

Pamela Samuelson

Why the Anticircumvention Regulations Need Revision

Like a tempest in a teapot, the storm rages on over DMCA's ambiguous provisions.

Every vision of the digital future foresees copyrighted content widely available via global networks. There is considerable debate, however, about the extent to which this content will or should be distributed in encrypted or other technologically protected form, and available only with permission from the rightsholder.

A highly charged aspect of this debate is whether technical protection systems will undermine the public's right to exercise fair uses of copyrighted works and its access to published information. In the U.S., this debate was an integral part of the struggle over the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) enacted in October 1998. The DMCA makes it illegal to circumvent access controls used by copyright owners to protect their works as well as to develop and distribute circumvention technologies. When enacting the DMCA, Congress believed it was doing everything possible to preserve fair use and public access to information while at the same time protecting the copyright industries against high-tech "burglars' tools." This column argues that this balanced objective may not have been achieved.

RANDALL ENOS

It would oversimplify the facts—although not by much—to say that the battle in Congress over the anticircumvention provisions of the DMCA was part of a larger war between Hollywood and Silicon Valley. Hollywood and its allies sought a broad ban on the act of circumventing a technical protection system and on circumvention-enabling devices. Silicon Valley firms and their allies generally opposed this broad ban, in part, because it would have outlawed reverse engineering, computer security testing, and encryption research. Silicon Valley firms supported legislation to outlaw acts of circumvention facilitating copyright infringement and would have supported narrowly drawn device legislation. However, by colorful use of rhetoric and forceful lobbying, Hollywood

and its allies were largely successful in persuading Congress to adopt broad anticircumvention legislation.

Given the administration's enthusiasm for the strong economic performance of the IT sector, and given the principles the administration endorsed in its 1997 framework for global e-commerce, one might have expected the administration to take a more balanced position on the anticircumvention issues. One can call the DMCA's anticircumvention provisions many things, but one cannot honestly speak of them as "predictable, minimalist, consistent, and simple" components of a legal environment for e-commerce, as the framework principles suggested they should be. The administration instead sided with Hollywood on a key information policy issue and Silicon Valley will likely suffer as a result.

The DMCA's Anticircumvention Rules

There are three anticircumvention provisions in the DMCA. The first is section 1201(a)(1) (A), which generally outlaws the act of circumventing "a technical measure that effectively controls access to a work protected under this title." This rule is subject to seven statutory exceptions and will not take effect until October 2000, in part to allow a study to be conducted of the potential impact of this norm on noninfringing uses of copyrighted works.

Section 1201 also contains two "antidevice" provisions. Sections 1201(a)(2) and 1201(b)(1) both regulate technologies with circumvention-enabling capabilities. The former pertains to technologies that "effectively control access to [copyrighted] works"; the latter pertains to technologies that "effectively protect a right of a copyright owner ... in a work or a portion thereof." As to each, section 1201 states that "no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" if it has one or more of the following characteristics: (1) if it is "primarily designed or produced for the purpose of circumventing [technical] protection"; (2) if it has "only limited commercially significant purpose or use other than to circumvent [technical] protection"; and (3) if it is "marketed by that person or another acting on its behalf with that person's knowledge for use in circumventing technical protection." The antidevice rules have a narrower range of statutory exceptions.

Although administration officials admitted in congressional testimony that its preferred legislation went beyond what the World Intellectual Property Organization (WIPO) Copyright Treaty required, it argued for this broader rule in part to set a standard for other countries to follow. Proponents of the administration's preferred anticircumvention regulations scoffed at arguments made by an alliance of consumer electronics firms and computer and software industry companies about the harm likely to result from broad anticircumvention regulations. They also dismissed as specious arguments made by library and educational groups about threats to fair use and the public domain arising from broad anticircumvention regulations. Yet, Congress eventually heeded some of these concerns.

Exceptions to the Act-of-Circumvention Ban

Section 1201's circumvention-of-access-control provision is subject to seven specific exceptions, as well as being qualified by several other subsections. While these exceptions and limitations respond to the gravest of concerns expressed by digital economy firms, they are narrowly crafted. Congress may eventually need to revise this provision to recognize a broader range of exceptions.

The administration initially sought to an almost unlimited ban of circumvention activities. The only exception in the administration's favored legislation was to enable circumvention of technical protection systems for legitimate law enforcement, intelligence, and other governmental purposes.

Without this exception, suspected Mafia bosses and terrorists, oddly enough, might have been able to challenge attempted law enforcement or intelligence agency decryption of their records or communications.

The administration's favored bill also included a provision stating that nothing in Section 1201 would "affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." Taken at face value, this provision seemed to recognize that circumventing a technical protection system for purposes of engaging in fair use or other noninfringing acts is lawful. Yet some copyright industry representatives argued that fair use should not be an acceptable reason to "break" a technical protection system used by copyright owners to protect their works, likening this act to burglary. However, the legislative history of the DMCA clearly reflects that Congress intended for circumvention for fair use purposes to be lawful.

Digital economy firms and their allies eventually persuaded Congress to create six additional provisions to the act-of-circumvention ban. One enables circumvention for purposes of achieving interoperability among computer programs. A second authorizes legitimate encryption research. A third privileges some computer security testing. Other exceptions responded to nonprofit group concerns. One, for example, provides a limited privilege to circumvent technical protections to ensure personal privacy. Another provision clarifies that software and hardware manufacturers are under no obligation to specifically

design their products to respond to particular technical measures.

However, Congress should have added a general-purpose “or other legitimate purposes” exception provision to Section 1201, recognizing many other legitimate reasons for circumventing technical protection systems that are not, strictly speaking, covered by the exceptions in the final bill (for instance, to determine if encrypted code transmitted via the Internet contains a destructive computer virus or an infringing copy of one’s intellectual property). Without such a provision, courts will have to contort the law or reach unjust results.

A general-purpose exception would add flexibility, adaptability, and fairness to the law. In many other parts of copyright law—with the fair-use doctrine, for example, or the distinction between ideas and expressions—Congress has trusted the common-law process to distinguish between legitimate and illegitimate activities. It should have done so with respect to the anticircumvention rules as well.

Fair Use and the Antidevice Rules

The most puzzling aspect of Section 1201 is whether Congress, in essence, created a number of meaningless privileges or whether it intended for people to be able to develop or have access to technologies necessary to engage in privileged circumvention #5. Only three of the exceptions to the act-of-circumvention rule specifically authorize the creation of tools necessary to achieving a legitimate circumvention activity (the encryption research, computer security, and interoperability privileges). The interoperability privilege exempts

necessary tools from both antidevice provisions of Section 1201, while the encryption and security research privileges exempt tools only from the access-control provision. Section 1201 says nothing about enabling the development or distribution of circumvention tools to enable fair use or other privileged uses.

How could Congress have expressly provided a right to “hack” a technical protection system to make fair uses without also allowing the development of tools necessary to effectuate fair uses? Under some readings of Section 1201(b)(1), a computer scientist who develops software enabling fair use of a lawfully acquired copy of technically protected material would violate the statute, regardless of whether he or she subsequently distributed that software to anyone.

Interestingly, it has long been lawful in the U.S.—at least until the DMCA—to make and distribute software designed to defeat a technical protection system necessary to enable noninfringing uses of copyrighted works. Quaid’s Ramkey software program was designed to defeat Vault’s Prolok copy-protection software. By spoofing Vault’s copy-protect system, Quaid’s customers could make unauthorized copies of the third-party software protected by Vault’s program. Quaid successfully defended against Vault’s copyright lawsuit by showing that Ramkey had a substantial noninfringing use, namely, to enable users to effectuate their rights under copyright law to make backup copies.

It is not clear how *Vault vs. Quaid* would be decided in the

post-DMCA environment. On the one hand, the DMCA seems to outlaw technologies if their primary purpose is to circumvent a technical protection measure that effectively protects a right of a copyright owner. On the other hand, the DMCA recognizes that fair-use-like circumventions should be lawful. Backup copying is a specially privileged activity in the copyright statute. Since a copyright owner doesn’t have a statutory right to control backup copying, perhaps a spoofing technology intended to enable backup copying should be outside the statute. It is important to understand that circumvention for backup copying or other fair-use purposes cannot occur without access to such a technology.

Privacy vs. Security

Intel has recently developed a line of semiconductor chips with a built-in identification system for each processor. Privacy advocates assert that processor identification systems threaten personal privacy on the Internet. In response, Intel announced it intended to ship these chips with the processor identity function “off.” Suppose, however, that Microsoft develops Windows 2000 as a trusted system technology to run on this particular line of Intel chips and that Microsoft requires licensees of Windows 2000 to agree to keep the Intel identification system on at all times. Microsoft might assert that the identifier is a critical component of its trusted system technology. Suppose further that Windows 2000 will not install until the Intel identifier is on, and that the installation software, after a user clicks “I agree” to the condi-

To limit an assessment of the circumvention ban to a certain range of possible effects ignores the wider swath of harm the anticircumvention rules may cause.

tions of the license, will actually activate the identifier. Assume further that a privacy advocacy group develops and distributes software that would “spoof” Windows into thinking the Intel identifier was on when it was not in order to protect user privacy. Would the privacy group have violated Section 1201(b)(1)?

Under a very strict interpretation of 1201(b)(1), development of this spoofing software would seem illegal. It is, however, difficult to believe judges would find this software violates the DMCA antidevice rules. They might observe the DMCA authorizes circumvention in order to protect personal privacy. Therefore, Congress must have intended for people to be able to develop or use technology to accomplish the privileged privacy act. This is clearly not the kind of black box circumvention device that Congress had in mind when adopting DMCA. Microsoft should not be able to employ the anticircumvention provisions of DMCA to force trusted system technology on the public.

Other Harms Caused by the Antidevice Rules

When testifying before Congress, proponents of the administration's antidevice rules repeatedly emphasized that the legislation was needed to stop deliberate and sys-

tematic piracy by black box providers. Yet, the antidevice provisions adopted by Congress are far broader. They provide a basis for challenging a wide range of technologies that arguably have circumvention-enabling uses. This creates a potential for “strike suits” by nervous or opportunistic copyright owners who might challenge the deployment of a new IT tool with capabilities that may include circumvention of some technical protection system. No doubt some expert might say that deployment of a particular technology in the market would meet one of the three conditions in the antidevice provisions, giving plausibility to the suit. Weak as such testimony might be, it may be enough to extract a settlement sum from the IT firm targeted.

The potential for strike suits becomes stronger if one realizes it is not necessary (or arguably even relevant) to litigation under the antidevice provisions of DMCA for any act of underlying infringement (for example, illegal copying of a protected work) to have ever taken place. Consider, for example, a recent lawsuit brought by Sony against Connectix, the maker of emulation software that permits games initially developed for Sony's Playstation to be played on iMac computers. Relying on the DMCA antidevice provision, Sony is seeking up to \$25,000 per

unit sold by Connectix because the emulation software allegedly bypasses an anticopying feature in the games. Sony does not need to allege or prove any actual illegal copying by users of the Connectix software.

Broad Study Needed

The DMCA provides for a two-year moratorium on enforcement of the act-of-circumvention ban during which the Library of Congress is supposed to study whether the ban is likely to impede noninfringing uses of copyrighted works. If the Library determines that noninfringing uses will be adversely affected, it can waive the act-of-circumvention rule as to affected works or users. Similar studies are supposed to be carried out every three years thereafter.

The Library of Congress is supposed to consider: “(i) the availability for use of copyrighted works, (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes, (iii) the impact [of] the prohibition . . . on criticism, comment, news reporting, teaching, scholarship, or research, [and] (iv) the effect of circumvention of technical measures on the market for or value of copyrighted works.” The Library also has authority to consider “such other factors as the Librarian considers appropriate.” Even though the Library can exempt certain classes of users or works from the act-of-circumvention ban, the DMCA is quite clear that the Library's determinations cannot be asserted as a defense to an antidevice claim. Nor does the Library have power to tell copyright owners to stop using technical protection systems

if these systems are impeding non-infringing uses.

While the study provisions in DMCA are surely better than nothing, they fall far short of the periodic review and reporting process needed given the unprecedented nature of the circumvention and the antidevice bans. To limit an assessment of the circumvention ban to a certain range of possible effects ignores the wider swath of harm the anticircumvention rules may cause. To assess the circumvention ban without considering the antidevice rules is to overlook the most significant provision in the DMCA. Unless construed narrowly, the antidevice provisions of the DMCA may do as much harm to competition and innovation in the IT industry as the circumvention ban may do to noninfringing uses.

One would think Congress and the administration would be concerned about deleterious impacts of the anticircumvention regulations on the IT sector given that this is the sector whose tremendous growth the Commerce Department has been trumpeting to the world. The Library of Congress should, therefore, decide that its studies can consider the impact of antidevice rules on the ability of certain classes of users or works to make noninfringing uses of protected works. The Library should also consider other unintended side-effects of the anticircumvention regulations. In order for this to happen, the Library needs to hear from the computing community on these issues.

Conclusion

Anticircumvention regulations were contentious in the U.S. Con-

gress and at the diplomatic conference leading up to adoption of the WIPO Copyright Treaty. The main concerns expressed in both venues were: the harmful effect such rules would likely have on public access to information and on the ability to make noninfringing uses of copyrighted works, and the harmful effect such rules might have on competition and innovation in the market for hardware and software products whose uses include bypassing technical protection systems.

The diplomatic conference had the good sense to adopt only a general norm on circumvention activities, leaving nations free to implement this norm in their own way. The flaws in the DMCA's anticircumvention provisions do not derive from the Treaty, but rather from the bad judgment of the administration and the major copyright industry groups that urged adoption of these overbroad rules.

The DMCA's anticircumvention rules envision an information society very different from the one we currently inhabit. People are used to making a wide range of uses of copyrighted works without seeking the copyright owner's permission. It is unclear how well they will react to a radical shift in the market for information products that the encryption-enraptured futurists are trying to build. NYU Law professor Yochai Benkler observes that “[w]e have no idea how a world in which information goods are perfectly excludable—as technical protection measures promise to make them—will look. Because of the nonrival nature of information, prevailing economic theory would suggest

that we are as likely to lose as to gain productivity from this technological change” [1]. In addition, if consumers won't buy tightly restricted copies, copyright owners may end up worse off than before. Branko Geravac, a professor at MIT, urges copyright owners to “protect revenues, not bits” [2].

If content providers believe that a good business model is the best way to protect intellectual property from market-destructive appropriations, perhaps the current debate over the DMCA's anticircumvention regulations will seem in time like a tempest in a teapot. In the meantime, the impact of this legislation should be closely watched because of the harmful consequences for the computer and software industries and for the public at large. **□**

This column is a derivative work of an article in *Berkeley Technology Law Journal* (Vol. 14).

For 10 years I have written “Legally Speaking” for *Communications*. This has been the most satisfying writing experience I have had, in large part because of such a receptive readership. I am deeply honored to have been named a Fellow of the ACM. While I expect to continue to write on issues of interest and concern to *Communications* readers members, I am taking a leave from the “Legally Speaking” column for a while. Thank you for having made my experience in this community so rewarding.

Pamela Samuelson (pam@sims.berkeley.edu) is a professor of Information Management and of Law at the University of California at Berkeley.

References

1. Benkler, Y. Free as the air to common use: First amendment constraints on the enclosure of the public domain. *New York Univ. Law Rev.* (forthcoming 1999).
2. Geravac, B. Electronic commerce and intellectual property protect revenues, not bits. Forum on technology-based intellectual property management: Electronic commerce for content. Sponsored by the U.S. Copyright Office and the Interactive Multimedia Assoc., Mar. 7, 1996.

© 1999 ACM 0002-0782/99/0900 \$5.00