Digital Rights Management: Ethical Analysis of an Engineering Controversy

By
Blake L. White

Developed and presented in conjunction with the graduate seminar -- ***Ethics, Science, and Technology*** – under the direction of Professor Robert McGinn, at Stanford University, June 5, 2003.

The Digital Rights Management Controversy

The Internet offers music, video, and book lovers virtually limitless possibilities. Digital technology brings media to a wider public, affords niche artists access to their audiences, makes our vast entertainment heritage widely available, and distributes old, new and unusual media at affordable prices. Unfortunately, the Internet also gives content pirates a new weapon.

Within the Internet culture of unlicensed use, theft of intellectual property is rampant. The music business and its artists are the most prominent victims, and ultimately consumers suffer also. Unauthorized Internet music archive sites (using multiple formats, such as .wav files, or MP3 files) provide illegal sound recordings online to anyone with a personal computer. Music can be downloaded and played indefinitely, without authorization of or compensation to the artists. Other music pirates use the Internet to peddle illegal CDs.

According to the Recording Industry Association of America (RIAA), "Because of the nature of the theft, the damage is difficult to calculate but not hard to envision. Millions of dollars are at stake. Many individuals see nothing wrong with downloading an occasional song or even an entire CD off the Internet, despite the fact it is illegal under recently enacted federal legislation. "

As the preamble to the recently held UC Berkeley Center for Law and Technology's conference on Digital Rights Management introduced the subject,

> "Music is being released on copy-protected CDs, movies on encrypted and region-encoded DVDs, and Congress is considering the mandate of technological protection for digital television. The next generation of information distribution will be defined by the purchase of rights to receive digital content for a set of defined and controlled uses. Digital Rights Management (DRM) systems are the technological measures built into the hardware or software of home computers, digital televisions, stereo equipment, and portable devices in order to manage the relationships between users and protected expression."

As technological solutions increasingly interact and even supersede the laws of intellectual property, privacy, and contract law, it is imperative for everyone from lawyers, technologists, and policy-makers to artists and consumers to re-evaluate society's notions of purchase rights, copyright protection's scope, and fair use in the context of the new realities of modern technically-enabled society.

If an ethical software engineer is working on the controversial DRM technology in the superheated battle of rhetoric and lawsuits between the entertainment industry, commercial pirates, and nuisance non-commercial pirates in college dorm rooms, what is one to do? The competing interests that need to be satisfied include: (a) content owners, who have the right to withhold their content until payment is received, and who are the customers and source of revenue for the software engineer's company, (b) shareholders, who expect maximization of profits, (c) Fair Use claimants, who have the federal law on their side, and (e) the public consumer, who applies a property rights model based on physical, hard-to-copy, hard-to-distribute media of a bygone era to the highly fluid digital media of today.

Stakeholders' Interests -- Arguments for DRM:

The RIAA is a trade association whose members create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States. The Anti-Piracy division of the RIAA investigates the illegal production and distribution of sound recordings. RIAA's position is that,

> "Many do not understand the significant negative impact of piracy on the music industry. Though it would appear that record companies are still making their money and that artists are still getting rich, these impressions are mere fallacies. Each sale by a pirate represents a lost legitimate sale, thereby depriving not only the record company of profits, but also the artist, producer, songwriter, publisher, retailer, … and the list goes on. The consumer is the ultimate victim, as pirated product is generally poorly manufactured and does not include the superior sound quality, artwork, and insert information included in legitimate product. Consumers also lose because the shortcut savings enjoyed by pirates drive up the costs of legitimate product for everyone. Plus, good luck returning a pirated tape or CD when the quality is inferior or the product is defective, as it often is. Honest retailers (who back up the products they sell) lose because they can't compete with the prices offered by illegal vendors. Less business means fewer jobs, jobs often filled by young adults." (RIAA Website: Position on Piracy)

RIAA believes that the principle that the work that one has created belongs to the creator and should be controlled by the creator is as timeless as it is global. Around the world, this principle is encoded in law. The industry's goal is to make the Internet a legitimate marketplace for sound recordings, and that can't happen unless artist and record company rights are respected.

The renowned film director George Lucas puts it this way, "There is no free lunch. No matter how free its seems someone is paying for it. In the end, when someone gets ripped off or someone is getting something for free, someone else is getting screwed" (Speech at 2003 COMDEX). The prevailing view among content owners, creators, and studio executives is that:

- Digital content (e.g., music, movies) won't really be secure until DRMs are in all digital media systems (including general purpose computers)
- The computer/software industry has resisted "voluntary" standards on DRMs
- Standards are essential to ensure interoperability among various vendors DRMs
- Broadband deployment has arguably been hindered by threat of "piracy," so stronger legal protection is necessary.

Our goal is … "protecting content against theft and illegal redistribution, while protecting the thrilling advances and digital abilities to which we are accustomed," notes Peter Chernin, President & COO, News Corporation Chairman and CEO of the Fox Group (Keynote speech at 2003 COMDEX).

DRM provides a comfort level to studio executives and enables powerful new business models that allow content owners and product developers to offer greater choice and pricing options to their customer base. The alternative, according to Lucas, is that "…only safe movies will get made, movies with mass appeal that distributors feel are likely to make money. Smaller, art, experimental, or even films like Star Wars would simply not get made, let alone distributed" (Speech at 2003 COMDEX).

Stakeholders' Interests -- Arguments Against DRM:

Property Rights

Referring to DRM's ability to limit copies to a specific number (including zero) and limit the devices on which a CD or DVD may be played, Julie Cohen of the Georgetown University Law Center observes that, "DRM systems impose restrictions on what individuals can do in the privacy of their homes with copies of works they've paid for." (Cohen 47) She continues, "Direct functionality restrictions intrude on the seclusion, or 'private space,' that long-established social practice reserves to the individual or family, while forcing changes in a set of behaviors within that space." (Cohen 48)

SRI cryptographer Drew Dean asks thorny questions for lawyers, such as:
- What does it mean to "own" something that I'm not allowed to understand how it works?
- Am I responsible for what my computer does without my knowledge?

Free Speech

Corley, a Norwegian teenager who also edits a hacker's magazine, wrote a program, DeCSS, to bypass CSS, the protection technology, and posted it on the Internet. He claimed a First Amendment right to post or link because DeCSS was a controversial issue of public importance. Corley also claimed that DeCSS is speech that he has a right to utter under the First Amendment. Corley claimed the Digital Millennium Copyright Act (DMCA) was unconstitutional because it was not narrowly tailored to achieve a substantial government purpose.

Fair Use

Critics argue that, because DRMs enforce a strict set of rules, those rules overreach the established doctrine of Fair Use, which allows copying for academic, research, criticism, backup, archival, and non-commercial sampling purposes. For example, the U.S Copyright Act of 1976 (17 USC) lists four nonexclusive factors courts must balance in determining whether a particular use is fair. They are:

- The purpose and character of the use
- The nature of the copyrighted work
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole, and
- The effect of the use on the potential market for or value of the copyrighted work.

Chilling Effect on Cryptographic Research

Boston College Law School Professor Joseph Liu argues that the DMCA will have a non-trivial impact on the conditions under which such research takes place by:

- Limiting who can conduct research
- Imposing additional hurdles before research
- Limit free communication about research
- Limit avenues for publication
- Require notice and disclosure of results
- Affect content of published work

Abuse of Privacy

According to the ACM, "Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups" (ACM Code of Ethics). Cohen argues that DRM systems are capable of reporting back to the copyright owners the activities of individual users. Such reporting may occur as part of a pay-per-use arrangement for access to the work or independent payment terms. It could also be designed to report attempts to make unauthorized copies or determine which software programs a user is running. "In Western culture, information about intellectual activity has long been regarded as fundamentally private, both for reasons related to individual dignity and because of the powerful chilling effect that disclosure of intellectual preferences would produce," notes Cohen (Cohen 47-48).

Open Public Debate

Princeton's Ed Felton argues, "Important public policy questions depend on understanding technology. [This is] especially true right now for DRM. Bans on understanding technology cripple the public debate about these issues" (Felton).

Other IT industry arguments common among DRM opponents include:

- It would prevent many beneficial uses of IT
- It would add expense to IT systems
- It would undermine system performance
- Would retard innovation & investment in IT
- It may make systems more vulnerable to hacking (DRM = "break once, break everywhere" system)
- The government & content industry shouldn't dictate how the IT industry builds its products.

As a result, UC Berkeley law professor Pamela Samuelson has asked the fundamental question in a paper by the same name, *DRM {AND/OR/VS.} LAW*. Is DRM a copyright enforcement mechanism? Is DRM as an alternative mechanism to copyright law whereby industry standard-setting processes act as alternatives to law? Is DRM a means to override the law, for example, as a way for content owners to override Fair Use, First Sale, and Public Domain principles? She also argues that the law can be a means to control DRM, e.g., require privacy protection and build in Fair Use capabilities (Samuelson 41-45).

The Facts

Piracy is a Problem for the Content Industry[1]

Intellectual property piracy accounted for 20 million pirated optical discs seized and 4.5 million pirated videos seized in 2000 (MPAA). Illegal copies are also made from legitimate advance screening and marketing copies, from illicit duplicating facilities, camcording in movie theatres, and though rare, theatrical print theft from couriers or facilities. Pirates steal from cable and satellite signals with circumvention devices, such as DeCSS, Macrovision defeaters, and black boxes. The most notable press goes to Napster (defunct), Kazaa, Limewire, Gnutella, and Morpheous, which enable free downloads of media from Internet FTP sites or via file swapping utilities.

In a brazen press release, Sharman Networks " …celebrated its 200 millionth download of Kazaa Media Desktop (KMD) on Tuesday 11th March. This further secures its position as the number one peer-to-peer software application in the world. The most downloaded, the largest number of users and the fastest growth. The first big leap for Kazaa Media Desktop was its 100 millionth download in August 2002. Now, 7 months later over 200 million copies of KMD have been grabbed from Download.com. And we're not

[1] The pirate's credo is still the same--why pay for it when it's so easy to steal? The credo is as wrong as it ever was. Stealing is still illegal, unethical, and all too frequent in today's digital age. According to the RIAA, "Piracy" generally refers to the illegal duplication and distribution of sound recordings. There are four specific categories of music piracy:

- Pirate recordings are the unauthorized duplication of only the sound of legitimate recordings, as opposed to all the packaging, i.e. the original art, label, title, sequencing, combination of titles etc. This includes mixed tapes and compilation CDs featuring one or more artists.
-
- Counterfeit recordings are unauthorized recordings of the prerecorded sound as well as the unauthorized duplication of original artwork, label, trademark and packaging.
- Bootleg recordings (or underground recordings) are the unauthorized recordings of live concerts, or musical broadcasts on radio or television.
-
- Online piracy is the unauthorized uploading of a copyrighted sound recording and making it available to the public, or downloading a sound recording from an Internet site, even if the recording isn't resold. Online piracy may now also include certain uses of "streaming" technologies from the Internet.
-

stopping here. We are currently working on some new features which will take us towards the next 100 million."

However, a federal court recently ruled that similar peer-to-peer file-sharing software programs Grokster and Morpheus do not infringe upon copyrights, instead placing the criminal burden on individual users of the software.

The impact on entertainment industry revenues is significant. The MPAA estimates $3 billion in annual revenues were lost by the US motion picture industry. Piracy upsets carefully planned release schedules. For example, *Star Wars: Episode 1 – The Phantom Menace* had much lower Asian attendance because of earlier US piracy. RIAA estimates the music industry loses about $4.2 billion to piracy worldwide and $300 million a year domestically. The music industry loses more than $1 billion per year from the illegal activities conducted in the world's four leading pirate marketplaces — Brazil, China, Russia and Mexico.

According to Universal Music Group's VP Asset Management, Jonathan Bender, at the 2003 Digital Content Delivery Conference, even though UMG held a 28% share of worldwide music distribution in 2002 (30% share of new releases), it experienced a decline of 20% in CD units over the past three years, due to in part to free downloads and burns. But, he also acknowledged that other factors, such as competition for disposable income of young consumers, ageing demographics, and new, incompatible audio formats also contributed to the problem.

The music industry is fighting back with seizures, raids, arrests and convictions. According to RIAA:

- More than 230 distribution operations were raided in 2001, compared to approximately 100 in 2000.
- More than 145 manufacturing operations were raided in 2001, compared to approximately 50 in 2000.
- 2.8 million unauthorized CD-Rs were seized, compared to 1.6 million in 2000.
- 21 million labels were seized, compared to 3.5 million last year.
- Search warrants were up 74 percent
- Arrests and indictments were up 113 percent
- Sight seizures were up 170 percent
- Guilty pleas/convictions were up 203 percent

Poor or Outdated Business Models are at the Root of the Piracy Problem

The recording industry can be legitimately criticized for enforcing a bundling strategy, where even if the consumer wants one or two songs, they have been forced to buy a full CD at high prices. Thirty years ago, the record industry (a) gave a small of amount of material away for free on the radio, (b) did not care if copies were made for personal use compilations or passed on to friends, (c) sold singles for under $1, (d) provided a better deal with albums for fans of artists than buying a dozen singles, (e) made money on the live concert, (f) made money on the T-shirts sold at concerts, and (g) captured the loyalty of consumers with fan clubs. Somewhere, the lure of the $14 CD caused the industry to move away from singles and a model that worked for them for decades. Arguably, what we are seeing today is a consumer demand for a return to a singles-based sales model.

However, according to RIAA, the vast majority of CDs are never profitable. After production, recording, promotion and distribution costs, most never sell enough to recover these costs, let alone make a profit. In the end, less than 10% are profitable, and in effect, it is these recordings that finance all the rest. Eighty-five percent of recordings released don't even generate enough revenue to cover their costs. Record companies depend heavily on the profitable fifteen percent of recordings to subsidize the less profitable types of music, to cover the costs of developing new artists, and to keep their businesses operational. The thieves often don't focus on the 85%; they go straight to the top and steal the gold. (Source: RIAA)

Finally, and perhaps most importantly, the creative artists lose. Musicians, singers, songwriters and producers don't get the royalties and fees they've earned. Virtually all artists (95%) depend on these fees to make a living. The artists also depend on their reputations, which are damaged by the inferior quality of pirated copies sold to the public. (Source: RIAA)

US Copyright Law is the Basis for Content Owner's Rights

"Copyright" is a term of intellectual property law that prohibits the unauthorized duplication, adaptation or distribution of a creative work. In the recording industry, there are usually two copyrighted works involved: 1) The copyright in the musical composition, i.e. the actual lyrics and notes on paper. This is usually owned by the songwriter or music publisher. 2) The copyright in the sound recording, i.e. the recording of the performer singing or playing a given song. This is usually owned by the record company. (Source: RIAA)

Under US Copyright Law, authors of original works of authorship generally have five exclusive rights:

– Reproduce work in copies
– Make derivative works
– Distribute copies to the public
– Public performance and public display

Congress passed the Digital Millennium Copyright Act (DMCA) in 1998, which created two new intellectual property rights:

– Anti-circumvention rules (sec. 1201)
– Protection for copyright management information (sec. 1202)

The rules are complex and somewhat ambiguous.

In addition, The No Electronic Theft law (the "NET" Act) is significant because now sound recording infringements (including by digital means) can be criminally prosecuted even where no monetary profit or commercial gain is derived from the infringing activity. Punishment in such instances includes up to three years in prison and/or $250,000 in fines. The NET Act also extends the criminal statute of limitations for copyright infringement from three to five years. Additionally, the NET Act amended the definition of "commercial advantage or private financial gain" to include the receipt (or expectation of receipt) of anything of value, including receipt of other copyrighted works (as in MP3 trading). Punishment in such instances includes up to five years in prison and/or $250,000 in fines. Individuals may also be civilly liable, regardless of whether the activity is for profit, for actual damages or lost profits, or for statutory damages up to $150,000 per work infringed.

According to Samuelson, the DMCA 1201(a)(1)(A) makes it illegal to circumvent effective technical measures used by copyright owners to protect access to their works. However, there are no corresponding provisions making it illegal to circumvent other technical measures, such as copy controls. Was this intended to leave room for circumvention of copy controls as long as it didn't result in copyright infringement?

Other DMCA rules include:

- 1201(k), which mandates Macrovision DRM in VCRs
- 1202 protects the integrity of "copyright management information" from alteration/removal
- 1203 provides broad remedies to successful plaintiffs (injunctions, statutory damages, etc.)
- 1204 makes willful violation of 1201 or 1202 for profit/financial gain a crime with penalties of up to $500K fine and up to 5 yrs in jail for the first offence, and up to $1 million and up to 10 years in jail for the second the offence.

In most respects, the EU's Copyright Directives is more restrictive than DMCA, in that it:

- Bans all acts of circumvention, not just of access controls
- Broad ban on circumvention technologies very similar to DMCA (but reaches possession as well)
- No exceptions, not even for encryption research
- No Library of Congress (LOC) rule-making processes
- But it requires member states to ensure that copyright owners enable users to exercise some copyright exceptions, although it does not say how.

While there is no such thing as an international copyright law, many treaties have been signed that establish a mutual respect for countries' copyright laws.

US Copyright Law is also the Basis for Consumer Claims of Ownership Rights

However, there are a series of limitations and exceptions to those exclusive rights, including Fair Use. (Samuelson, DRM Presentation, UC Berkeley, Feb. 27, 2003) The exceptions to DMCA 1201(a)(1)(A) include:

- Non-profit "shopping" privilege
- Legitimate law enforcement/national security
- When necessary for program interoperability
- "Legitimate" encryption research
- To protect minors vs. harmful material
- To protect against collection of personal data (surveillance without notice)
- Computer security testing

Samuelson also notes that under DMCA 1201(c) certain rights are unaffected. They include:

- No effect on rights, limits or defences, including fair use, under this title
- No effect on contributory or vicarious liability
- No requirement to respond to technical measures in computer/consumer products
- No effect on free speech/press rights

Does Fair Use apply to DMCA rules? Authorities disagree:

- 1201 is not copyright, so no fair use (Corley decisions; Nimmer; but Boucher/Lofgren seek change)
- 1201(c)(1) preserves it (Ginsburg, Samuelson)
- DMCA anti-circumvention rules are unconstitutional unless some Fair Use hacking is allowed (Ginsburg, Netanel, Lunney, EFF)
- Is it also Fair Use to build a tool to enable Fair Use circumvention? (Boucher/Lofgren would allow)

DMCA has modest consumer protections for these cases:

- Non-profit "shopping" privilege
- Protection of personal data privilege
- Parental control privilege
- LOC rulemaking added two others:
- Broken access control
- Study of filtering software

DRM Technologies Can Prevent Much, but not All of the Piracy Problem – How it Works

DRM is the industry term used to describe the process of managing access, usage and reproduction of electronic products, including databases, research reports, music, newsletters and publications. Owners of these electronic materials have been reluctant to distribute and sell their products over the Internet because they have been unable to control what people subsequently do with these items. According to Barbara Fox, Senior Fellow at Harvard's Kennedy School of Government and a Microsoft Software Architect, Digital Rights Management is an infrastructure to support secure promotion, sale, and delivery of digital content.

DRM Systems always incorporate cooperating, autonomous components. DRM provides for encryption[2] of content, authentication[3] of rights claimants and rights permitted, and secure execution

[2] Encryption's goal is to prevent tampering during distribution. Examples include CSS for DVDs and Pay-per-view, symmetric ciphers, where the same (secret) key is used to encrypt and decrypt a block of content, and key wrapping. (Fox)

environments.[4] Digital Rights Management is based on the ability to protect or 'lock' the content inside an electronic package. The content can only be accessed when a user is furnished with an electronic key (also called a license). That key is tied to the purchaser's computer and can't be shared. If the user passes the content on to another viewer, only the protected package can be transferred. Subsequent recipients must purchase their own access - and receive their own key - in order to access the content. Access to the content is managed by a remote process, which determines which users are granted keys. Typically, access is granted when a user buys the content, or is a member of a group (like subscribers) who are scheduled to receive information on a regular basis.

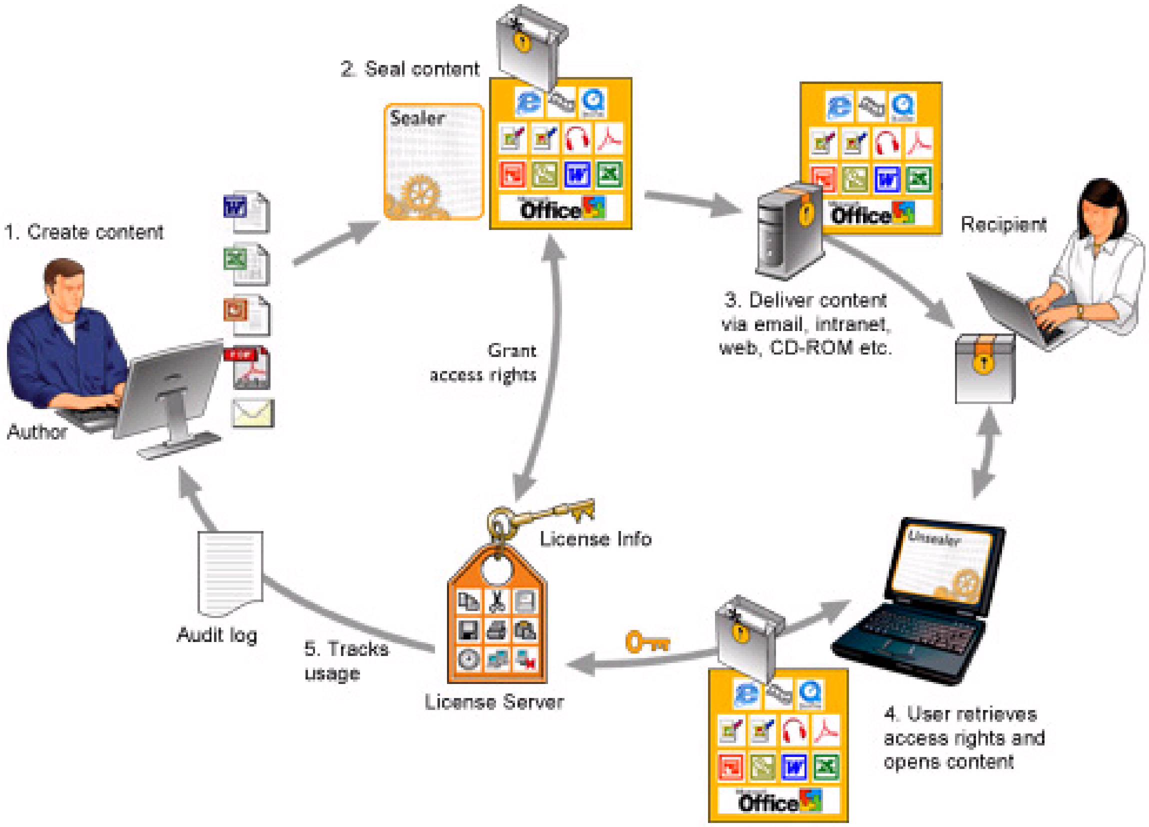


Image Courtesy SealedMedia

DRM-enabled applications, such as those using technology from Adobe, InterTrust, Microsoft, Macrovision, IBM, Real Networks, Apple, or Sealed Media, include management of the process for granting access. DRM can be integrated with media commerce applications to handle the credit card transactions, manage subscription rights, and can discontinue granting new access keys when a document becomes obsolete or has been updated.

[3] Authentication is the process of establishing confidence in the truth of some claim. The goals in DRM systems include content authenticity, device authentication, user authentication, and authorization to access content. Authentication technologies include: biometrics, tickets/tokens, user authentication shared secret, smartcards, Public Key certificates, watermarking (embed a secret message in an image), and fingerprinting (identify and compare images). (Fox)

[4] Secure Execution Environments include hardware-based closed systems, such as purpose-built boxes with “trusted” software, no programmability, and controlled outputs, or its software analog, such as “Trusted” subsystems within a PC used to “containerize” content controlled by permissions derived from machine-readable licenses. (Fox)

The policy-related tasks in DRM system include:

- Content owners (or their agents) author policy statements for content.
- Owners license their exclusive rights (in a copyright sense) to consumers or distributors. DRM-aware servers (or networks) distribute policy statements. Maybe they distribute the content too.
- End-user DRM systems consume and abide by policy statements when processing the content.

Lamaccia observes that, "As an industry, we understand the "crypto" aspects of DRM better than we understand the "policy" aspects. Key management is easier than policy management. Critical "policy" work areas include authoring and evaluating policy expressions and projecting policy expressions with confidence into remote environments" (Lamaccia). It is just that ability to project policy with confidence in technology implementations that is one of the critical sources of the controversy. Fundamentally, technology cannot be expected to implement a policy that the human beings involved have not agreed to.

DRM Has Limitations as an Implementation of Social Policy

Drew Dean of SRI concludes that:

- Technical measures for DRM have a bad track record
- Technical solutions to legal problems are a bad idea
- Legal solutions to technical problems are a bad idea

Likewise, John Erickson of HP Labs cites the constraints imposed by software. He cautions, "Policies that are subject to many exemptions or based on conditions that may be indeterminate or external are difficult or impossible to automate with DRM. Only those policies that can be reliably reduced to yes/no decisions can be automated successfully." (Erickson 36-37).

Alex Alben, VP of Real Networks, summarizes that, "Digital products can be parsed by: time, number of plays, identity of user, location of user, type of device." However, "Expectations derived from our familiarity with manipulating physical copies no longer apply." He asks whether enhancing the value of rights in copies necessarily diminish personal use rights? What is needed is a system design that maintains both personal use and copy protection in order to create a marketplace that works. (Alben)

In a keen observation of the dichotomy between legal policy and software limitations, Joan Feigenbaum of Yale argues that, "In US Copyright Law, owners are given (fairly) well defined rights. Users are given "exceptions" to owners' rights. This is no way to specify a system!" She concludes a need for an affirmative, direct specification of what users are allowed to do. "Fair Use analysis therefore requires a fact intensive, case-by-case approach. This is no way to engineer a mass-market system!" (Feigenbaum)

DRM Technologies Can Indeed Enable Intentional and Unintentional Privacy Abuses

However, as Cohen states, "Stronger privacy protection is not necessarily incompatible with stronger copyright enforcement." (Cohen 49) Privacy protections can be built in and DRM systems can be designed so certain classes of information cannot be tracked, as Macrovision claims.

Decision-Making Dimension – Re-evaluate the Real Problem

What is an ethical software engineer to do? The engineer faces a conflict between Fundamental Moral Responsibilities (FMRE), as Stanford's Robert McGinn would state it. (McGinn, *Moral Responsibilities* 6-19) Those FMREs in conflict include:

- FMRE1 – Not act in any way that one knows (or should have known) will harm (or pose an unreasonable risk of harming) the public interest. Consumers' property rights and Fair Use rights may be impacted.

- FMRE3 – Assure that all parties likely to bear non-trivial risks from one's engineering work are adequately informed about them upstream and given a realistic chance to give or withhold their consent to their subsequent imposition. Consumers need to know the constraints that will be imposed on them by DRM technology. Content owners need to know that no security software will ever stop 100% of the dedicated pirates 100% of the time, and that just one pristine digital copy roaming the Internet can cause serious financial harm.

- FMRE4 – Work to the best of the engineer's ability to serve the legitimate business interests and objectives of the employer or client. Make products that are demanded by customers (content owners) that allow them to protect their property rights. But this must be done in a manner that is legal for the content owner and ultimate consumer. In addition, the engineer likely knows that the DRM alone will not solve nor make up for the problem that intrusive technology demanding new or painful consumer behavior will cause the consumers to "vote with their pocketbooks" and refuse to buy the protected content.

The Ethical Path Forward

Two principles put forward by McGinn can lead the way to resolution.

- A bounded Contextualized Theory of Human Rights (CTHR), and
- The Derived Moral Responsibility of the Engineer (DMR)

What gives consumers the right to expect that their experience of ownership with a physical album of songs, a physical CD, or a physical book should be replicated in the technologically maximalist and risky world of instantaneous global communications and information transfer? Why do academics and critics automatically assume that their ability to copy intellectual property for non-commercial uses in the physical book or photo world automatically translate into the same rights when the work is in electronic form? What gives cryptographic researchers the right to circumvent security codes and publish the hacks to a global audience, regardless of its potential negative impact on the livelihood of an entire industry of creative artists, production staff, investors, and developers of DRM technology? What makes the content industry have the right to shift its costs for outdated business models of a pre-digital industry to the Criminal Justice System in a digital era, rather than absorb the inordinate costs of pursuing suits in Civil Courts for intellectual property infringement?

While a case could be built citing artists as natural resources, debilitating financial costs to content owners as a group, and threats to aesthetic and cultural amenities, the case of entertainment industry content owners would be weak and non-compelling to the public. However, when these peripheral CTHRs are combined with compelling DMRs, a course of action can become apparent.

In the case of McGinn's DMRs, two, applicable in this case, derive from the engineer's fundamental moral responsibilities of related to loyalty to the employer/client (FMRE4). They are:

- The DMR to disclose to the employer or client any unrecognised options, and
- The DMR to help the employer or client reach a clarified definition of problems originally presented to the engineer in distorted form.

These DMRs are important because the real problem, hidden among the throng of competing rights holders, is that consumers want to buy exactly what they want (no more and no less), when they want it, make personal copies of it, share it with friends, and take it along with them. Using the music example, consumers want to buy single songs for less than $1, like they did with 45-RPM vinyls. They don't want to have to buy 12 songs on a $14 CD when they only like two of them. They want to make copies to mix for parties or to take along in the car. They want to loan them to friends. They want to be sure that they can play an archived version 10 years later. They want to own the work, not rent it. These consumer wants have to be tempered with the realities of the modern technologically maximalist society where personal wants in aggregate can destroy an industry.

If the content owners provide high value content, at the right price point, in a convenient manner, with an invisible rights management system that explicitly states and enforces rights that both the content owner and consumer claim, the competing interests may be managed through the normal working of the marketplace. What the content owners need is financial protection while they take a reasonable amount of time to turn a very large entrenched industry from analog to digital.

What the content owners need from engineers, is advice on formerly unrecognized options to a redefined problem.

New Ethical Paradigm

Maximize the Most Just Distribution of Benefits -- Give Customers More and Better Choices

The production constraints on traditional content developers force them into offering “one size fits all” products. Digital rights management services can let the client easily produce a variety of offerings from existing content. In some cases, potential customers may only need a ‘slice’ of a larger product and wouldn’t purchase the entire offering. By producing electronic products, publishers can easily sell content segment-by-segment, since the client won’t actually print a new piece of content. Similarly, clients can create "ultra premium" products for their most demanding, high-end customers. This ability to easily offer different pricing and content combinations is a revolutionary capability for studios.

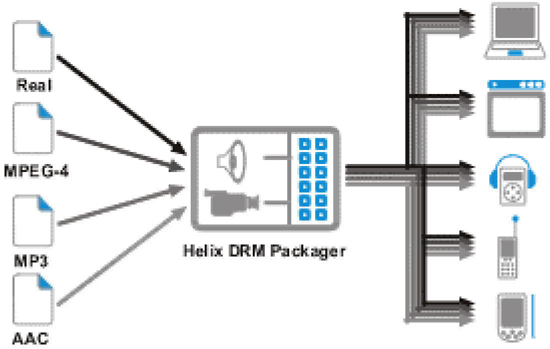


Image Courtesy Real Networks

New, creative, DRM-enabled business models might include:

- Multiple content files on multiple devices per user
- Rights tied to membership groups
- Rights revocation and renewal based on status change
- Subscription, as has been done in cable and satellite
    - Membership-based
    - Time limits (Rental)
    - Usage limits
    - Copy limits and conditions
    - Flexible pricing structure (ex: discount cards, volume discounts, fan clubs)
- Superdistribution – Benefit from pass-along
- Syndication – Many fluid relationships, many contracts Slicing – Repackaging chunks of content as new product
- Content Re-Use – Exploit existing footage, models, characters, backgrounds, clips, scores, etc.

Offering better, more targeted products means the client can find new customers who are willing to purchase content in the form in which they need it. The client will be able to develop a wide range of electronic products that it wouldn't ordinarily keep in inventory, yet still can create revenue with a DRM-enabled service.

Context-Sensitive, Bottom-up Framework that Inverts the 'Sacred' Claims of Rights Holders

Rather than reinforce an outdated notion among consumers that they have the right to expect that their experience of ownership with a physical album of songs, a physical CD, or a physical book should be replicated in the technologically maximalist and risky world of instantaneous global communications and information transfer, DRM developers and content owners need to make it clear that in return for new creatively bundled electronic products and equally creative price points, these products are being made available based on explicit licensing terms.

Fair Use advocates, such as academics and critics, should not automatically assume that their ability to copy intellectual property for non-commercial uses in the physical book or photo world translate into the same rights when the work is in electronic form. Rather, free previews of selections, lower resolution and lower audio quality versions can be made available as part of a good DRM application design.

Cryptographic researchers may have the right to circumvent security codes for academic reasons, but severe penalties must ensue for violations of intellectual property non-disclosure agreements and patent violations that result from publishing the hacks to a global audience.

Fundamentally, the content industry should not have an unbounded right to shift its costs for outdated business models of a pre-digital industry to the Criminal Justice System in a digital era, rather than absorb the inordinate costs of pursuing suits in Civil Courts for intellectual property infringement. It needs to embrace the DRM technology, make legitimate alternatives available to consumers, and abandon the Copyright Law as the basis for DRM rights and rules, in favor of Civil Law that should be explained in simple opt-in/opt-out license terms. As Larry Lessig proposes, we should plan for the 80%-90% of the mass market that wants to do things legally, instead of treating the majority as the criminal minority. (Lessig)

Build the Ethics into the Product Design Process

Since it is easier for software developers to build in explicit permissions than to build in context-sensitive exceptions, DRM applications should consider address the property rights claims by product disclosure labels on the packaging and by enabling explicit consumer and content owner rights in simple licensing agreements based on civil Contract Law, instead of the exception-based Copyright Law. Likewise, Fair Use for most cases can be accomplished with preview capabilities, such as giving a sample chapter of an eBook, playing a 30-second sample of an audio file, showing a short video clip or a lower resolution version of a longer video clip, and offering creative information barter options to the consumer. As Cohen proposes, DRM developers and standards bodies also should be encouraged to address privacy interests of users by incorporating privacy protections, such as anonymization techniques, into their systems. (Cohen 49)

The Basis for the Conclusions

DRM Cannot Enforce a Context-Sensitive Copyright Law

HP Lab's Erickson argues that, "Responsible development of DRM requires that technologists understand the legal and social contexts in which these systems will operate." (Erickson 39). As such, as Erickson reminds us, "In the case of fair use, no explicit set of rules can be implemented and automatically evaluated by computing systems." He acknowledges a more freeform textual statement of intended use is required in DRM systems. Perhaps there is a role for impartial third-parties that act as license-granting authorities, notes Erickson. (Erickson 38)

Copyright Law Should Not be the Basis of DRM Implementations

As Feigenbaum aptly notes, "There are lots of clever arguments in favor of users' rights to reverse engineer and users' rights to circumvent. These arguments are correct but insufficient. As system engineering and as a philosophical position, if fair use is a part of the copyright bargain, one should not have to hack around a [DRM] to make fair use." DRM designers need to be able to recognize the typical, vast majority of fair uses extremely efficiently and permit them.[5] She recommends a way forward to include:

- "The best TPS is a Great Business Model." [Lacy, Maher, and Snyder 1997]
- Use technology to do what it does naturally.
- An Internet content-distribution business should benefit from uncontrolled copying and redistribution. (Feigenbaum)

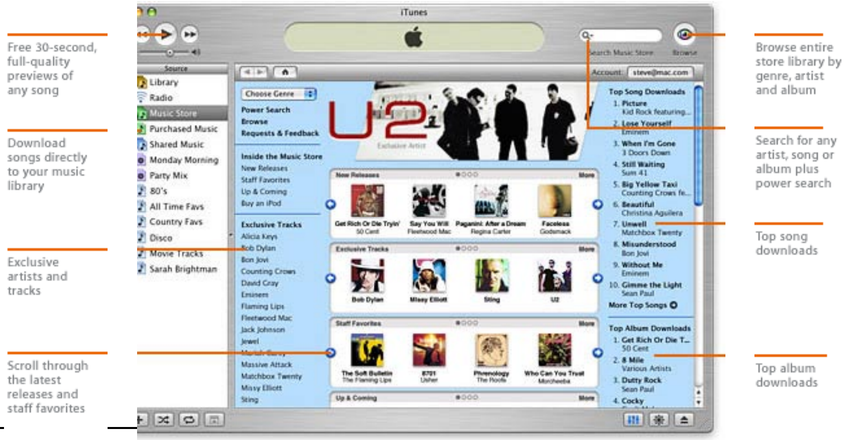
Peer-to-Peer File Sharing is not the Problem, but it Can be Combined with DRM to Become an Enabler of New Business Models

Peer-to-Peer file sharing technology is not inherently illegal. As such, we see ways in which one might take advantage of the enabling capabilities of P2P in a manner that goes beyond exclusively preventive approaches. For example, the music industry might be able to use DRM technologies to provide persistent content protection, creative use of free previews, and online purchase offers in combination with the highly favorable business models and marketing strategies of superdistribution.[6] While not a 100% cure to neutralize the P2P piracy threat, content owners could use P2P as a significant enabling device for massive marketing channels and extensive pass-along content distribution.

See Appendix 1, which presents a hypothetical financial model. It shows how P2P distribution of DRM protected files can be highly profitable, even with a small amount of piracy accepted. It also shows how the same technology with unprotected files results in disastrous financial results. Finally, it demonstrates how simple pass-along via email attachments to personal friends is a net marginal gain for the content owner.

Give the Consumers what they Want – The Apple Example

Apple's recently announced iTunes Music Store has the most relaxed rights requirements among online music services. It uses an internally developed DRM called Fairplay that restricts the titles to three Macintoshes plus and an unlimited number of iPods. It allows unlimited CD burns for a single song, but restricts it to individual songs, and restricts playlist burning to 10 times per unchanged playlist.


Free 30-second, full-quality previews of any song
Download songs directly to your music library
Exclusive artists and tracks
Scroll through the latest releases and staff favorites
Browse entire store library by genre, artist and album
Search for any artist, song or album plus power search
Top song downloads
Top album downloads
iTunes

[5] Note that, in the analog content-distribution world, the vast majority of Fair Uses are non-controversial.

[6] Superdistribution scenario --The v Shop nd Exclusive Content is c Browse digi Search t distribution opportunity that had not been conceived of a few years ago. When customers download electronic content, they may choose to email it to their colleagues or friends. In this fashion, a single piece of content can be reproduced repeatedly and shared among individuals, groups, and even communities. It's a powerful capability if the owner can be paid for each pass along copy. Using a DRM-enabled application or service provider, studios "package" their content inside an electronic container, and it's only accessible to customers who have paid for the content. Customers can send colleagues copies of a purchased product, but in protected form only. The recipient can't access it until they have purchased their own copy. When a potential customer receives the content and tries to open it (play it), an offer page soliciting online payment, coupled with some free preview capability is presented. Persistent protection ensures that the content can't travel freely over the Internet. This concept of superdistribution, where a piece of content is continuously multiplied and forwarded, is a core benefit of doing business over the Internet. Presumably, this model can be extended to peer-to-peer networks.

Image Courtesy Apple Computer

From a security perspective, they have made the DRM very painless, almost invisible for the typical legal customer. But, it also makes it very difficult to upload songs for massive illegal distribution. The burns are restricted to a Macintosh (5% of the market), so the risk of rampant PC file sharing is addressed. Limiting the playlist to 10 burns makes it tough to copy the equivalent of a CD.

From a feature perspective, it adds value to the consumer experience by: (a) making great use of the preview capability, (b) tying into downloadable music videos, (c) enabling CD burning for legitimate uses, and (d) allowing the CDs to be portable from Mac, to CD player, to car. Where the other PC-based services compete with incompatible DRMs, Apple can own its niche with seamless integration between the music service, the Mac, Quicktime, iMovie, iDVD, and iPod.

From a business model perspective, the DRM has allowed Apple to trump the other services, which offer subscriptions, by selling singles for $0.99 without the requirement of a subscription. It supports impulse purchases. It makes a 10-song iTunes collection cheaper than a 10-song CD. They are giving people what they want and in its first week, Apple sold over 1 million songs.[7]

They have benefited from the hard lessons of the other services that went before them. Apple also has a loyal Mac-based following that trusts Apple. One quote from Steve Jobs is, "We are the only service that doesn't treat its customers like criminals." Even though much of the PR is hype, they look like heroes to the "little guy" the way they became heroes to the same market with the Macintosh.

Apple certainly starts to validate that DRM is best used to enable a creative business model, not just tie the content down. By addressing the business model, Apple makes DRM acceptable. It remains to be seen if this very engaging business model can be trusted in the PC space

Professional Responsibility of Software Developers

The Ethics espoused by the ACM and the IEEE-CS Group reaffirm, not only the obligation of software engineers to do no harm, but they must also work in a positive, proactive, life-affirming fashion to the betterment of society. Excerpts from the ACMs ethics canons include:

- Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work. Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.
- Moderate the interests of the software engineer, the employer, the client and the users with the public good.
- Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.
- When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.
- Computing professionals are obligated to protect the integrity of intellectual property. Even when software is not so protected, such violations (illegal copying) are contrary to professional behavior.
- It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

- See Appendices 2 and 3 for complete versions of the ACM and the Joint ACM/IEEE-CS ethics canons.

[7] From Apple press release, May 4, 2003.

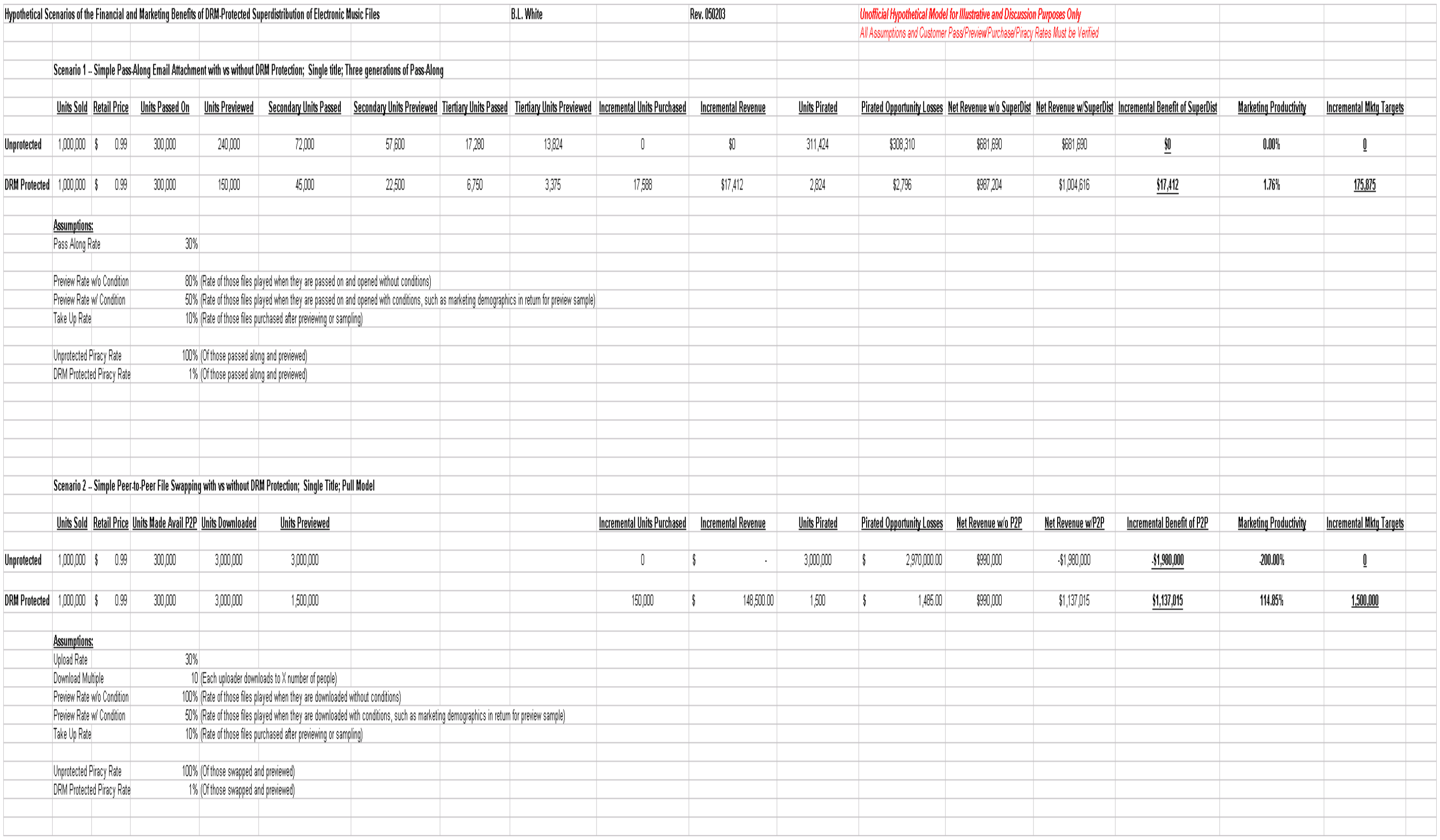
- ○

List of Works Cited and End Notes follow Appendices 1-4

Appendices

Appendix 1 ---

Scenarios of DRM vs. Non-DRM Enablement of Digital Music in Superdistribution



Hypothetical Scenarios of the Financial and Marketing Benefits of DRM-Protected Superdistribution of Electronic Music Files B.L. White Rev. 050203

Unofficial Hypothetical Model for Illustrative and Discussion Purposes Only

All Assumptions and Customer Pass/Preview/Purchase/Piracy Rates Must be Verified

Scenario 1 -- Simple Pass-Along Email Attachment with vs without DRM Protection; Single title; Three generations of Pass-Along

	Units Sold	Retail Price	Units Passed On	Units Previewed	Secondary Units Passed	Secondary Units Previewed	Tiertiary Units Passed	Tiertiary Units Previewed	Incremental Units Purchased	Incremental Revenue	Units Pirated	Pirated Opportunity Losses	Net Revenue w/o SuperDist	Net Revenue w/SuperDist	Incremental Benefit of SuperDist	Marketing Productivity	Incremental Mktg Targets
Unprotected	1,000,000	$ 0.99	300,000	240,000	72,000	57,600	17,280	13,824	0	$0	311,424	$308,310	$681,690	$681,690	**$0**	**0.00%**	**0**
DRM Protected	1,000,000	$ 0.99	300,000	150,000	45,000	22,500	6,750	3,375	17,588	$17,412	2,824	$2,796	$987,204	$1,004,616	**$17,412**	**1.76%**	**175,875**

Assumptions:

Pass Along Rate	30%	
Preview Rate w/o Condition	80%	(Rate of those files played when they are passed on and opened without conditions)
Preview Rate w/ Condition	50%	(Rate of those files played when they are passed on and opened with conditions, such as marketing demographics in return for preview sample)
Take Up Rate	10%	(Rate of those files purchased after previewing or sampling)
Unprotected Piracy Rate	100%	(Of those passed along and previewed)
DRM Protected Piracy Rate	1%	(Of those passed along and previewed)

Scenario 2 -- Simple Peer-to-Peer File Swapping with vs without DRM Protection; Single Title; Pull Model

	Units Sold	Retail Price	Units Made Avail P2P	Units Downloaded	Units Previewed	Incremental Units Purchased	Incremental Revenue	Units Pirated	Pirated Opportunity Losses	Net Revenue w/o P2P	Net Revenue w/P2P	Incremental Benefit of P2P	Marketing Productivity	Incremental Mktg Targets
Unprotected	1,000,000	$ 0.99	300,000	3,000,000	3,000,000	0	$ -	3,000,000	$ 2,970,000.00	$990,000	-$1,980,000	**-$1,980,000**	**-200.00%**	**0**
DRM Protected	1,000,000	$ 0.99	300,000	3,000,000	1,500,000	150,000	$ 148,500.00	1,500	$ 1,485.00	$990,000	$1,137,015	**$1,137,015**	**114.85%**	**1,500,000**

Assumptions:

Upload Rate	30%	
Download Multiple	10	(Each uploader downloads to X number of people)
Preview Rate w/o Condition	100%	(Rate of those files played when they are downloaded without conditions)
Preview Rate w/ Condition	50%	(Rate of those files played when they are downloaded with conditions, such as marketing demographics in return for preview sample)
Take Up Rate	10%	(Rate of those files purchased after previewing or sampling)
Unprotected Piracy Rate	100%	(Of those swapped and previewed)
DRM Protected Piracy Rate	1%	(Of those swapped and previewed)

-- Appendix 2 --
ACM Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles, which apply to computer ethics, are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1. GENERAL MORAL IMPERATIVES.
As an ACM member I will ....

1.1 Contribute to society and human well-being.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

1.2 Avoid harm to others.

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society,all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honor property rights including copyrights and patent.

Violation of copyrights, patents, trade secrets and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

1.6 Give proper credit for intellectual property.

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

1.7 Respect the privacy of others.

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages,without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honor confidentiality.

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.
As an ACM computing professional I will ....

2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence.

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways:doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work.

ACM members must obey existing local, state,province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate,individual members should seek and utilize peer review as well as provide critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm,including the reporting of professional violations.

2.6 Honor contracts, agreements, and assigned responsibilities.

Honoring one's commitments is a matter of integrity and honesty.For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences.

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 - "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.
As an ACM member and an organizational leader, I will ....

BACKGROUND NOTE:This section draws extensively from the draft IFIP Code of Ethics,especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context"leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context"organizations" are corporations, government agencies,and other "employers," as well as volunteer professional organizations.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore,organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.

Current system users, potential users and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems.In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4. COMPLIANCE WITH THE CODE.
As an ACM member I will ....

4.1 Uphold and promote the principles of this Code.

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM.

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct: Ronald E. Anderson, Chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund. This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

ACM/Code of Ethics. Last Update: 01/16/98 by HK.

--- Appendix 3 ---

Software Engineering Code of Ethics and Professional Practice

ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices

PREAMBLE

Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.

The Code contains eight Principles related to the behavior of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession. The Principles identify the ethically responsible relationships in which individuals, groups, and organizations participate and the primary obligations within these relationships. The Clauses of each Principle are illustrations of some of the obligations included in these relationships. These obligations are founded in the software engineer’s humanity, in special care owed to people affected by the work of software engineers, and the unique elements of the practice of software engineering. The Code prescribes these as obligations of anyone claiming to be or aspiring to be a software engineer.

It is not intended that the individual parts of the Code be used in isolation to justify errors of omission or commission. The list of Principles and Clauses is not exhaustive. The Clauses should not be read as separating the acceptable from the unacceptable in professional conduct in all practical situations. The Code is not a simple ethical algorithm that generates ethical decisions. In some situations standards may be in tension with each other or with standards from other sources. These situations require the software engineer to use ethical judgment to act in a manner which is most consistent with the spirit of the Code of Ethics and Professional Practice, given the circumstances.

Ethical tensions can best be addressed by thoughtful consideration of fundamental principles, rather than blind reliance on detailed regulations. These Principles should influence software engineers to consider broadly who is affected by their work; to examine if they and their colleagues are treating other human beings with due respect; to consider how the public, if reasonably well informed, would view their decisions; to analyze how the least empowered will be affected by their decisions; and to consider whether their acts would be judged worthy of the ideal professional working as a software engineer. In all these judgments concern for the health, safety and welfare of the public is primary; that is, the "Public Interest" is central to this Code.

The dynamic and demanding context of software engineering requires a code that is adaptable and relevant to new situations as they occur. However, even in this generality, the Code provides support for software engineers and managers of software engineers who need to take positive action in a specific case by documenting the ethical stance of the profession. The Code provides an ethical foundation to which individuals within teams and the team as a whole can appeal. The Code helps to define those actions that are ethically improper to request of a software engineer or teams of software engineers.

The Code is not simply for adjudicating the nature of questionable acts; it also has an important educational function. As this Code expresses the consensus of the profession on ethical issues, it is a means to educate both the public and aspiring professionals about the ethical obligations of all software engineers.

PRINCIPLES
Principle 1: PUBLIC

Software engineers shall act consistently with the public interest. In particular, software engineers shall, as appropriate:

1.01. Accept full responsibility for their own work.

1.02. Moderate the interests of the software engineer, the employer, the client and the users with the public good.

1.03. Approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the user, the public, or the environment, that they reasonably believe to be associated with software or related documents.

1.05. Cooperate in efforts to address matters of grave public concern caused by software, its installation, maintenance, support or documentation.

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

1.07. Consider issues of physical disabilities, allocation of resources, economic disadvantage and other factors that can diminish access to the benefits of software.

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

Principle 2: CLIENT AND EMPLOYER

Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest. In particular, software engineers shall, as appropriate:

2.01. Provide service in their areas of competence, being honest and forthright about any limitations of their experience and education.

2.02. Not knowingly use software that is obtained or retained either illegally or unethically.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge and consent.

2.04. Ensure that any document upon which they rely has been approved, when required, by someone authorized to approve it.

2.05. Keep private any confidential information gained in their professional work, where such confidentiality is consistent with the public interest and consistent with the law.

2.06. Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic.

2.07. Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.

2.08. Accept no outside work detrimental to the work they perform for their primary employer.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

Principle 3: PRODUCT

Software engineers shall ensure that their products and related modifications meet the highest professional standards possible. In particular, software engineers shall, as appropriate:

3.01. Strive for high quality, acceptable cost and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public.

3.02. Ensure proper and achievable goals and objectives for any project on which they work or propose.

3.03. Identify, define and address ethical, economic, cultural, legal and environmental issues related to work projects.

3.04. Ensure that they are qualified for any project on which they work or propose to work by an appropriate combination of education and training, and experience.

3.05. Ensure an appropriate method is used for any project on which they work or propose to work.

3.06. Work to follow professional standards, when available, that are most appropriate for the task at hand, departing from these only when ethically or technically justified.

3.07. Strive to fully understand the specifications for software on which they work.

3.08. Ensure that specifications for software on which they work have been well documented, satisfy the users' requirements and have the appropriate approvals.

3.09. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work and provide an uncertainty assessment of these estimates.

3.10. Ensure adequate testing, debugging, and review of software and related documents on which they work.

3.11. Ensure adequate documentation, including significant problems discovered and solutions adopted, for any project on which they work.

3.12. Work to develop software and related documents that respect the privacy of those who will be affected by that software.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized.

3.14. Maintain the integrity of data, being sensitive to outdated or flawed occurrences.

3.15 Treat all forms of software maintenance with the same professionalism as new development.

Principle 4: JUDGMENT

Software engineers shall maintain integrity and independence in their professional judgment. In particular, software engineers shall, as appropriate:

4.01. Temper all technical judgments by the need to support and maintain human values.

4.02 Only endorse documents either prepared under their supervision or within their areas of competence and with which they are in agreement.

4.03. Maintain professional objectivity with respect to any software or related documents they are asked to evaluate.

4.04. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

4.06. Refuse to participate, as members or advisors, in a private, governmental or professional body concerned with software related issues, in which they, their employers or their clients have undisclosed potential conflicts of interest.

Principle 5: MANAGEMENT

Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance . In particular, those managing or leading software engineers shall, as appropriate:

5.01 Ensure good management for any project on which they work, including effective procedures for promotion of quality and reduction of risk.

5.02. Ensure that software engineers are informed of standards before being held to them.

5.03. Ensure that software engineers know the employer's policies and procedures for protecting passwords, files and information that is confidential to the employer or confidential to others.

5.04. Assign work only after taking into account appropriate contributions of education and experience tempered with a desire to further that education and experience.

5.05. Ensure realistic quantitative estimates of cost, scheduling, personnel, quality and outcomes on any project on which they work or propose to work, and provide an uncertainty assessment of these estimates.

5.06. Attract potential software engineers only by full and accurate description of the conditions of employment.

5.07. Offer fair and just remuneration.

5.08. Not unjustly prevent someone from taking a position for which that person is suitably qualified.

5.09. Ensure that there is a fair agreement concerning ownership of any software, processes, research, writing, or other intellectual property to which a software engineer has contributed.

5.10. Provide for due process in hearing charges of violation of an employer's policy or of this Code.

5.11. Not ask a software engineer to do anything inconsistent with this Code.

5.12. Not punish anyone for expressing ethical concerns about a project.

Principle 6: PROFESSION

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01. Help develop an organizational environment favorable to acting ethically.

6.02. Promote public knowledge of software engineering.

6.03. Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04. Support, as members of a profession, other software engineers striving to follow this Code.

6.05. Not promote their own interest at the expense of the profession, client or employer.

6.06. Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07. Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08. Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09. Ensure that clients, employers, and supervisors know of the software engineer's commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10. Avoid associations with businesses and organizations which are in conflict with this code.

6.11. Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12. Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13. Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

Principle 7: COLLEAGUES

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01. Encourage colleagues to adhere to this Code.

7.02. Assist colleagues in professional development.

7.03. Credit fully the work of others and refrain from taking undue credit.

7.04. Review the work of others in an objective, candid, and properly-documented way.

7.05. Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06. Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07. Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08. In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

Principle 8: SELF

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03. Improve their ability to produce accurate, informative, and well-written documentation.

8.04. Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05. Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08. Not influence others to undertake any action that involves a breach of this Code.

8.09. Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

This Code was developed by the ACM/IEEE-CS joint task force on Software Engineering Ethics and Professional Practices (SEEPP):

Executive Committee: Donald Gotterbarn (Chair), Keith Miller and Simon Rogerson;

Members: Steve Barber, Peter Barnes, Ilene Burnstein, Michael Davis, Amr El-Kadi, N. Ben Fairweather, Milton Fulghum, N. Jayaram, Tom Jewett, Mark Kanko, Ernie Kallman, Duncan Langford, Joyce Currie Little, Ed Mechler, Manuel J. Norman, Douglas Phillips, Peter Ron Prinzivalli, Patrick Sullivan, John Weckert, Vivian Weil, S. Weisband and Laurie Honour Werth.

Last Update: 09/02/98 by HK

--- Appendix 4 ---

IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making engineering decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;

2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;

3. to be honest and realistic in stating claims or estimates based on available data;

4. to reject bribery in all its forms;

5. to improve the understanding of technology, its appropriate application, and potential consequences;

6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;

8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;

9. to avoid injuring others, their property, reputation, or employment by false or malicious action;

10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

Approved by the IEEE Board of Directors
August 1990

Works Cited

Alben, Alex. *Digital Rights Management and Public Policy.* RealNetworks, Inc. Berkeley, CA. Presentation given at the UC Berkeley Law & Technology of DRM Conference, February 28, 2003.

Cohen, Julie E. *DRM and Privacy.* **Communications of the ACM.** Vol. 46. No. 4, April 2003, pp 47-49.

Dean, Drew. *Digital Rights Management: A Contrarian's View.* SRI International Computer Science Laboratory. Presentation given at the UC Berkeley, Tutorial for the Law & Technology of DRM Conference, February 27, 2003.

Erikson, John S. *Fair Use, DRM, and Trusted Computing.* **Communications of the ACM.** Vol. 46. No. 4, April 2003, pp 34-39.

Feigenbaum, Joan. *Looking at Copyright Law as a Computer Scientist, Consumer, and Teacher of an E-Commerce Course.* Yale University. Presentation given at the UC Berkeley Law & Technology of DRM Conference, February 28, 2003.

Felton, Edward W. DRM, Black Boxes, and Public Policy. Dept. of Computer Science, Princeton University. Presentation given at the UC Berkeley Law & Technology of DRM Conference, February 28, 2003.

Fox, Barabara. *Introduction to DRM Technologies and Their Applications.* Microsoft. Presentation given at the UC Berkeley, Tutorial for the Law & Technology of DRM Conference, February 27, 2003.

LaMacchia, Brian. *DRM Policy and Rights Expression on the Trusted Platforms of the Future.* Microsoft. Presentation given at the UC Berkeley, Tutorial for the Law & Technology of DRM Conference, February 27, 2003.

Lessig, Lawrence. Stanford University Law School. Presentation given at the UC Berkeley Law & Technology of DRM Conference, February 28, 2003.

Lessig, Lawrence. *The Architecture of Privacy, Draft 2*. Presented at the Taiwan Net '98 conference. Taipei, March 1998.

Liu, Joseph. *The DMCA and the Regulation of Scientific Research*. Boston College Law School. Presentation given at the UC Berkeley Law & Technology of DRM Conference, February 28, 2003.

McGinn, Robert. *Ethics, Science, and Technology.* 1990.

McGinn, Robert. *Moral Responsibilities of Professional Engineers: Empirical and Theoretical Approaches.* Presentation given at the Engineering Ethcis Forum, University of Nagoya, Japan. December 8, 2002.

McGinn, Robert. *Technology, Demography, and the Anachronism of Traditional Rights.* Journal of Applied Philosophy, Vol. 11, No. 1, Spring, 1994, pp. 57-70.

Samuelson, Pamela. *The Legal and Policy Landscape Concerning DRM Technologies.* Presentation given at the UC Berkeley, Tutorial for the Law & Technology of DRM Conference, February 27, 2003.

Samuelson, Pamela. DRM {AND, OR, VS.} The Law. **Communications of the ACM.** Vol. 46. No. 4, April 2003, pp 41-45.