



COMPETITIVE ENTERPRISE INSTITUTE

Tech Briefing 2001

*A Free-Market Guide to Navigating Tech Issues
in the 107th Congress*

The Digital Millennium Copyright Act

by
JAMES V. DELONG

Background. Copyright holders know that if they make their work easily available in digital form, whether over the Internet or on a disk, it can and will be taken by others without payment. The solution is to use a system of technical protection, such as a password or encryption, which allows access only to those approved by the holder. Often, approval is contingent on payment.

Protection systems can be and are circumvented by hackers. To prevent this, in 1998 Congress enacted the “anti-circumvention” provisions of the Digital Millennium Copyright Act (DMCA).

The DMCA.¹ The first part of the act says that “no person shall circumvent a technological measure that effectively controls access to a [copyrighted work].” This part of the statute became effective in 2000. It contains a safety valve, in that starting in 2000, and every three years thereafter, the Librarian of Congress (LOC) is to conduct a rulemaking. The proceeding is to identify any “classes of works” for which application of DMCA would adversely affect legitimate, non-infringing uses of the works. The LOC can then exempt the legitimate users from DMCA’s prohibition.

The next prohibition became effective in 1998. It outlaws the manufacture, import, offering, or trafficking in any technology, product, service, device, component, or part that is (1) primarily designed to circumvent technology of a copyright owner that limits access to a work; (2) has only limited commercially significant purpose other than circumvention; or (3) is marketed for use in circumventing a protective technology. (This is referred to as the “access control” provision.)

The last prohibition, also effective in 1998, repeats the language of the access-control rules, but applies it to any technology, product, etc., that “protects a right of a copyright owner.” (This is referred to as the “copy control” provision.)

Two pieces of the fine print in the access-control and copy-control provisions are important: (1) the use of the word “or”; these requirements are alternative, not cumulative; (2) while these provi-

sions cover technologies that circumvent either access controls or copy controls, the first prohibition—against the act of circumvention—applies only to access controls. An individual having legitimate access to a work who then circumvents a technology limiting that access does not violate DMCA.

The act also: (1) contains complicated exceptions from only the first prohibition for libraries and schools deciding whether to purchase a work; law enforcement; researchers trying to achieve interoperability; encryption research; protection of minors; protection of privacy; and security testing; (2) disclaims any intent to change any other dimension of copyright law; (3) imposes both civil and criminal liability.

Controversies. *Rulemaking.* Starting in 1999, the LOC conducted its first rulemaking on whether to exempt specific classes of works. The proceeding drew 364 comments, and 34 witnesses from 50 organizations appeared during five days of hearings. The final rule exempted only two classes of works: compilations of lists of websites blocked by filtering software, and materials for which access controls fail to permit access because of a glitch.² The LOC found that opponents of DMCA raised many hypothetical problems, but could not persuasively identify specific situations in which the problems were likely to occur.

*The DeCSS Litigation (Universal City Studios v. Reimerdes).*³ In 1996, the electronics industry developed a content scrambling system (CSS) to prevent unauthorized access to the digital video disks (DVD) that record movies in digital form. Manufacturers of DVD players license this technology, paying an administrative fee but no royalties. Manufacturers are required to maintain security to keep the technology from becoming generally available. DVD players cannot make copies of DVDs or export files.

With CSS in place, movie studios began releasing DVDs—over 4,000 titles by mid-2000. By the end of that year, manufacturers had shipped 14 million DVD players to dealers, an estimated 60 percent of which were sold to consumers.⁴ DVDs rapidly became big business, accounting for 35 percent of revenue from the home-video market and 13 percent of total movie-distribution revenue.

Until late 1999, the government forbade export of effective encryption systems, so CSS is based on a weak one: “[CSS] encryption keys are only 40 bits long,” writes CEI’s Ananda Gupta. “It’s not too difficult to crack. By comparison, the program Pretty Good Privacy has keys 128 bits long—

that is, keys with more possible combinations than seconds have passed since the beginning of the universe.”⁵

So, CSS got cracked, and by late 1999 a program called DeCSS appeared widely on the Internet. It can be used to play CSS-encoded DVDs on any computer. Decoded files are long—up to six gigabytes. A compression utility called DivX can reduce them to 650 megabytes, a size that can be stored on a CD-ROM, without significant loss of quality. The combination of the two technologies produces a file that can be burned onto a blank CD, which creates the conditions necessary for mass piracy.

A consortium of movie companies started a campaign to send cease-and-desist letters to websites that posted DeCSS, accusing their operators of trafficking in circumvention devices in violation of DMCA. In January 2000, the studios obtained a preliminary injunction against the site run by Reimerdes. The defendant responded by posting links to other websites offering DeCSS, a list that grew to 500 by mid-2000. At trial, the court enjoined both the website and the links. This case, now on appeal, has drawn numerous participants on both sides, and is the primary arena for an ongoing battle over the wisdom and constitutionality of DMCA.

The contenders. Supporters of DMCA include producers of intellectual property: Motion Picture Association; American Society of Media Photographers; American Society of Composers, Authors, and Publishers; Recording Industry Association; Business Software Alliance; AOL Time Warner; Association of American University Presses; Reed Elsevier, Inc.—the list is long.

The supporters take the view that intellectual property must be protected if its creators are to have any incentive to make it available in digital form. If putting a movie or a software program on DVD means that it will promptly be pirated and mass distributed for free, then no new material will be issued in this form. Since encryption is the key to protecting IP, and since hackers are proving themselves adroit at circumventing the protections, the creators of IP regard legal protection as vital.

Furthermore, *consumers* have a strong interest in the development of effective protection of intellectual property. Consumers need to be able to pay for what they want in a market; they do not want to be dependent on the whims of an advertiser who wants to sell them a product.⁶

The opponents of DMCA are a mixed group. Some are best thought of as adolescent vandals; if movies are there for the taking, they want them,

with no regard for the health of the overall system that produces intellectual property.⁷ Other opponents seem concerned about any innovations that would upset their settled ways of doing business. They talk of the bugbear of “pay per use,” as if this approach were an obvious evil. Actually, it is a new and interesting business model that can produce exponential expansion in the quantity and quality of intellectual property available.

Some—including the defendants in the DeCSS case—seem to be ideologically opposed to the idea of intellectual property. They think IP should be freely exchanged without payment, and regard as legitimate all efforts to undermine an institution that they regard as illegitimate.⁸

Many opponents of DMCA are more nuanced. They acknowledge that IP is, to at least some extent, legitimate and its protection is necessary, but think the act goes too far. (This group takes in a lot of territory, from the proponents of the Open Source movement to people who think DMCA needs only a few tweaks.) Intellectual-property law has always been a complex balancing of the demands and needs of copyright holders and users, and this group says DMCA tips too far toward the former. In particular, they are concerned about ambiguities in the law, about the limited and confused nature of the exceptions, and about the imposition of criminal penalties and harsh statutory damages.⁹ The use of criminal penalties is particularly disturbing. These provisions of DMCA are part of a broader floodtide of overuse of criminal law.¹⁰

Intertwined with concern about the technical reach of DMCA is a more comprehensive point. As a general principle, society should be extremely reluctant to allow the government to suppress a technology, ever. Once the genie of technology suppression is out of the bottle, putting it back is difficult, because dozens of interests will press their special claims on Congress. In this view, it is better not to yield, ever, and to force the threatened interests to find a different approach.

The proponents of the “do not suppress technology” view have collected formidable support from the academic and foundation worlds, as well as from self-interested businesses.¹¹ They raise serious constitutional points, arguing either that: (1) the power to protect intellectual property given to Congress by the Constitution does not give it the power to ban whole technologies; and/or (2) DeCSS and other circumvention technologies are computer code, which is a form of expression, and their suppression is forbidden by the First Amendment.

The First Amendment argument becomes particularly strong as owners of intellectual property try to expand DMCA's prohibition of "trafficking." Is an Internet Service Provider (ISP) "trafficking" if a customer's website offers circumvention technologies?¹² Is a website "trafficking" if it contains a link to another site that provides such technologies? What if a website offers circumvention technologies, but adds a notice that these were not created but gathered from general sources, and that they are "for testing and/or educational purposes only"?¹³

Forcing ISPs to police their customers, or websites to police their links, would quickly reduce "Internet time" to a crawl, and would impose prohibitive costs on the system.

Policy recommendation. Both sides in this controversy make compelling points. Effective protection of intellectual property is crucial not only to the entertainment business but to the entire US economy, which is increasingly based on the value of IP more than on the value of physical assets, such as buildings and machinery.

However, one cannot dismiss the concerns that DMCA is ambiguous and perhaps over-extensive, that criminal penalties are not appropriate, that serious First Amendment values are at stake, that anti-technology laws lead down an exceedingly dangerous path, and that forcing ISPs and websites to police content is an impossible idea.

Supporters of DMCA recognize that those who are concerned about the law raise serious points. However, they must grapple with the reality that the widespread use of DeCSS will certainly inhibit, and may destroy, the DVD industry. Similar programs could wreak havoc on the software industry as well, and on other industries dependent on IP.

In the end, the answer is likely to be the creation of better encryption systems, and the junking of the existing stock of weakly encrypted machines and DVDs. But the feasibility of effective systems is a matter of great dispute, so it is not clear that this answer will work. Probably, it will. Technological protection need not be perfect. It need only raise the costs of piracy sufficiently to make it not worth the hassle for most people, and to keep copyright violations at a low-enough level so they do not destroy incentives to produce intellectual property.

For the present, Congress need not act. It could usefully clean up some of the technical problems with DMCA, but, beyond this, *Reimerdes* is already in the Second Circuit Court of Appeals, and is clearly headed for

the Supreme Court. Any major revision of the act by the 107th Congress would abort the case without settling the important issues, and would only prolong uncertainty.

~ JAMES V. DELONG

¹ DMCA can be found at www.loc.gov/copyright/1201/anticirc.html, the website maintained by the US Copyright Office for the anti-circumvention rulemaking described in this section. This site also contains legislative history, all comments filed during the rulemaking proceeding—a useful source of information on DMCA generally—and the final rule on exceptions.

² Library of Congress, “Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies,” 65 *Federal Register* 64555, 27 October 2000; available at frwebgate5.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=0276225874+0+0+0&WAISaction=retrieve.

³ *Universal City Studios, Inc., v. Reimerdes*, 82 F.Supp.211 (SDNY 2000); available at www.copyrightlaw.homestead.com/Page1.html.

⁴ DVD File, www.dvdfile.com/news/sales_statistics/hardware.htm.

⁵ Ananda Gupta, “The DeCSS Mess: A Study in Unintended Consequences,” *CEI C:\SPIN*, 31 August 2000; available at www.cei.org/CSPINReader.asp?ID=1170.

⁶ See James V. DeLong, “Do You Really Want to be a Product?” *Intellectual Capital*, 3 August 2000; available at www.speakout.com/Content/ICArticle/2899/.

⁷ James V. DeLong, “Barbarians at the Gate: Napster Gets Pushed Back,” *CEI C:\SPIN*, 12 February 2001; available at www.cei.org/CSPINReader.asp?ID=1368.

⁸ In recent years, a strong anti-property ethos has developed in some parts of the culture, nurtured particularly by the environmental movement and the academic community. See James V. DeLong, *Property Matters: How Property Rights Are Under Assault—And Why You Should Care* (New York: Free Press, 1997). The anti-IP movement is closely related.

⁹ See, e.g., Pamela Samuelson, “Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised,” 14 *Berkeley Journal of Law & Technology* 2 (Spring 1999); available at www.law.berkeley.edu/journals/btlj/articles/14_2/Samuelson/html/reader.html. For example, DMCA exempts law-enforcement activities from the ban on the act of circumventing. But it does not exempt production of, or trafficking in, the technologies necessary for law enforcers to circumvent. So the FBI can legally decode a terrorist’s copyrighted communications, but no one can legally sell the decoding technology.

¹⁰ James V. DeLong, *The New Criminal Classes: Legal Sanctions and Business Managers*, National Legal Center for the Public Interest (July 1997); available at centerset.com/regpolicycctr/RegState.htm.

¹¹ A good gateway into this work is the website of the Electronic Frontier Foundation, www.eff.org/IP/Video/MPAA_DVD_cases/20010126_ny_eff_pressrel.html.

¹² See, e.g., Lisa Bowman, “ISP takes a stand in dispute over DVD-cracking code,” *CNET News*, 24 January 2001; available at news.cnet.com/news/0-1005-202-4587946-0.html. DMCA contains provisions exempting ISPs from liability for copyright infringement if they respond promptly to complaints, but this issue is not the same as possible liability for circumvention.

¹³ See www.unixer-ee.com/gifts/disclaimer.htm. (And is this footnote “trafficking”?)