Articles

"Weighing the Freedom to Copy Against Freedom From Copying,"

Business section of San Jose Mercury News, p. 58.

by Steve G. Steinberg

For the digerati, the slogan "Information wants to be free" is both a political rallying cry and a fundamental law of nature. That’s a suspicious combination: The history of science is filled with examples of political beliefs determining what is "natural."

It makes me wonder if the ease with which digital information can be copied is the result of how computers are currently designed rather than any natural law. After all, scientists and engineers - the people who brought us the digital era - are inclined to support the free flow of information. Perhaps if computers were designed by lawyers, it would seem that information wants to be expensive.

What started me thinking about this was the recent spate of announcements concerning new techniques for discouraging unauthorized copying. More publishers are offering their wares on the Internet, and they all desperately wish that digital information would behave more like words on paper.

What surprises me are the actual anti-copying schemes. They’re radically different from the software protection techniques you might remember from the 1980’s - more sophisticated, less obtrusive, and consequently more likely to be accepted by consumers and publishers. If these schemes catch on, they will fundamentally change the "natural laws" of information.

In the early days of the digital revolution, most anti-copying schemes focused on prevention. The goal was to make copying software as hard as possible, and a number of techniques were developed that made life difficult for software pirates. Unfortunately, they also made life difficult for honest users. The resulting consumer outcry quickly drove copy-prevention schemes out of the market.

It was a decisive rout, but the designers of anti-copying schemes appear to have learned from it. The new generation of techniques focuses on detection. Instead of trying to prevent copying, they help ferret out unauthorized copies. This way, only dishonest users are affected.

Perhaps the simplest example of copy detection is the scheme developed for electronic documents at AT&T Bell Laboratories. The system makes tiny adjustments to the spacing between words so that each copy of a document is unique. The alterations are too small for the human eye to notice, but they can be detected by computer.

The result is a "digital watermark" that is unique and inextricably intertwined to each copy. True, the watermark doesn’t prevent someone from printing out a confidential memo and faxing it to their friends. But if an unauthorized copy turns up, it can be analyzed and traced back to the source. That makes for a powerful deterrent.

Digimarc, a small start-up in Portland, Ore., recently announced a system that encodes data into an image by subtly altering individual pixels. The system could be used by a photographer to attach her name to digital photos to prove authorship.

The encoded data is invisible to the human eye, and nearly impossible to modify or remove. Even if an image is manipulated with Adobe Photoshop filters or printed out and scanned back in, the data will still be intact.

Digital watermarking schemes are elegant and have a lot of potential uses. But they primarily deter copying with the threat of getting caught rather than with detection.

This shortcoming persuaded researchers at Stanford University to develop a more proactive copy-detection technique. The system is essentially an automated watchdog that can check documents found on Usenet newsgroups or World Wide Web sites against a database of registered documents. If it finds two documents that are very similar, it flags the violation for human examination.

The database doesn’t contain the full text of every document - that would require too much memory. Instead, it calculates a unique fingerprint for each document and uses these for comparisons.

Admittedly, the system is far from infallible. Encryption, for example, would prevent messages from being analyzed. But, just as with digital watermarking schemes, the goal is to deter rather than prevent.

To explain why copy-detection schemes don’t need to be perfect, John Brassil, a scientist at Bell Labs, compares them to padlocks. Everyone knows that padlocks can be easily clipped, yet we still rely on them, partly as totems and partly in the hopes that it will be enough of a bother to persuade thieves to pick an easier target.

With this in mind, current copy-detection schemes are almost certainly good enough to be credible deterrents. But technical feasibility isn’t enough to ensure the acceptance of copy detection.

Will copy detection be seen as only helping to line publishers’ coffers, or will it be credited for improving the quality and quantity of information available online? That’s really just another way of asking the question we started with: Does information want to be free?

While trying to figure out the answer, I asked Digimarc’s Geoffrey Rhodes why the average person would want to use digital watermarks. He replied with a question of his own: "Why do artists sign their paintings?"

That’s exactly right.

Information wants to be free, and it doesn’t. It wants to be freely distributed, but it doesn’t want to be free from attribution. Those who create information want credit, and those who consume information want to know where it comes from. Copy-detection schemes answer both needs.

Steve G. Steinberg is an editor at Wired magazine.

Copyright Sites

BACK TO PRESS RELEASES | NEXT

Products & Technology