AN MIT ENTERPRISE
TECHNOLOGY REVIEW

Digital Entertainment Post-Napster: Music

By David Kushner November 2002

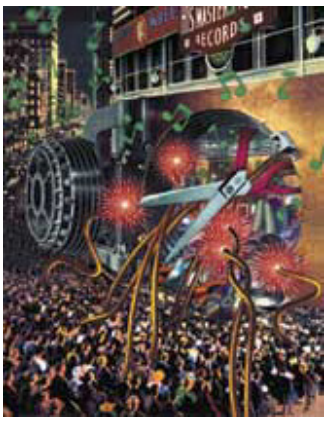

Illustration by John Craig

Antipiracy technology will halt illegally copied music—or so the recording industry hopes.

Samuel Johnson once said that “music is the only sensual pleasure without vice.” Evidently, Mr. Johnson was not a punk rocker. And had there been something like Napster in the 18th century, he surely would have viewed music in a different light.

These days, for the estimated 40 million Americans who trade songs over the Internet, music and vice go hand in hand. After all, much of this music is copyright protected. The recording industry did successfully shut down Napster, mother of all song-swapping sites, for contributing to copyright infringement. But stifling the next generation of file-trading programs such as Kazaa, Morpheus, and LimeWire has proven more difficult. Unlike Napster, these are truly open networks that connect traders directly with each other. For the recording industry, these peer-to-peer networks are a high tech Wild West.

What’s at stake? Plenty, according to a recent report by the Recording Industry Association of America, which represents the major record labels. Last year, shipments of full-length compact discs slipped by about 6 percent—the worst decline in a decade. Nearly one-quarter of the music consumers the association surveyed admitted to illegally downloading music rather than buying new CDs. The study also found that ownership of CD “burners” (disc drives that can record music onto blank CD-ROMs) has tripled since 1999; two out of five music consumers now own the machines. According to the International Federation of the Phonographic Industry, music piracy, including nearly one billion black-market CDs, cost the industry $4.3 billion last year.

Against such odds, the industry is bracing to deliver what could be a lethal counterpunch: new technologies that provide copy protection at the root of the problem, the compact disc. “We’re looking for ways that will maintain the personal copying capability that consumers want,” says Recording Industry Association of America president Cary Sherman, “without taking the risk of unlimited copying.”

Already widespread in Europe and Asia and undergoing trial use in the United States, copy protection will transform the way consumers listen to the music they buy. The same technology could also be applied to videos and computer games. It’s no surprise that the new copy-protection schemes are ruffling the feathers of some consumer advocates. These technologies “are created under the guise of preventing piracy but tend to have the effect of denying the legal right of the consumers,” says Joe Kraus, cofounder of DigitalConsumer.org, which opposes copying restrictions.

In short, copy protection technology aims to put media under lock and key. It remains an open question, though, whether the locks will be strong enough to hold.

Illustration by John Craig

Plugging the Music Hole

The show begins. Britney Spears struts onstage as the music blasts. As if on cue, thousands of teenagers hold up their glowing cell phones, so their distant friends can hear, too. In the 21st century, a live concert is only a telephone call away.

To understand copy protection technology, it's important to understand the nature of what's being protected: the music. Music is inherently free—slippery sound waves that meander through concert halls, living rooms, and dentist offices and into listeners' ears. Selling music, in its purist form, would be like selling air. But engineers know how to restrain the unruly tunes. They carve music into vinyl. They embed it in tape. They seal it between sheets of plastic. And the record companies turn these goods into an industry. So when listeners buy Britney's latest CD, they aren't really buying the music, they're buying a wafer-thin Frisbee. The economy of content is based on physicality.

The Internet has undermined this business model, setting the music free again. Songs are being converted into digital bits, ones and zeroes that go flying over wires, spilling into homes, gushing into dorm rooms. Music fans run to the taps with buckets. And a whole industry is scrambling to stem the flow. The problem is clear. As P.J. McNealy, a senior analyst at Gartner Group, a market research company headquartered in Stamford, CT, puts it: "Music is ultimately not secure because of the way it is delivered." The mission, according to many in the recording industry, is to plug the delivery hole.

One attempted solution has been the use of technologies that allow content providers to track and control electronic media. DVD-Audio discs and digital-music subscription services, are experimenting with a technique known as digital watermarking—interleaving a file with a pattern of bits that verify authenticity without affecting the music itself. But any effort to make watermarking a common practice for protecting music CDs will, for the next several years at least, run into a big problem: many CD players are unable to read watermarks. A watermarked CD inserted into such an oblivious machine means "there's no control or protection," says Joseph Winograd, chief technology officer for Verance, a leading developer of watermarking software.

The recording industry has had similar difficulty deploying its own watermarking standards. This point was brought home painfully in September 2000 when a widely hyped coalition of music and technology companies, the Secure Digital Music Initiative, issued a public challenge to anyone who could defeat its newly minted watermark. Hackers succeeded almost immediately, and the coalition eventually fell apart, leaving an even greater need for a workable copy-protection scheme.

In the absence of a universal watermark-reading standard, the federal government has taken up the cause. Fritz Hollings (D-South Carolina), chairman of the Senate Committee on Commerce, Science, and Transportation, introduced the controversial Consumer Broadband and Digital Television Promotion Act. This legislation would require CD players and other digital-media devices to incorporate a government-sanctioned copy-protection standard if the private sector does not deliver its own standard within one year of the law's enactment.

While a standard remains elusive, technology and recording companies are heading down a more accessible and somewhat militant path. They are developing technology that attempts to nip bootlegging in the bud by clamping down on the most ubiquitous form of music distribution. If the compact discs are copy protected, then the music is no longer free.

How Protection works

For the embattled music business, copyproof CDs are the killer app in the industry's mounting war against digital piracy. The essential idea is to manufacture discs that can be played on stereo audio machines but cannot be copied onto computer hard drives.

A few systems now on the market provide such protection. The Cactus Data Shield, developed by Tel Aviv, Israel-based Midbar Tech, is embedded in more than 30 million CDs worldwide. Try to convert a Cactus-enabled CD into an MP3 file (a process known as "ripping"), you'll get no sound at all. Sony has released 10 million CDs in Europe using its own key2audio copy-protection scheme. Such technologies are finally entering the United States as well. They debuted recently on two albums: the soundtrack *More Fast and Furious*, released by Universal Music Group, was protected by Midbar's Cactus Data Shield. Charley Pride's *A Tribute to Jim Reeves*, from Music City Records, used the MediaCloq encryption software developed by SunnComm in Phoenix.

Each technology works by exploiting the technical differences between traditional stereos and disc players inside computers. Stereo CDs must comply with what is known as the Red Book standard, a set of technological rules defined by Philips and Sony in 1980. The rules concern, in part, how a CD separates its tracks into different sectors on the disc. CD-ROMs, on the other hand, comply with a so-called Yellow Book standard.

Red Book and Yellow Book machines read audio in different ways. Red Book devices correct for slight defects, such as skips and scratches. And herein lies the science of copyproof CDs. When a traditional CD player encounters bad code, it skips over it and keeps playing. When a CD-ROM drive in a PC runs into such data, it loops back repeatedly until it gives up and refuses to play the disc. Midbar's Cactus Data Shield modifies the way the tracks are encoded onto the disc in the Red Book format, rendering the audio invisible to a CD-ROM drive but still playable on a CD audio player.

While Cactus focuses on this high tech vanishing act, a competing technology developed by Macrovision in Santa Clara, CA, takes a different approach. Rather than strictly prohibiting copying, Macrovision's SafeAudio software just makes the results close to worthless. SafeAudio employs several different methods to achieve this effect; one is based, according to product manager Steve Phillippo, "on the introduction of errors into the music." This technique, called coding, embeds audio attributes that, when deciphered by a computer, produce a series of annoying crackles and pops. This degradation of sound quality doesn't stop people from copying a CD, but it sure makes the results unsatisfying. Another SafeAudio technique, called timing, subverts the way in which a CD-ROM player reads audio from a spinning CD; by purposefully misleading the player into reading the data either too quickly or too slowly, it contaminates the music with unpleasant sounds or simply prevents copying.

Finding the Golden Path

And such technologies mark just the first phase of the recording industry's larger copy-protection campaign. Consumers, as industry executives well know, want the flexibility and portability of digital-audio files. They want to listen to the new Beck recording on their living-room stereos, their computers, and their portable MP3 players. The recording companies go along with that, but they want to retain the power to control how those digital files are used. The answer: CDs that include two sets of the same songs, one set (which can be played without restriction) for the stereo, and another set (which is restricted) for the computer.

This year both Macrovision and Midbar will be rolling out products that take this dual approach. In Macrovision's scheme, the stereo tracks will continue to be protected by SafeAudio. The computer tracks, however, will be created using a technology called SafeAuthenticate, which implants an encrypted "digital signature" onto the disc. This identifying code goes further than a watermark. Not only does it verify the authenticity of the recording, it also enables a record company to set limitations on the use of the music. For instance, the code can be set to allow only a certain number of exports to a PC for playback.

Midbar's Cactus Data Shield allows listeners to play YellowBook tracks on a CD-ROM. Later this year the company will introduce a version of the software that allows listeners to copy the music to hard drives as well. But these will be curtailed freedoms; control over its use belongs to the record company, not the consumer. A song might be playable only a certain number of times, for example.

The goal of all this technology, says Eyal Shavit, Midbar's vice president for R&D, is "to find the golden path between compatibility and protection." But that's easier said than done. In 2000 Midbar tested 130,000 dual-approach CDs in Europe only to discover that because of a flaw in the Cactus scheme, 3 percent of listeners could not play the discs on their stereos. That might sound like a small percentage, but it was more than enough to sully the credibility of the emerging copy-protection

wares.

More recently in Europe, some 1,000 consumers who purchased Cactus-encoded copies of Natalie Imbruglia's *White Lilies Islands* CD complained about playability problems. And in Los Angeles, two consumers filed a lawsuit against each of the major record companies (including Bertelsmann Music Group, EMI Music Publishing, Sony Music Entertainment, Universal Music Group, and Warner Music Group) after purchasing what they contend are defective products. The plaintiffs have a point: because copy-protected discs improvise on the Red Book standard, they do not technically fit the definition of a CD.

As the copy protection technologies emerge, the politicians are entering the fray. Their concern is fair use—that is, consumers' legally protected right to make copies of purchased content for their own enjoyment. Earlier this year, Representative Rick Boucher (D-Virginia) wrote a highly critical letter to Recording Industry Association of America chairman and CEO Hilary Rosen, challenging the industry's adoption of copy-protected CDs. Boucher asked what steps were being taken to inform consumers that discs were being altered, whether such technologies would detract from sound quality, and whether the software breaks any laws.

Even if the technologies do not violate fair-use laws, they face another obstacle: hacker ingenuity. CDfreaks.com, a haven for audio geeks, has posted detailed instructions for cracking Macrovision's SafeAudio. And hackers in Germany have revealed a technique that they claim disables Sony's key2audio copy-protection scheme. The very simplicity of their hack shows the magnitude of the task the recording industry faces.

Unlike copyproof systems that embed the copy protection coding right in the music bits, key2audio adds a physically distinct data track to audio CDs. When a CD-ROM reads this track, it assumes the disc is a data CD and gives up looking for music to play.

The German hackers found they could disable that protection simply by covering the data track, which resides near the outer edge of the disc, with ink from a felt-tip marker or even a piece of paper. No sooner did the news spread, than Macrovision, Midbar, and other companies posted bulletins saying that future versions of their products would be impervious to such tricks. But judging from the outcome of similar battles in the past, the hackers have the upper hand: there always seems to be another way to get around a digital fence. It is possible, for instance, to rip songs using an alternative CD-ROM software driver that allows consumers to convert a CD's songs into a file that eludes existing copy-protection schemes.

Analysts, in fact, don't believe that anything is truly immune in this digital age. "No matter how secure the music is on a CD, it can always be hacked," says the Gartner Group's McNealy. "All you have to do is put two microphones in front of your computer speakers." For someone with high-end recording equipment, the results aren't at all shabby.

Truth in Labeling

Despite the backlash against copy protection, momentum for the technology is building. Recording companies are using Europe as a test market for systems that will appear in the United States by the end of this year. And as politicians debate the issues of fair use, U.S. record companies will need to adopt a labeling system to notify consumers that the discs have been altered in a way that makes it impossible to copy their music onto a computer.

Such labeling is crucial not only for the recording industry, but also for the creators of portable players, says Andy Wolfe, chief technical officer of Santa Clara, CA-based SonicBlue, which makes the popular Rio digital-music players. "Consumers want to buy music and be able to listen to it on a variety of devices," he says. "It's not productive for the music industry to put out technology that creates more problems for people. If this doesn't get fixed, consumers might stop buying CDs."

With proper labeling and government approval, however, copy protection will likely be here for the long haul. Companies such as Roxio in Santa Clara, CA, a leading developer of CD-burning software, have already pledged their support. "We're going to work with whoever become leaders in copy protection," says Vito Salvaggio, Roxio's vice president of product management.

Ultimately, by employing copy protection approaches in combination with digital rights management technologies, the recording industry just might suppress the music-bootlegging vice. After all, if Eminem fans can buy a single DVD that contains digital-quality music that they can play on their stereos, their computers, and their portable MP3 devices, they'll be getting all the flexibility they need.

There's also the potential to extend the copy protection strategies developed for music to other digital media; bits, after all, are bits. This extension is especially possible given the migration from the CD to the DVD format. DVDs can hold up to 25 times as much information as CDs; to take advantage of this extra space, video and computer games, music, and video releases will come bundled with more and more additional media. If, for example, a future Tomb Raider game should come with an Angelina Jolie slide show and an Aerosmith theme song, the extra goods would need to be locked up together.

But even if copy protection technology ultimately fails, the recording industry is unlikely to suffer—at least if history is any guide. Emerging technologies have always induced panic among those ensconced in a world of traditional media. The player piano was supposed to kill the need for musicians. The printing press, writers. The television, movies. Jack Valenti, president of the Motion Picture Association of America, presented a notorious example of such panic some 20 years ago when he railed against video recording machines. In a statement to Congress, Valenti said that "the VCR is to the motion picture industry and the American public what the Boston Strangler is to the woman alone."

Valenti was a wee bit off in his gloomy prognostication: home video sales and rentals now bring in nearly twice as much money for the industry as do box-office sales. The fate of digital music—and the technologies being developed to control it—could well prove just as surprising.

Arming the Copy Cops

COMPANY	LOCATION	COPY-PROTECTION ACTIVITY
Macrovision	Santa Clara, CA	SafeAudio distorts music of copied files. SafeAuthenticate puts a digital signature on a CD, restricting its use. Both are being evaluated by record companies.
Midbar Tech	Tel Aviv, Israel	Cactus Data Shield, which "hides" music on a CD to keep computers from copying it, is used on more than 30 million CDs worldwide.
Sony DADC	Salzburg, Austria	Key2audio, which disguises an audio CD as a data disc so that a computer cannot find the music, is already on 10 million CDs in Europe.
SunnComm	Phoenix, AZ	MediaCloq pioneered copy-protection for CDs released in the United States.

Verance	San Diego, CA	Its digital watermarking technology, which interleaves music files with data that verify a disc's authenticity, is in use on CDs in the United States.

David Kushner writes for publications including Rolling Stone, The New York Times, and Entertainment Weekly. Masters of Doom, his book about the creators of the computer games Doom and Quake, will be published in May 2003 by Random House.