5 DeCSS: Origins and the Bunner Case

Like the Sklyarov case, the DeCSS case, another important landmark in the evolution of the digital rights movement, involves the development of a technology that infringed on the DMCA's anticircumvention provisions. The movement framed the prosecution of individuals who were linking to the DeCSS source code as an infringement on free speech and a disincentive to innovation. This chapter shows the changing configuration of technology and users. Whereas the AEPBR was a consumer product that came to be politicized through the legal process and movement framing, DeCSS, which emerged from hacker groups rooted in the open-source/free-software movement, came with some politics already articulated in its design. DeCSS designers imagined users who had advanced technical capabilities but also saw them as key intermediates who would bring DVD players to wider publics using the Linux operating system. DeCSS served as a "locale" for projecting other important movement frames and highlighting the logical problems in the way the law understood journalism, code as speech, and technological innovation. Like the AEPBR before it and iTunes after it, the DeCSS technology became meaningful beyond its functionality, and the discourse surrounding it helped solidify important movement beliefs.

Although both this chapter and the next focus on DeCSS, they examine different cases that highlight the different approaches that the content industry and movement advocates took in arguing against or for DeCSS's legitimacy.

DeCSS

The DeCSS story has its beginnings with the Content Scrambling System (CSS) present in all DVDs carrying commercial films since 1999. Matsushita, the parent company for Panasonic, and Toshiba jointly developed the CSS

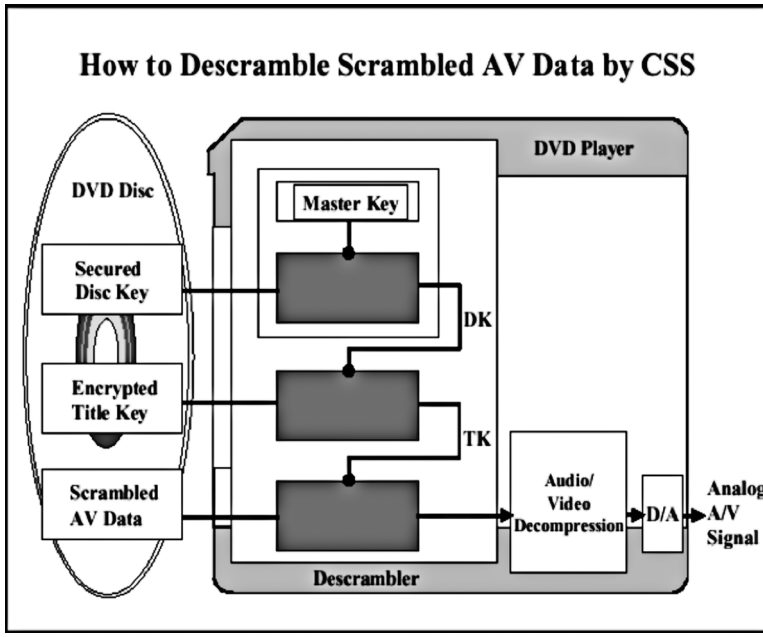


Figure 5.1
Schematic of how CSS works. From Touretzky n.d.

technological protection measure and incorporated it into the standard DVD format. The CSS technological protection measure uses a series of keys to encode the video content on DVDs and establishes the technological system that enforces the DVD's licensing terms. As the schematic in figure 5.1 shows, there are three encryption keys associated with DVD playback: (1) the master key on the DVD player; (2) the disk key on the DVD; and (3) the title key, also on the DVD. A DVD player uses its master key to decrypt the disk key, which it can then use to decrypt the title key. In turn, the title key can be used to decrypt the actual content on the DVD.

Because all DVDs are encoded with CSS, all DVD players must have a licensed CSS master key that allows them to decrypt the content. Because the master keys are licensed, all DVD player manufacturers pay a royalty to the movie industry through its representative, the DVD Copy Control Association (DVD CCA). It is important to note that CSS is not considered a DRM system because the user is given no privileges over the content on the DVD. In contrast, with a DRM system a user might have some limited copying or distribution privileges. Thus, CSS is not like the eBook copy-protection technology.

As noted earlier, the CSS does enforce licensing terms that (1) dictate regional playback permissions so that DVD players in the United States will not play DVDs bought in China or Europe; (2) designate certain sectors on the DVD as non-fast-forward sectors, such as the parts on the DVD that contain the standard FBI warning and, in some cases, commercials and adverts; and (3) prevent content on DVDs from being copied on VHS recorders by interfacing with the Macrovision technological protection measure, which is standard on VCRs.[1]

As personal computers (PCs) and then DVD players became mainstream consumer devices in the late 1990s, DVD players became standard hardware on PCs. However, all DVD players made for PCs at the time had software support for only Windows systems, so DVD players for alternative operating systems, such as the open-source system Linux, were left out of this market. Open-source systems must have "open" applications that make source code available, so these players and the software that ran them could not comply with the licensing terms. To get around this hurdle, the open-source community set out to design drivers and other software that would allow the Linux system to use DVD players.

In October 1999, an anonymous German programmer known only by his online name "Ham" cracked the CSS encryption algorithm and released it to two hacker groups working on DVD player applications for the Linux operating system: the Drink or Die (DoD) group from Russia and the Masters of Reverse Engineering (MoRe) group, whose members were distributed throughout Europe. Both groups used the decryption algorithm to design applications that would not only read content from DVDs but also "rip" the content from the DVD and allow it to be stored in an unscrambled format on a PC's hard drive. DoD designed the application DoD DVD Speed Ripper, and MoRe designed DeCSS. Although the two applications were designed simultaneously and released within weeks of each other, DeCSS garnered the majority of media attention for two reasons. First, DeCSS worked for every movie title in DVD format available at the time; in contrast, Speed Ripper had some difficulty with certain titles. Second and most important, the DeCSS source code was released to the DVD Linux development community, making the CSS decryption algorithm a matter of public knowledge. This meant that anyone could look at the DeCSS source code and glean from it how CSS scrambled video content. Therefore, anyone with enough knowledge of cryptography could design his or her own DeCSS-type program.

The significance of having the DeCSS source code available to the public cannot be overstated. It impelled the DVD CCA to start its legal campaign

against individuals and organizations linking to or distributing the source code. It was this legal campaign that gave the digital rights movement another opportunity to frame its ideals along lines congruent with free speech and fair use.

The Bunner Case

Two months after DeCSS was released on the Internet, the DVD CCA and the MPAA separately filed suits in California and New York against a host of individuals posting or linking to posts of the DeCSS application and its source code. The two cases took different approaches in explaining why DeCSS posed a danger to the motion picture industry.

In DVD CCA, Inc. v. Andrew Bunner et al. (California Superior Court, Santa Clara County, 1999), the DVD CCA sought an injunction on distributors and Web sites linking to the DeCSS source code and application, arguing that posting DeCSS was a misappropriation of trade secrets. In its complaint to the court, the DVD CAA argued that only licensed DVD player manufacturers and their affiliates had access to the CSS code and that those manufacturers were bound by the license agreement not to reveal the CSS code. The existence of DeCSS implied that CSS must have been accessed in breach of the license agreement, so those individuals posting DeCSS, because it was developed using a misappropriated trade secret, must be enjoined from continuing to post the information. The DVD CCA named twenty-five defendants and more than five hundred "John Does" in its complaint to the California Superior Court in Santa Clara County. Some of the named defendants were from Denmark, France, England, Germany, and Norway. The DVD CCA argued that hackers had illegally obtained master keys by hacking the well-known DVD player application X-ing for Windows systems. They noted that anyone running X-ing on their computers would have to click-through a license agreement that precluded the user from reverse engineering the software.[2]

Many of the defendants in the case sought legal advice and help from the EFF, and so it once again found itself as a central organization in voicing important points about the DMCA's impact and the growing technological enforcement of copyright. The EFF noted that to enjoin hackers, cryptographers, research scientists, and Linux developers from posting and distributing the source for DeCSS would be an abridgement of First Amendment rights. Furthermore, the EFF noted that a court-administered gag order on discussing these types of encryption technologies would have a chilling effect on research and development in cryptography.

In their statements to the court, the defendants, some of whom were well-known cryptographers, noted that CSS was highly flawed and highly susceptible to attack and that DeCSS was consistent with professional practices of exposing security flaws in supposed trusted systems. One defendant, a graduate student in computer science at Berkeley, said: "I examined the CSS encryption algorithm soon after its flaws were first revealed to the public. In my opinion, the CSS was extremely poorly designed. . . . I believe breaking it would make a fine homework exercise for a university-level class in cryptography and code breaking" (DVD CCA v. Bunner et al. [1999], Declaration of David Wagner).

The defendants also argued that DeCSS would be of great help in designing software to play DVDs on the Linux operating system, a system ignored by the DVD CCA. They defended their decision to keep the code public because they "felt that providing others with access to the DeCSS program, and thereby enabling Linux users to play DVDs, was important because it would make Linux more attractive and viable to consumers, thereby making Linux a more viable and accepted Operating System platform" (DVD CCA v. Bunner et al. [1999], Defendant Andrew Bunner's Declaration).

Furthermore, they pointed out that claims that DeCSS would lead to rampant piracy were greatly exaggerated, noting that most computer and Internet users lacked the technological know-how and communication resources to traffic in large volumes of media. For example, one programmer explained that hard-drive limitations alone would preclude computer users from pirating movies. Hard drives had about a thirty-gigabyte capacity at the time, enough for only three or four movies. Furthermore, it would take days to properly encode the files to be viewed on the computer screen, and no commercial DVD burners were yet available. "CSS primarily prevents one from building DVD players without permission from the DVD industry, and does not prevent large-scale copy of DVD content," noted one defendant (DVD CCA v. Bunner et al. [1999], Declaration of David Wagner). The majority of DVD piracy, he continued, occurs through large operations where the content of DVDs is imaged directly onto blank DVDs, encryption included.

Defendants from outside the United States also submitted statements for the court. Most interesting for our purposes are the statements from defendants from Norway, the home country of Jon Johansen, the young man partially credited for designing and posting DeCSS. Although Johansen was not named a defendant because he initially removed his posting of DeCSS, many defended the posting of DeCSS in Norway, citing

Norwegian statute that gave users the right to reverse engineer. They argued that this right could not be given up with a click-through agreement administered by X-ing. Although the merits of a click-through license have not been settled in the United States or Norway, the conflict between local copyright laws and international copyright regimes is a recurring theme in the global regulation of intellectual property. It was highlighted when many supporters of DeCSS questioned how the United States justified enforcing its laws (on trade secret, for example) on citizens of other countries.[3]

Much of the frustration expressed by the defendants centered on what appeared to be unfair regulation of regional encoding that prevented DVDs made in the United States from being viewed in Asia or vice versa. Defendants complained that CSS was not designed primarily to protect content on DVDs because a weak encryption would appear vulnerable to even the novice cryptographer. Rather, defendants believed that the CSS was a way to control traffic of movies from one part of the world to another so that the film industry could control release dates and prices for different regions.[4] They saw this control as an unfair business practice and thus felt justified in circumventing the CSS.

Despite the arguments made by the EFF and the defendants, Judge William Elving of the California Superior Court decided to grant a temporary injunction on distribution of the DeCSS code and application. At the same time, however, he refused to enjoin defendants from linking to the code because, he reasoned, that linking was a central function of the Internet. The judge noted that although there was no clear indication that the defendants or even Jon Johansen had violated a click-through license in order to develop DeCSS, the circumstantial evidence overwhelmingly suggested that the code had been derived by some violation of the license. This issue was and continues to be debated. Many of the hackers who had commented on DeCSS during its development and release noted that the makers of X-ing had failed to encrypt their keys in the program itself and therefore had made it very easy for the keys to be found. The makers of X-ing denied having exposed the keys in this fashion, knowing well enough that such a breach of security on their part would also make them liable for the loss of trade secret. Even if the keys were unencrypted, they said, hackers had to look at the X-ing's source code and therefore must have violated X-ing's license agreement.

In one of his final remarks on the case, Judge Elving noted that although the code was barred from the Internet, discussion of it was not. He noted, "Nothing in this Order shall prohibit discussion, comment or criticism, so

long as the proprietary information identified above is not disclosed or distributed" (DVD CCA v. Bunner et al. [1999]). Defendants perceived this directive as inconsistent—the equivalent of saying you can discuss *War and Peace*, but no one should be able to read it. This difficulty did not go unnoticed at the time, and the EFF appealed the injunction. Despite the setback, fifty-two of the seventy-two named defendants and most of the five hundred unnamed defendants continued to post DeCSS in some form or another.[5]

When the injunction was appealed, however, the Appeals Court of Southern California overturned it based on its interpretation of copyright law, trade-secret law, and precedents in First Amendment decisions concerning software as expressive or "pure" speech.

First, the appellate court found that the precedents that the plaintiffs had used to show that injunctions had been awarded in trade-secret cases did not compare to the case before the court. The DVD CCA had used precedents describing injunctions to direct violators of secrecy agreements, and the court reasoned that the Internet posters were not direct violators. Furthermore, the court found that because the DVD CCA was trying to bring suit against Andrew Bunner under trade-secret law, which is designed specifically for those who have voluntarily entered into a contractual agreement (something Bunner did not do), that law could come into conflict with the First Amendment. In such a case, protection of free speech would take precedence. *The court implied that had the plaintiffs couched their arguments under copyright law, then the court would have had to balance carefully between two constitutionally protected rights.* As it was, the appellate court found that software *is* a form of speech and that the lower court exercised prior restraint of the defendant's speech, something that has been consistently opposed by the Supreme Court (see, for instance, Universal City Studios, Inc. v. Corley, 273 F. 3d 429, US Court of Appeals [2nd Cir. 2001]). Importantly, the content industry argued both the Sklyarov case and the Reimerdes case, discussed later in this chapter, as copyright cases, so the court in those cases had constitutional grounding when it found for the content industry, a luxury the Bunner court did not have. Furthermore, the court of appeals in Bunner, unlike the court in Sklyarov, noted that although source code has an only functional speech element, that element should not preclude it from being protected as pure speech.

The issue of code's speech and nonspeech elements was an important theme in these early cases in the digital rights movement. As noted in chapter 4's analysis of the Sklyarov case, the court presented an arbitrary distinction between speech and nonspeech elements of code. As I argued

in that chapter, the speech/nonspeech distinction is made for the sole purpose of regulating speech that has become commercially important but that is increasingly politicized. The central error in all understandings of code is that it is perceived as both expressive and functional. Code is not functional in any sense; it is a set of instructions to a computer. The computer is the functional component. *If code is written with the expressed intent of resistance, then it is expressive speech telling computers exactly how to help the movement achieve its goals*.

Not satisfied with the appeals court decision, the DVD CCA petitioned the California Supreme Court for further review. In its petition, it relied heavily on *Universal City Studios, Inc. v. Reimerdes* (111 F. Supp. 2d 294 [SD NY 2000]), which had just been decided in the State of New York. The New York court rejected as gross misinterpretation the view that software code is speech. In the DeCSS case, returning to the idea of speech versus nonspeech elements, the DVD CCA attacked the appeals court's refusal to see that DeCSS was primarily functional speech, which would mean that it required only an intermediate level of free-speech protection. It noted,

> By posting DeCSS on his website, knowing that it contained stolen trade secrets, Respondent Bunner engaged in no expressive discourse about issues of public concern. . . . The Court of Appeal erroneously applied the First Amendment doctrine against prior restraints that can be found in cases involving pure, political speech, such as New York Times Co. v. United States (1971) 403 U.S. 713 (the Pentagon Papers case) . . . without considering how dramatically different the speech in those cases was from the dissemination of stolen trade secrets here. The speech sought to be enjoined in *New York Times* . . . lay at the very heart of First Amendment concern—public debate about policy issues. (DVD CCA v. Bunner et al. [2001], California Supreme Court, Petition for Review).

But what constitutes public discourse of social concern and importance to debate about public policy? Surely, as code becomes technological resistance, it constitutes some form of speech about the way technologies ought to work. And is it not important discourse within communities of hackers? As these technologies become widely used, it is important for groups outside of those narrowly interested in the workings of technology to discuss its wider implications. The point is that as technologies are further marginalized by law yet remain valid forms of discourse and acceptable tools for getting something done, then they acquire meanings that are consistent with resistance. DeCSS, eBook, and later on iTunes hacks follow this trend from controversial consumer item to technological resistance. The point the DVD CCA made regarding this issue turns a blind eye to that reality.

The DVD CCA continued to see technologies such as DeCSS as "hackerware" and so took the case to the California Supreme Court, which remanded the appellate decision back for review. In its discussion of the merits of the analysis, the California Supreme Court disagreed with the appeals court interpretation of code as speech worthy of strict protection, choosing not to engage in an analysis of speech versus nonspeech elements, but rather focusing on whether trade-secret law allows for prior restraint. The court found that the injunction was content neutral (not concerned with the opinions expressed by the code, but rather by the code itself) and found that an injunction on Bunner was subject to intermediate speech protection. Finding that although a ban on posting impinged on Bunner's free speech, it served a legitimate government interest, and the court noted that the appeals court had wrongfully judged the DeCSS case as a case of prior restraint subject to the strictest free-speech analysis. The court did, however, request that the appeals court review the Superior Court's application of the injunction with respect to California's trade-secret law, inquiring whether CSS had entered into the public domain and no longer deserved trade-secret protection.

Although all the legal considerations in the case (e.g., trade-secret law) are beyond the scope of this discussion, what is interesting is how the EFF, whose lawyers argued the case, chose to interpret this decision. The California Supreme Court's argument that code merits only intermediate speech protection was a blow to the movement's claim that code ought to be protected speech in the highest sense. This argument was consistent with other decisions occurring at the time (such as in the Reimerdes, Corley, and Sklyarov cases) and should have been considered a defeat in the movement's attempt to define circumvention technologies as matters of free speech. The EFF, however, spun the decision in the best possible light, stating in a press release curiously titled "California Supreme Court Upholds Free Speech in DVD Case" that "the appeals court can now examine the movie industry's fiction that DeCSS is still a secret and that a publication ban is necessary to keep the information secret. . . . DeCSS is obviously not a trade secret since it's available on thousands of websites, T-shirts, neckties, and other media worldwide" (Cohn 2003).

The DVD CCA anticipated this response and quickly tried to have the case dismissed in the appeals court before the court could judge that CSS was no longer a trade secret. Cognizant of this tactic and, in fact, aware that DVD CCA had delayed judgment for more than two years under the pretext of clarifying the issue, the court denied the dismissal and reversed the injunction on Bunner on February 27, 2004, four years after

the injunction had been issued. The court noted some important developments in the case. First,

> [t]he lawsuit outraged many people in the computer programming community. A campaign of civil disobedience arose by which its proponents tried to spread the DeCSS code as widely as possible before trial. Some of the defendants simply refused to take their postings down. Some people appeared at the courthouse on December 28, 1999 to pass out diskettes and written fliers that supposedly contained the DeCSS code. They made and distributed tee shirts with parts of the code printed on the back. There were even contests encouraging people to submit ideas about how to disseminate the information as widely as possible. (DVD CCA v. Bunner et al., Court of Appeal, State of California (6th District, 2004], Decision on Remand)

Second, the court noted that just because someone chooses to publish a trade secret does not mean that it ceases to be a trade secret or that the person is not liable for damages. Rather, once that information is in the public domain, no state action can bring it back without abridging speech. The court noted that the evidence demonstrated that in the Bunner case "the initial publication was quickly and widely republished to an eager audience so that DeCSS and the trade secrets it contained rapidly became available to anyone interested in obtaining them" and that "DeCSS had been so widely distributed that the CSS technology may have lost its trade secret status" (DVD CCA v. Bunner et al. [2004], Decision on Remand). Thus, because CSS had lost trade-secret status by the time the injunction was issued, the appeals court found that the Superior Court's injunction on Bunner overextended its powers under California's trade-secret act.

Conclusion

The outcome of the Bunner case was important for the digital rights movement in many respects. On the one hand, it was a victory for the movement. The EFF, as it continued to define itself as *the* SMO concerned with digital rights issues, showed that the content industry could be defeated in its attempts to censor technology that can potentially benefit consumers. The Bunner case (and really the whole of the DeCSS legal history) highlighted the potential of seeing code as speech and the consequences for the movement. It illustrated that technologies meant to allow user-centered functions, such as copying for personal backups or reverse engineering to design a DVD player, not only had a functional purpose but were meaningful as acts of political speech. On the other hand, the fact that the court failed to agree with the "code as speech" argument was a failure for the movement in that this particular frame did not gain traction

in institutional settings. Therefore, although the movement was increasingly able to articulate its viewpoint along important themes (such as fair use and free speech), these themes and their related arguments continued to have a hard time finding positive reception outside the movement and its allies. In the Bunner case, the injunction was ultimately denied based on practical issues: the DeCSS had made the CSS code a matter of public knowledge, and it was too late to put the cat back in the bag. The decision was not based on perhaps the more important and enduring issues of fair use and free speech, which could have greatly helped the movement's cause in future court cases.

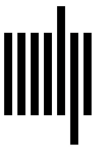
The Digital Rights Movement

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