SRC Technical Note

2001-002

January 21, 2001

Why Rights Management is Wrong
(and What to Do Instead)

Mark S. Manasse

Systems Research Center
130 Lytton Avenue
Palo Alto, CA 94301
http://www.research.compaq.com/SRC/

Abstract

Digital rights management based on enforcement is moribund. The bits are free and they can't be put back in the bottle. Yet, content creators want to get paid and users want superior quality content. Assuming that users are willing to pay for content they like, we propose a scheme for digital rights licensing modeled after shareware licensing.

Introduction

Digital content has irrevocably changed the relationships between the content creators, the copyright-owners, and the purchasers of the content. The creators and users care about the content and don't care about the bits. The copyright-owners own the rights to the bits, but the bits are loose and they aren't coming back.

To paraphrase Scott McNealy of Sun, "You have zero control over your bits anyway. Get over it."

But all need not be lost. Readers, viewers, and listeners are fans, not thieves. They understand that their payments are necessary to reward and encourage the creation of desirable content. As has been seen in many forms and many instances, users are willing to pay a reasonable price for desirable content. Even when the content may be available at lower cost, users are willing to pay for convenience, timeliness, packaging, reliability, and quality assurance. Many consumers gladly buy a video rather than wait to tape the same movie off of cable tv, buy a book rather than borrow it from the library, or buy a newspaper rather than hope to find a discarded copy on the train.

Unquestionably, digital content changes the relationship between the copyright-owner and the purchaser of content. Without physical embodiment, the uniqueness of a piece of content cannot be maintained or enforced-the bits can be copied. Rights-management systems attempt to make a faithful digital copy harder to produce, or harder to use, but with limited success. Instead, personalized licenses to content can be unique, and can serve as a practical method for establishing a user's rights to digital goods.

The Terrain

Napster, Gnutella, MojoNation, Freenet, Scour (Scour Exchange is now defunct), and their ilk show us a world in which static content can no longer be secured against digital reproduction. The Digital Millennium Copyright Act may have declared reverse-engineering to be unlawful, but copies of deCSS are widely available-recent court decisions notwithstanding-and T-shirts and songs are available which capture the code for posterity. Decentralized sharing and open source removes large targets for legal remedies, so Gnutella. MojoNation, and Freenet should prove harder to eradicate than Scour was and Napster may be. MP3 audio and MPEG compression of video (as well as other compression technologies either independent of MPEG or layered as codecs for MPEG, such as DivX ;-)), together with advancing storage and networking capabilities, remove the necessity to package content on physical media-even the contents of DVDs are being traded online today. The desire to have your books, magazines, music, and video available in every room, and in the car, and on the device you buy next year to replace the one you bought last year places additional constraints on attempts to solve this problem through technology or cryptography. The expectations of an audience conditioned to collect (by the first-sale doctrine governing further disposition of the embodiment of intellectual property) must be reconciled with a world in which there is no tangible embodiment of the content.

What are we left with? Must we agree that information actively wants to be free; that there can be no value in the creation and distribution of static content? I would argue not. In particular, users of content have an interest in supporting the creators of content. Without economic justification, the quantity and diversity of available content would be greatly reduced. Readers and listeners are fans, not thieves, and should want to financially encourage the creation of desirable content.

Many proposals have been made for equitably addressing the needs of content providers to be paid. The sponsorship models (see Kelsey and Schneier's Street Performer proposal, for example, or OpenCulture) may work for established artists whose work commands adequate compensation sight unseen. Subscription models provide the economic efficiencies of extracting revenue from users with different preferences, with the drawback that dividing the revenue equitably has historically been a difficult problem. Purely voluntary payment, such as Tipster, provides no durable record to the purchaser, which works for payment for ephemeral content, but may be inappropriate for archival material. While all of these may provide parts of the solution in the future, I believe that cash-and-carry sale of individual items will remain integral to the exchange of content. Further, devising a system in which existing players in content production and distribution each have roles to play analogous to their current roles may ease the transition to a digital goods economy.

Other proposals follow more restrictive paths: that of enforced rights management. Enforcement through hardware is feasible, but restricts content to devices with appropriate hardware modifications. This works against the trend to using general-purpose computing hardware for content viewing. Moreover, the existence of unrestricted players for personal computers, and the need for content to be presented in a human-sensible format means that no content can be made technologically infeasible to pirate. A single sample of a presented piece of content may suffer from reduced quality, but averaging multiple presentations can extract the original digital information to whatever degree of precision is presented. A faithful digital copy can be rendered impossible if players never present all the bits, or reproduce the content with imperfections, but if the differences are imperceptible, then the transcoded copy hasn't lost anything useful. If the differences can be perceived, the user isn't getting much advantage of a faithful digital copy to begin with. Such considerations make copy prevention possible only in a world where all performance and recording devices are produced according to the plans of the content industry, an impractical restriction. Copying can be made difficult by making devices capable of copying more expensive (as was tried in the distinction between consumer-grade digital audio tape (DAT) recorders and professional-grade ones), or by requiring additional equipment (image stabilizers to strip Macrovision encoding from videotapes); future efforts are likely to be outstripped by technology (in the software industry, an early Infocom game was protected by having a large table of data necessary at an early stage of the game printed on paper with a blue background, defeating photocopiers of the time, but of no value against scanners or color copiers) or, as in the case of DAT, viewed as restrictive enough to prevent the adoption of DAT as a consumer technology. Further, in the case of CD or DVD based content, outright piracy can't be the issue: recreating a master from a copy, and then stamping out thousands of discs doesn't require much skill beyond the ability to mass-produce discs.

Rights management systems and watermarking don't try to prevent large-scale piracy; they work to discourage small-scale sharing of goods. In defense of such sharing, it's considered by most to be a perfectly acceptable use of a book or CD to loan it to a friend, or to leave today's newspaper on a bus for others to peruse. Rights management systems which fail to respect the rights which users consider themselves to possess will slow copying primarily by reducing all distribution. A digital encyclopedia which disables cut-and-paste will not flourish, unless its audience discovers screen capture and OCR tools. A market for digital collectibles can exist only to the extent that the collected items can meaningfully be bought and sold in secondary markets; rights management systems which fail to account for resale foreclose a market for digital Pokemon cards or comic books.

The software industry has faced the problems of copied and pirated material for years, and has evolved models which work in exactly this environment: that of shareware, and of licensed use of software. When Microsoft distributes a copy of Office 2000 on a CD, they don't insist on verifying possession of that CD every time the software is used. Instead, they provide a license number for the use of the software. Subsequent transfers of the software to future computers owned by the same party are of no particular concern to Microsoft, nor is the resale of the software: only one person can hold title to the license at a time. The existence of a physical document representing the license makes this a little easier to enforce, but doesn't encumber the shareware distributors at all: they're happy to allow people to register software by providing an identity, which can be tracked across time. I don't know of shareware services providing for transfer of registration, to allow resale or inheritance of their wares, but one can imagine it; for content such as books or music, satisfying the needs of the collector requires that transfers can exist. Existing markets in first editions can be retained by producing limited edition licenses, with digital signatures and notarization proving authenticity.

Licenses

How, then, can producers of music and films profit from the digital release of their goods? I argue that selling licenses to their customers, and compensating the agents serving as a distribution channel, is a good fit to both existing business models, and to what's achievable on the internet.

A license should give the user the right to use a piece of content on any playback device of their choice. Playback devices have very limited lifetimes; technological progress guarantees that. Having bought the right to listen to a song on my current personal computer, I shouldn't need to repurchase the right to listen to it on my next computer or portable MP3 player. We're trying, as best we can, to emulate what I could do with a physical format for the content. I currently have the right to listen to a piece of content on any CD player I have access to, or to read it using any source of adequate light.

A license should be a digital good. If I could only use a piece of content while in possession of a physical token specific to the content, then sales must always involve moving atoms. If we instead hypothesize a token associated with a user. then the rights to a single piece of content can be transferred only with the active cooperation of the owner-I can't sell you a single book, only my entire library. Further, user tokens might restrict simultaneous performance of licensed content in unintended ways: shouldn't I be able to watch *The Hidden Fortress* and *Star Wars* simultaneously on two screens, or listen to *Dark Side of the Moon* while watching *The Wizard of Oz?*

Mechanical enforcement of licenses should be lax to non-existent. Strictly enforced licenses would either be so permissive as to be useless, or they would make it difficult to loan an album to a friend, or to bring a video to a party. There are too many players for unencumbered content for enforcement to work as a mandatory check-transcoding into unencumbered formats will persist as long as copy-protection schemes do. Mechanical enforcement has other drawbacks for archival purposes: copyrights *do* eventually expire, which automatic enforcement may not recognize. Further, companies go out of business, so it may not be possible or appropriate to transfer a license if that requires the active cooperation of the owner. Restrictive enforcement of rights will only make sense once we recognize that users of content have rights, too. It is appropriate and desirable for players of content to check for the presence of a license, so that the user can be encouraged to acquire a license; it is inappropriate for players to refuse to play content because the player is unable to verify the validity of the license.

Legal enforcement of licenses is good, however. Distribution of a piece of content with the license detached should be aggressively prosecuted. Distribution of content without a license to do so should be frowned upon, as well. But a license to distribute should be part of nearly every license purchased by a user; this legitimizes Napster. In addition, complementary licenses, without transfer rights, may be granted by content owners to legitimate distributors.

It would be better, I submit, for licenses to afford the user the right to a piece of content in whatever compression format the content finds itself in. If tomorrow a superior compression technology to MP3 becomes available, one, say, which provides identical fidelity in half the space, people will recompress their music collection. Making this illicit is bad for credibility, at least. However, owning a license to this year's release of *The Phantom Menace* shouldn't provide me the rights to next year's enhanced release with the director's commentary. The license is to a specific piece of content, but not a specific representation of that content.

We'll come back to consider how to construct licenses satisfying all of these requirements, after a short detour into emerging distribution channels.

Peer-to-peer sharing and distribution

Is peer-to-peer sharing inevitable? This is more difficult to answer with certainty, because it depends quite strongly on the particulars of the economic milieu. If licensing were easy, and distribution was rewarded, would peer-to-peer servers be the primary distribution channel?

Peer-to-peer sharing makes good use of some existing economies. Users possess computing power, storage, and bandwidth in excess of their average requirements, and already supply a place for their computer to sit. All of these resources are viewed by a user as free, or at least as the cost of playing the game; an ISP stepping into the role of an edge-distributor of content would see the incremental need for processors and disk and floor space as a cost. The sole advantage to the ISP is bandwidth: the bandwidth requirements are reduced by serving the content from inside, and the bandwidth is available in a single large chunk. MojoNation already addresses this last issue, by splitting files into multiple smaller pieces which can be simultaneously downloaded, taking advantage of the asymmetric nature of DSL and cable connections. If housing the content at an ISP can be done more cost-effectively than making the upload bandwidth from subscribers sufficient to the task, then ISPs will become the distribution centers for content. If suppliers were compensated for providing bits, the economics would shift some; if ISPs chose to bill for 'excessive' uploading, that would change the market conditions around file-sharing.

Nonetheless, if economic incentive can be provided to content owners to make their goods widely available, edge-based distribution of content will dominate while bandwidth remains a significant expense. Whether that content will live exclusively in individual machines or in data centers just depends on the expected revenue and expense for storing it centrally, and the difficulty of locating content. It is likely that some content will not justify being stored at the edges in ISPs: what is held will be a simple matter of engineering and economics. Just as video stores today sell off videos whose expected future rental revenue doesn't pay for the cost of shelf space (and don't even buy videos whose expected return is less than the cost of purchasing the movie), we can expect ISPs to have enough space so that they store those pieces of content which will be profitable. Since individual tastes may support more esoteric content, we can expect peer-to-peer distribution to remain useful. Moreover, to the extent that good collections of content serve to advertise items, peer-to-peer sharing may encourage distribution and sales of content previously unknown to the user. If I stumble on a Napster user with a few uncommon items of interest to me, browsing his or her collection for further suggestions of things in the same category may be helpful.

License details

In order to facilitate mechanical assistance in keeping track of licenses, the license terms should be expressed in an easily-parsed format, for example RDF. The terms should spell out a lifetime for the license, expressed as an expiry date and time. The terms should name the owner, with enough specificity to uniquely identify the content holder. To allow privacy, a nym ought to be acceptable, if the owner can demonstrate ownership of that nym. Details of what constitutes acceptable use should be described, probably in natural language for now. Content redistributors should provide a short list of nyms they distribute content under.

For compactness, and to spare people from having to individually absorb the use conditions, these details may be incorporated by reference to a persistent URL. Such URLs should contain datestamps in their name, and the content of such a URL should be notarized for that date and name.

The license should also contain publication information: a name for the edition of the work, the number of licenses authorized in that edition, the serial number of this license in that edition.

The license should then be digitally signed using a public key, and digitally notarized. The notarization establishes the validity of the license as of the date of notarization, even if the public keys become compromised; using two disparate hash functions, the notarizations can be redone when one of the hashes is no longer considered secure, providing an auditable trail of validity.

The license should include a hash value as part of the signed body; the pre-image of the value should not be disclosed when sharing the contents, but is required to demonstrate valid possession.

The license should include a URL for purchasing another license to the content: the submission requires a previous license to be submitted, so that distribution can be tracked. Content holders should set a nominal distribution percentage to be credited to an account established for the distributor.

To ward against arbitrage of distribution fees, requests for content might return a MAC of the license and content using a customer-supplied key. If valid supplier of content refuse to stream out the last bytes of content until at least a minute has passed from the request, ordinary users will time out the MAC request before an arbitrager possessing a valid license can retrieve the bytes from a third party.

Players should display the license status of content, and make it simple to acquire a license, assert that no license is required because the content was ripped from a copy already owned by the user, or because licenses could no longer be obtained, to assert that the player should perform the content without a license, or to remove the content.

Any transfer of license requires renotarization; a hash of the license being abandoned is entered into a public registry of abandoned licenses. Transfers should ordinarily be notarized by the original notary, or their successor; otherwise, license transfers should be provisional, with a delay between abandoning he original license, and issuing the transferred license with a long enough delay to allow for updates of the copies of the public registry.

Temporary licenses, such as might be used when lending content from a library, can be issued with a local notarization log, with periodic notarization of the notarization log to safeguard against issuing duplicate leases on content.

Subversion

If I ran RIAA a year ago, what would I have done? To me, it's obvious: peer-to-peer sharing of content should be the best marketing tool the labels have ever had. By releasing degraded copies of a wealth of content, the music industry could take advantage of other people's bandwidth to distribute music which competes primarily with radio as a mechanism for introducing listeners to their goods. Distributing content with restricted bandwidth, or with appended advertising from enough servers to swamp the bulk of Napster users, and with enough bandwidth and enough different servers to be a preferred source for content would effectively transform Napster into an ideal advertising channel.

Along these lines, some individuals with interests in preserving the existing copyright regime have taken it upon themselves to release damaged content files on Napster and Gnutella with file lengths matching the most popular version's length. This detracts from the utility of peer-to-peer sharing, and provides the motivation for providing one-way hash checksums of content when purchasing a license.

Conclusions

In my opinion, content protection and rights management exist only as vestigial efforts to preserve existing models of content sales for as long as the bulk of the consumer market remains clueless. History has shown every content-protection scheme invented for consumer-grade goods to have almost no impact on piracy, and little impact on casual copying, except when it has doomed the technology carrying it. This is inevitable.

The question before us is not about how to protect the bits, but how to protect the investments in creation of the bits, and how best to preserve the relationships between people and content. I submit that establishing a market for licenses to digital content is the last best hope for providing a continuing revenue stream for static content.

Acknowledgements

My thanks to Steve Glassman and Mark Lillibridge of SRC for having helped shape my ideas and the presentation of them.