ELEVEN
COPYRIGHT LAW IN THE DIGITAL MILLENNIUM

In the wake of the enactment of the Digital Millennium Copyright Act, the content industries' chief strategy combined litigation with the threat of further litigation. They searched out, identified, threatened, and if necessary sued intermediaries who arguably facilitated individuals' unauthorized use. They used automated programs that roamed the Internet searching for signs of infringement to find suspicious sites, and the DMCA's expedited subpoena procedures to force service providers to identify alleged pirates. In many cases, a threat was all that was necessary. The Recording Industry Association sent scores of letters to universities demanding that student Web sites be shut down, and they were shut down. The RIAA demanded that Internet service providers terminate subscribers and subscribers were terminated.

The software industry had begun to sell its products online long before the enactment of the DMCA. Advertising-supported works like newspapers and magazines spawned online versions in the early 1990s. The motion picture, music, and book publishing industries, however, had maintained that until the DMCA's protections became law, they would not risk their valuable content on the Internet. After the DMCA's protections became law, they still declined to make their works available for download, concerned that existing technological protections were insufficiently leak-proof. Even after the popularity of MP3.com, Napster, MP3Board, iCraveTV, and Scour demonstrated the tremendous demand for digital music and television, the recording and motion picture industries remained reluctant to license Web distribution of their material. Instead, they pursued relentless campaigns designed to educate, deter, and avenge.

As individual offenders were shut down, others sprang up. The recording industry association's suit against Napster inspired a number of Napster-variants supplying similar functionality without Napster's vulnerabilities. A start-up introduced "Aimster"—a Napster-like add-on to America Online's Instant Messenger program that permitted file sharing within a

small group of "buddies." Programs like Gnutella and Freenet supplied distributed search and file-sharing capability, bypassing a central server entirely, so that there would be no intermediary to sue and no records of who had transferred what files to subpoena.

As a comprehensive strategy, litigation works best against commercial actors. If it takes a lot of money to produce or distribute content, producers and distributors will need money, will have money, will be likely to hire lawyers, and will be vulnerable to weapons aimed at their pocketbooks. MP3.com and Napster have investors to keep happy. Universities have legislatures and donors to soothe. Thus it is completely understandable that the content industry focused its lobbying efforts on pinpointing intermediaries to sue. It eschewed the politically difficult course of seeking an amendment expressly imposing liability on individual consumers for noncommercial copying and private transmission. It sought instead to prevent individual infringement by securing a tough anticircumvention law. That focus turned out to be shortsighted. When producing and distributing content is cheap, commercial intermediaries are optional. The Internet permits individuals to share material with one another on an immense scale and at negligible cost. Stopping each of them is not the sort of task that litigation does best—especially when the basis for their liability is murky.

The strategy of making it impossible for millions of teenagers to engage in unauthorized uses by enacting legal protection for access controls has not worked particularly well either—at least so far. Content owners started pressing for anticircumvention laws as early as 1993. The Lehman Working Group recommended such a law in its Green Paper report in 1994. Multiple access-control technologies appeared under the name of "electronic rights management systems" in 1995, and commercial systems appeared early in 1996. Yet, in the spring of 2000, several generations later in Internet time, record companies had failed to secure their recordings, or to make them available for digital download. Had record companies begun encrypting their recordings in 1993, or even 1996, the vast majority of content traded on Napster would have been unavailable to the ordinary consumer with no hacker skills, because the source recordings would have been technologically protected. Having failed to deploy secure digital music, record companies have relied on courts to revise the bargain to insert a provision imposing liability on consumers for noncommercial copying, private performance, and private distribution. That's a hard sell, especially if the consumers don't go along.

Moreover, the music industry's reluctance to release product over the Internet undermined its campaign to persuade citizens to "say yes to licensing." The RIAA failed in its bid to marginalize MP3 software and keep portable MP3 players from the market. It failed to persuade consumer electronics manufacturers to make their portable digital music players MP3 incompatible. It promised consumers, repeatedly, that the availability of licensed major-label music for their SDMI-compliant portable players was imminent, and then it didn't deliver any. What did it imagine consumers were going to play on their portable MP3 players? If unlicensed major-label music was the only major-label music available, consumers didn't have the option to say yes to licensing.

Nor was the record companies' moral position appealing. The recording industry's insistence that unless musicians were fairly paid, there would be no music rang particularly hollow with fans given the industry's years of demonstrating that when musicians are not fairly paid, they continue to play, write songs, perform at concerts, and cut records. Record companies had collected the lion's share of record revenues for years, arguing that their part of the process of creating and selling records was the expensive part. They controlled the recording studios, record pressing and CD burning plants, and the distribution network, and if studios, pressing plants, and distributors don't get paid, they don't stay in business. The Internet makes much of that infrastructure optional. Yet not one major label proposed reallocating the share of revenue as between the record company and the artist. No major label has been willing to invest in models in which individuals pay artists and authors directly, even one obliging artists and authors to send the record companies their cut. Not one major label has announced that the money it won't spend burning, packaging, and shipping CDs would be shared with consumers in the form of lower prices. Instead, the recording industry suggested that when it did make its catalog available online, the consumer should pay the same $17.99 for an encrypted, downloaded digital file (protected from copying, sharing, lending, or resale) that she pays for an unencrypted, loanable, copyable, resalable CD. No wonder consumers aren't going along.

And they aren't. Napster has more than forty million subscribers despite the record industry's attempts to paint it as a pirate. In the forty-eight hours after the court ordered Napster to shut down, Napster traffic increased markedly. Napster subscribers checked out Gnutella and Freenet. Millions of people apparently decided that they would continue to share

files without regard to the court's ruling. In the following weeks, several small start-ups announced their own file-sharing applications. Either they figured that they had incorporated some features that evaded Napster's legal problems, or they gambled that the legal ruling wouldn't last. If forty million people refuse to obey a law, then what the law says doesn't matter. It may be that people flout it because they're natural lawbreakers, or it may be, as I argue in chapter 8, that they don't comply because it doesn't make sense to them. Whatever the reason, the law is not going to work well in the real world.

Bandwidth constraints have so far limited both the demand for digital, downloadable movies and the unauthorized trading of feature films. Digitized movies comprise very large files; 56k modems are slow. The movie studios are even further from distributing encrypted product via download than their siblings in the recording industry. Although the motion picture industry distributes CSS-encrypted DVDs, it has limited its release of online product to low-resolution, video streaming of movie trailers. The ease with which DeCSS was created and disseminated, however, suggests that, as high-speed Internet connections become more common, the motion picture industry may face similar difficulties. Its litigation strategy, aimed in part at banishing unwanted links from the Internet, suggests that it insists on tighter control of the networked digital environment than the public is likely to allow it to exercise.

Beyond a very small number of well-publicized "e-books,"[1] the print publishers' forays into online publishing of technologically protected words has thus far been limited to a rudimentary and leaky subscription model. Online newspapers, magazines, technical publishers, and information services condition access to text on registration, payment (in money, personal data, or both), and clicking "I accept" to a long recital of restrictive terms of use. Subscribers who click seem to feel little compunction, however, about reposting access-protected texts to their friends, their acquaintances, and the world at large.[2] Again, the publishers' moral position is not especially appealing. At the same time newspaper publishers joined as plaintiffs in a copyright infringement suit to shut down a site encouraging individuals to repost copyrighted news stories,[3] many of them were posting or licensing others to post content online without permission from or payment to the individual copyright owners who had written it.[4] Digital print publishers are only beginning to deploy heavy encryption and disappearing digital ink to prevent authorized readers from saving what

they read and passing it along. It remains to be seen how much control the public will be willing to let publishers exercise over reading.

Access controls and anticircumvention laws may yet enable the content industry to assert its control over audiences' eyes and ears, once it does get its encrypted content online. Or, the industry may need to return to the bargaining table and try to achieve yet another law to plug the perceived leak. There are noises being made in that direction already.[5] Unless the stakeholders do things very differently this time around, though, that law won't work either.

NOTES

1. *See, e.g.*, Stephen King's home page, <http://www.stephenking.com>.

2. *See Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2D (BNA) 1453 (C.D. Cal. 2000).

3. *See* ibid.

4. *See, e.g., Tasini v. New York Times*, 192 F.3d 356 (2d Cir. 1999), *cert. granted*, 121 S.Ct. 425 (2000).

5. *See, e.g.*, Shane Ham and Robert D. Atkinson, *Napster and Online Piracy: The Need to Revisit the Digital Millennium Copyright Act*, Progressive Policy Institute Policy Report (May 2000).