisher, may someday use that material to violate the law.
2. That the press may be enjoined from even linking to such material.
3. That a lesser degree of First Amendment protection applies to expression that is "functional."
4. That Sect. 1201 [of the DMCA] trumps any right of fair use of digital works by preventing publication of technologies that allow fair users to have access to the works. (Universal City Studios, Inc. v. Corley, US Court of Appeals [2nd Cir. 2001])

Also, Corley's defense made note of the open animosity the court had shown the defendant during trial. Indeed, the court in all phases of the case had deployed some truly unfortunate metaphors to describe DeCSS and the work of hackers. It said that DeCSS was like a propagated outbreak epidemic where "individuals infected with a real disease are driven to seek medical attention, and are cured of the disease. Individuals infected with the 'disease' of the capability of circumventing measures controlling access to copyrighted works in digital form, however, do not suffer from having that ability. They cannot be relied upon to identify themselves to those seeking to control the 'disease.' And their self-interest will motivate some to misuse the capability, a misuse that, in practical terms, often will be untraceable" (Universal v. Corley [2000], Opinion of Judge Lewis Kaplan).

Comparing hackers to assassins, the court noted, "Computer code is expressive. To that extent, it is a matter of First Amendment concern. But computer code is not purely expressive any more than the assassination

of a political figure is purely a political statement. Code causes computers to perform desired functions. Its expressive element no more immunizes its functional aspects from regulation than the expressive motives of an assassin immunize the assassin's action" (Universal v. Corley [2000], Opinion of Judge Lewis Kaplan).

These metaphors to describe hackers and their work served to alienate them further and paint their work as activities deplorable within society. But hackers and the open-source community had strong allies. On appeal, the case was argued by Kathleen Sullivan, the dean of Stanford Law School, and the briefs in support of Corley's position read like a *Who's Who* of legal scholarship and activism in the field of digital copyright (see table 6.2).

Despite the strong support from the academic and technical community, however, the appellate court affirmed the lower court's application of the DMCA, acknowledging that issues of equitable balance in copyright were to be settled by Congress. Corley and his supporters chose not to appeal the decision any further, noting that by the time any new decision was pronounced, DeCSS would be so widely available that an appeal would be irrelevant.

Table 6.2
Corley's Supporters in Universal v. Corley

Name of Supporter	Affiliation
Peter Jazsi	Professor, Washington College of Law, American University
Jessica Litman	Professor, Wayne State University
Pamela Samuelson	Professor, University of California at Berkeley
Ann Beeson	Associate Legal Director, American Civil Liberties Union Foundation
Christopher Hansen	National Staff Counsel, American Civil Liberties Union Foundation
Andrew Grosso	Association for Computing Machinery Committee on Law and Computing Technology
Julie E. Cohen	Professor, Georgetown University Law Center
Yochai Benkler	Professor, New York University School of Law
Lawrence Lessig	Professor, Stanford Law School
David A. Greene	Executive Director, First Amendment Project, Oakland, Cal.
Jane E. Kirtley	Professor, Silha Center for the Study of Media Ethics and Law, University of Minnesota
Erik F. Ugland	Graduate Assistant, Silha Center for the Study of Media Ethics and Law, University of Minnesota

Conclusion

In sum, this case put on trial the practices of academics such as David Touretsky, hackers such as Eric Corley and his readership, and Linux/open-source developers such as Matt Pavlovich. These groups proved difficult to suppress, primarily because they had the technological means to avoid the consequences of ignoring enjoinment and fomenting subversion. Furthermore, these groups had strong allies in institutions of higher learning, the media, and the legal profession. Even though Judge Kaplan sided with the plaintiffs, few of his stipulations would be met, and DeCSS would remain widely available.

But has DeCSS contributed to online pirating as feared? As noted earlier, economists and industry analysts wondered whether the projected losses in revenue due to DeCSS were accurately calculated, noting that individuals would not necessarily buy a movie if they could obtain it otherwise for free. Furthermore, the court relied heavily on presumptions of broadband penetration and the specter of Napster to inform its opinion. It noted that "while not everyone with Internet access now will find it convenient to send or receive DivX'd [compressed versions of movies] copies of pirated motion pictures over the Internet, 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" (Universal v. Corley [2000], Opinion of Judge Lewis Kaplan).

Recent studies show that broadband penetration has steadily risen over the past few years. Yet Americans who share copyright-protected content have been increasingly doing so outside of the traditional peer-to-peer fashion—using iPods, for example (Rainie and Madden 2004). The content industry's efforts have contributed to curbing distribution of pirated content, yet this outcome may be due to the music industry's prosecution of individual users[7] rather than to suits against technology makers, who have not been handed complete defeats in the courts.[8] Also, enforcement may not be the only reason many users do not share files online. The availability of file-distribution businesses has helped funnel would-be consumers into legal channels, for example.

Illegal movie distribution on the Internet never reached the level of illegal online music sharing, for a variety of reasons. First, even though broadband penetration continues to increase, the time required to transfer a movie file, even when compressed, can be quite long. Second, peer-to-peer networks tend to be very unreliable in terms of the

continuity of a given connection and in terms of the content actually available. Third, the compressed format must be viewed on a computer, which is an inconvenience for those who enjoy movies on their TV sets. Fourth, if a file is downloaded in a format that can be viewed on a television, such as Super Video Compact Disc (SVCD) or Video Compact Disc (VCD), it will be quite big (between 1.5 to 3.0 gigabytes); it must be burned onto multiple CDs, and many home DVD players will not play SVCD or VCD formats. Fifth, even when compressed, these videos take up about 650 megabytes of disk space. One of the reasons the music-distribution phenomenon took hold was that the mp3 format compressed music files to about 3.5 megabytes with little loss of quality. Therefore, distributors could have hundreds of songs stored on their hard drives without taking up much space. This is not the case for video, where a computer movie library would take up a great deal of space and be difficult for the average computer owner to maintain and share. Taken together, these technological realities, not the legal realities, have kept video from being shared in the fashion that the movie industry and the courts predicted. With the advent of mobile video (streaming), perhaps this state of affairs may change, but that remains to be seen. And last, even though there is illicit sharing of video online, there has yet to be convincing evidence that the movie industry has lost any revenue to it; its sales continue to be healthy. If such losses do occur, other emerging entertainment media that compete for the "entertainment dollar" must be accounted for.

Most recently, however, torrent technology (BitTorrent is discussed in chapter 8), together with effective video compression and higher bandwidth penetration, has overcome some of the technological hurdles that originally made video distribution impractical (primarily bandwidth limitations and the preservation of visual quality). Although it remains to be seen what the actual impact of such advances are, torrent technology signals yet another instance of technological systems that are made with explicit social-cultural intentions (sharing information efficiently on bandwidth-limited networks) and that run up against copyright owners' attempts to control distribution channels. In Sweden, this issue went to court when owners of the torrent site thePirateBay.org were found guilty of contributory infringement—not for distributing movies, but for distribution of torrent seeds that would allow users to distribute content (not just video) in a peer-to-peer fashion.

The court verdict not withstanding, users have framed the torrent system as a viable content-distribution system alternative to that governed

by encryption, DRM systems, and centralized services such as Amazon.com and iTunes. The case study in the next chapter shows resistance by users and activists to such centralized systems of distribution and consumption. In iTunes and its DRM system, users and hackers found an important target for technological resistance, and they designed and used hacks with explicit values rooted in the movement's ultimate belief that users ought to have freedom in their consumption and use of digital content.

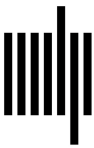
The Digital Rights Movement

The Role of Technology in Subverting Digital Copyright

By: Hector Postigo

Citation:

The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright
By: Hector Postigo
DOI: 10.7551/mitpress/8698.001.0001
ISBN (electronic): 9780262305334
Publisher: The MIT Press
Published: 2012



The MIT Press

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Postigo, Hector
The digital rights movement: the role of technology in subverting digital copyright / Hector Postigo.
p. cm. — (The information society series)
Includes bibliographical references and index.
ISBN 978-0-262-01795-4 (hardcover: alk. paper)
1. Copyright and electronic data processing. 2. Digital rights management. 3. Hacktivism. 4. Internet—Law and legislation. 5. Piracy (Copyright)—Prevention. 6. Fair use (Copyright). I. Title.
K1447.95.P67 2012
345'.02662—dc23
2012004559

10 9 8 7 6 5 4 3 2 1