

The DVD Rebellion

BUY A COPY OF *THE MATRIX* on DVD and take it home. Play it on a Mac or on a Windows PC and you're in for a pretty good time. But play it on a PC running the Linux operating system, and the movie industry says that you're breaking the law.

Your transgression is that of "circumvention," a criminal act created by the 1998 Digital Millennium Copyright Act. You see, the video on DVDs is scrambled. Windows and Macintosh DVD players licensed by the DVD Copy Control Association contain the algorithms to unscramble the signal. The Linux DVD player contains these secrets as well. But since the Linux-based program isn't licensed, using the software constitutes an illegal circumvention of copyright management.

Things have gotten nasty as this new crime gets its tryout in the legal system. Last year, eight major film studios, all members of the Motion Picture Association of America, sued the magazine *2600* for posting on its Web site a program that unscrambles DVDs. Not only did the organization win its case, but U.S. District Court judge Lewis A. Kaplan even barred *2600* from posting links to other sites that contained the program. That case is now on appeal.

For the movie industry, the DVD case is about piracy and revenue protection. For the programmers among us, the attempts to suppress this software are an attack on fundamental freedoms of speech and inquiry. It is a battle the movie industry is sure to lose. The only question is, "when?"

At the core of the controversy is

technical data about the copy protection techniques used to make DVDs. The information on each DVD is protected by an encryption scheme called the Content Scramble System, or CSS. This technology prevents computer users from duplicating a movie, compressing it down to fit on a CD-ROM, and then giving copies to their friends. Playing the DVD entails decrypting the data—an act that used to require a licensed DVD player with the appropriate descrambling algorithms, stored either in a program or in a set-top box.

Then in 1999, an anonymous European programmer cracked the code and distributed a program—called DeCSS—over the Internet. Ever since, the movie industry has been filing lawsuits and sending threatening letters to individuals and businesses that distribute this and related DVD decryption programs.

How did we get here? In the 1980s, compact discs revolutionized high-fidelity sound. But CDs were not well suited for movies: their roughly 600 megabytes could store barely 10 minutes of video. (Advanced compression systems can put an entire movie on a CD, but the quality suffers.)

Enter DVDs, which can store more than two hours of compressed video on a disc the same size as a CD. If you want to make your own DVDs, you can buy a recording drive for less than \$500. Rewritable discs that hold 4.7 gigabytes cost about \$30.

It's easy to see why the movie studios are worried. The price of recordable DVD discs is sure to fall. Three years ago, writable CD-ROMs cost \$2; today, they're 40 cents or less. Expect writable DVDs for \$5 by mid-2002. Equipped with programs like DeCSS, consumers will be able to make high-fidelity copies of DVDs on the cheap.

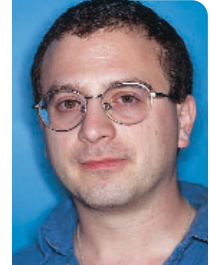
Movie studios have long been terrified of home recording technology. In 1983, Sony and Universal City Studios



DUNG HOANG

faced off over the legality of home videocassette recorders. Universal said VCRs should be outlawed because they could be used to make illegal copies of copyrighted materials. But in 1984, the U.S. Supreme Court ruled that “the sale of [VCRs] to the general public does not constitute contributory infringement of respondents’ copy-

For the movie industry, the issue is piracy. But for programmers, the attempt to suppress DVD unscrambling software is an attack on fundamental freedoms of speech and inquiry.



rights.” The Court reasoned that recording a television show at one time for viewing at another fell under the “fair use” provision of copyright law.

The movie industry has never been happy with this decision, and in 1998 it prevailed upon federal lawmakers to do something about it. Unable to overturn a Supreme Court ruling, Congress did the next best thing: it passed the Digital Millennium Copyright Act, which created the crime of “circumvention.”

Copyright is supposed to balance the rights of publishers and the rights of the public, explains Cindy Cohn, legal director of the Electronic Frontier Foundation, a civil-liberties organization defending *2600* magazine. The new law, says Cohn, makes an end run around fair use by making it illegal for any person to use or distribute technologies that can circumvent a copyright protection system. Because of the public’s right to fair use, Cohn says, “every time the content holders have tried to reach out and get more control, as they did with VCRs, the Supreme Court has slapped them down.”

It isn’t just movies that could fall under this new form of protection. Any company that wants to prohibit fair use can simply wrap its products—movies or books or magazine articles—in a thin layer of cryptography. The content purveyor could then apply restrictions that made it possible to view the material only by using the publisher’s

proprietary software. If the software doesn’t allow fair-use rights, then the 1998 legislation makes it illegal for people to circumvent that software to get their rights back.

The original 1999 program that broke the DVD encryption algorithm was created not for piracy but to let people who bought DVDs play them on computers running Linux. But science marches on. In March 2001, two programmers at MIT reduced the original 215-line decryption algorithm to just six lines. It has become so small that people are putting it at the bottom of e-mail messages as a “signature.” You can even purchase a T-shirt displaying the forbidden code. *Technology Review* would probably not consider printing a 215-line program; the six lines appear below. “The shorter the program gets, the sillier the studios look for trying to suppress it,” says Carnegie Mellon computer scientist Dave Touretzky, who posts a gallery of DVD decoders on his Web site.

Another front in the DVD wars has opened up at Princeton University.

THE DVD UNSCRAMBLER

Six lines of code that have rattled the movie industry

```
s'$/=2048;while(<>){G=29;R=142;if((@a=unqT="C*")[20]&48){D=89;_ =unqb24,qT,@
b=map{ord qb8,unqb8,qT_^$a[-D]}@INC;s/...$/1$/;Q=unqV,qb25,;H=73;O=$b[4]<<9
|256|b[3];Q=Q>>8^(P=(E=255)&(Q>>12^Q>>4^Q/8^Q))<<17,O=O>>8^(E&(F=(S=O>>14&7^O)
^S*8^S<<6))<<9,_(map{U=_%16orE^R^=110&(S=(unqT,"\xb\ntd\xbz\x14d")[_/16%8]);E
^=(72,@z=(64,72,G^=12*(U-2?0:S&17)),H^=_%64?12:0,@z[_%8])(16..271)}[_]^((D>>=8
)+=P+(~F&E))for@a[128..$#a]}print+qT,@a';s/[D-HO-U_]^\$$/g;s/q/pack+/g;eval
```

In April, the Recording Industry Association of America sent computer science professor Edward Felten a chilling letter stating that Felten's publication of a paper on the Secure Digital Music Initiative's watermarking algorithm might constitute a criminal act. Felten pulled the paper from its scheduled release at a conference. Since then, however, it has been all over the Internet.

All this recalls what happened back in the 1990s in response to the Clinton administration's absurd restrictions on cryptography. Strong encryption was classified as munitions; exporting crypto was punishable by up to 10 years in prison and up to a \$1 million fine. So programmers reduced a powerful encryption algorithm known as RSA to three lines of code and plastered it all over the Web; at least three people even had the lines tattooed onto their bodies. In 1997, the U.S. Department of Commerce decreed that exporting this potent snippet of text required a license. Not that it mattered. Two years later, the administration caved.

Mark Litvack, an attorney representing the MPAA, insists "it has not been our intention to stop debate on the merits and values" of DVD encryption. Instead, he says, his organization is merely trying to wipe out Web sites that are distributing illegal "circumvention devices." Thus, in February, the association wrote a letter to Carnegie Mellon demanding that the university remove Touretzky's Web pages from university servers. The university did not comply.

The movie industry lost its battle over DVDs when it decided it would be neat to let people play DVDs not just on TV sets but on computers. There's no way to keep secret something that's distributed to millions of PC users. Information is power, and computers are machines designed to process and distribute information. Moviemakers are about to learn what the Clinton administration learned with crypto: no matter how you legislate, information wants to be free. 