Journal of
INDUSTRIAL
TECHNOLOGY

Volume 20, Number 4 - September 2004 through December 2004

Contextualizing Digital Rights Management: Past, Present, and Future

By Dr. Paul Cesarini

Peer-Refereed Article

KEYWORD SEARCH

Information Technology
Internet
Leadership
Legal Issues
Philosophy

The Official Electronic Publication of the National Association of Industrial Technology • www.nait.org

Dr. Paul Cesarini is an Assistant Professor in the Department of Visual Communication & Technology Education (VC&TE) at Bowling Green State University. His current research and work focuses on digital rights management and the on-going erosion of fair use for audio, video, and text. Prior to teaching in VC&TE, Paul created and managed the BGSU Student Technology Center, Laptop Loan Program, and annual Technology Fair. He reads Wired far too much.

Contextualizing Digital Rights Management: Past, Present, and Future

By Dr. Paul Cesarini

Introduction

This article explores the historical context of digital rights management (DRM), and it examines how DRM technologies and the accompanying assumptions that initially arose from them evolved into the host of rights models educators and others now use, or in most cases, are forced to use. It suggests that the reasoning behind even the earliest forms of DRM remain essentially the same even today; that is, under the guise of protecting existing intellectual property and exploring new market opportunities, DRM cements existing business models and distribution methods, regardless of whether doing so hinders emerging technologies and emerging opportunities in education. This article also includes a brief overview of the Digital Millennium Copyright Act (DMCA), including an analysis of the reasoning behind its initial creation and the resultant unintended consequences it has had on innovation, creativity, and computer-mediated learning.

Why Digital Rights Management?

When discussing DRM, what, precisely, am I talking about? Digital Rights Management usually has been broadly defined, with approximate definitions such as "the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders" (Planet eBook, 2003). How could such a harmless-sounding term as digital rights management potentially create so much difficulty for teachers and learners? In order to examine how DRM "fits" in terms of teaching and learning with technology, it is necessary to examine how DRM originally evolved.

Hard-fought skirmishes in the past concerning copyright and intellectual property may initially seem far removed from the various measures of digital protection employed today (Cesarini, 2003). Yet, the current state of DRM technologies and policies now exist only because such debate ever occurred. In 1908, for example, the music industry railed against player pianos (Maier, 2002). Decades later in 1931, the music industry waged pitched battles against the latest technology at the time: radios. They unsuccessfully argued that hotels could not play recordings of their copyrighted songs on their in-house hotel radio stations. Additionally, in 1968 the publishing industry fought vigorously against photocopiers, claiming libraries did not have the right to allow researchers to make copies of medical articles and documents. Similar battles went on between content producers and users of new technologies over the next few decades, pitting the television networks against cable television, and Hollywood against the VCR. The battle over the VCR reached such a level of divisiveness that Jack Valenti, the recently retired Chairman of the Motion Picture Association of America (MPAA), compared the VCR to a murderer. Valenti stated "the VCR is to the American film producer and the American public as the Boston strangler is to a woman home alone" (Maier, 2002).

The current policies and technologies of control asserted over new and emerging technologies like Internet radio, digital video recorders (DVRs, also called personal video recorders, or PVRs), and peer-to-peer file sharing networks (P2P) closely resemble similar battles fought over the past century. In each successive case, the technology

may be different but the central issue remains: What is the balance between giving content consumers convenience, flexibility, and choice, and giving content producers security and revenue?

Although it is difficult to isolate the historical origins of DRM with any degree of certainty, Rosenblatt, Trippe, and Mooney (2002) generally agree that it came about with the maturation of the Internet. That is, the Internet is the primary arena that duplicates of copyrighted digital files are distributed. Prior to that, the arena was largely one of "sneakernet": duplicate copies of copyrighted digital files were manually distributed either by hand or mail. As such, it could then be argued that before the Internet existed as we have come to know it, DRM was limited to technologically enforcing software copyrights. There was simply no large-scale mechanism in place for the distribution of unauthorized audio and video. Of course, bootleg cassette tapes of concerts were available, but were limited to underground cultures (i.e., face-to-face exchanges at social events). Consequently, there was no equally large-scale effort to squelch such efforts.

All that has changed. Metcalfe, Cerf and others collectively brought together Ethernet, TCP/IP, and a host of other connectivity protocols needed to link together millions of computers worldwide. Web browsers and file transfer protocol (FTP) applications gave users of information technologies convenient, point-and-click interfaces for exchanging content. Search engines such as Google and Metacrawler gave people the means to sift through and isolate the information and content they needed. New compression techniques and cheap hard drives enabled them to condense and store vast amounts of audio, video, and text on devices the size of keychains. These technological advances grew and continue to grow each year, and our collective capacity to find uses for them also has grown. Unfortunately, the same technologies that educators use to communicate, teach, and learn, can also easily be used to illegally encode and transfer copyrighted digital works. Such a Jekyll-and-Hyde use associated with many of these technologies has lead to a barrage of frustration for content producers and content consumers yet, as Strong suggests, the issues associated with this struggle over the future of digital media and copyright "are never clearly defined and frequently are not known until the end of a lawsuit" (Strong, p.178). Herein lies the problem.

"Letting Loose the Light"

As the proliferation of bandwidth and inexpensive storage media grew, so did rights models, or the "specification of who can do what to or with a file" (Rosenblatt et al., 2002, xi). Rights models first arose out of UNIX-based mainframe environments, and their associated permission settings capable of being imposed on directories and individual files. The methods of imposing rights models manifested in a variety of forms throughout the 1980s and early 1990s, depending on the specific company and product. Quark, for example, was infamous for its widely adopted use of the so-called "hardware dongle". It would be physically attached to a port on a computer, and it was necessary to run authorized copies of their flagship design tool, Quark Xpress. According to Rosenblatt et al., other rights models that were adopted by different companies included "guiltware" or "scareware," which made stern warning messages visible on the media and during installation, and the somewhat offensively named "naziware," whereby combinations of both serial numbers and product activation keys were needed to unlock software. Additional methods included requiring the physical media that the software had been shipped on be inserted into the computer using it, whenever the software was needed. These various methods of imposing rights models proved at best only slightly effective, though, and often resulted in confusion and frustration.

For example, the widespread rollout of Quark Xpress at university computer labs was difficult at best. Quark did not allow their product to use typical site license management tools, such as Sassafras Software's Key Server program. Although most software site licenses could be rolled out remotely then scaled to whatever numbers of computer the license dictated, the widespread adoption of Quark Xpress on campuses necessitated an equally widespread dongle adoption--all manually installed, in a one-to-one ratio per system. Quark has since modified its methods of imposing rights models for Quark, but it is still generally considered one of the more inconvenient and frustrating ones currently in use.

The term "digital rights management" itself was likely first coined in 1994, when IBM and Electronic Publishing Resources launched two of the first well-known, commercially available DRM products (Rosenblatt et al., 2002, xi – xii). Even though these products no longer exist, much of the technology used in them continues in other forms. These and other DRM efforts were then collectively shoved into the public eye by way of a landmark paper by Mark Stefik, titled "Letting Loose the Light: Igniting Commerce in Electronic Publication." Stefik was a researcher at the famed Xerox Palo Alto Research Center, the center responsible for innovations such as the graphic user interface, the mouse, ethernet, postscript printing, and a host of other technology systems that comprise much of modern computing. In this paper, Stefik argued that "it should always be possible to strictly define and control who can do what to a piece of content, when, on what devices, and for how much money or other form of consideration" (Rosenblatt et al., 2002, xii). Additionally, Stefik coined a term that now carries with it much negative connection: trusted system. Trusted systems were, in Stefik's view, devices that hold data and "implement a precisely defined set of behaviors on that data", with no way of accessing or modifying that data other than by way of the trusted system. Stefik's view of DRM and trusted systems amounted to a rigid, restrictive world where "all content rights are defined and controlled by automated

processes"(Rosenblatt, et al., 2002, xii). Luckily for educators, Stefik's views were only partly accepted by business and commercial interests.

Enter the Digital Millennium Copyright Act

Regardless of whether Stefik's notions of near-complete control of media by copyright holders were embraced, or even technically possible, the idea of the trusted system remains very much alive today. This is perhaps where the 1998 Digital Millennium Copyright Act (DMCA) truly comes into play as the enforcement and punitive mechanism of DRM. That is, without the DMCA, it would not matter what rights models are employed by different types of content producers. Trusted systems would exist only if their features were desirable by consumers and institutions. However, this is not the case. The DMCA and proposed legislation such as the so-called "Berman Bill" (a Bill sponsored by Rep. Berman and Sen. Hollings) that would legalize network attacks by content producers essentially call for the universality of trusted systems, in the home, at the workplace, and in the classroom.

If this sounds somewhat far-fetched, it may be because federally mandated trusted systems and federally sanctioned computer cracking seem antithetical not only to higher education, but also to America. It may also seem as though such legislation would not be enacted in the first place or would be technically unfeasible even if enacted. In the case of the Berman Bill, it remains to be seen if it will be passed into law and then whether it will be technically possible to implement it.

However, the lobbying organizations for the content-producing industry, including the Recording Industry Association of America (RIAA) and MPAA, have already initiated similar undertakings using far more questionable tactics. In fact, the RIAA recently attempted to attach a rider to an antiterrorism bill that would have authorized the RIAA to launch Distributed Denial-of-Serve (DoS, or DdoS) attacks to computers suspected of storing copyrighted audio and video files. The end result would be partially or completely disabled systems. The key term in this case is suspected. That is, no actual proof would be necessary to launch such an attack; it would be left up to the discretion of the content producer (McCullagh, 2002). Had this rider passed, it would have effectively meant it was open season on personally or institutionally owned systems. Students working against a paper or presentation deadline could well have been locked-out of the computer they were using. Faculty giving a lecture via distance learning software could well have been knocked offline by a DoS attack if their computer was suspected of storing such infringing content.

Additionally, the rider stipulated that content producers could not be held liable or otherwise responsible for any data loss or corruption resulting from the attack. This particular rider did not pass; however, newer efforts are under way which would not only allow the RIAA or MPAA to partly or completely disable a system, but would also potentially allow the remote deletion of certain file types often associated with piracy. Students or faculty with vast libraries of legally acquired digital audio or video files might unexpectedly find them being deleted by way of virus-like programs. These programs are being quietly financed and stealthily distributed by the content producing industry, all under the shield of the DMCA (Sorkin, 2003).

As for the DMCA itself, it has been used as a legal club to stifle innovative classroom technologies and squelch academic freedom for over fours years and shows little sign of abatement in this regard. The DMCA was enacted as a compromise solution to protect Internet Service Providers (ISPs) from being held liable for the transmission of copy-protected works by their subscribers. Sara Duetsch, associate general council at Verizon, described the DMCA being conceptually started much earlier, though. She states that:

> It started in . . .1994 when the U.S. Patent and Trademark Office came up with their 'green paper' (policy document) on the National Information Infrastructure (NII). It talked about this horrible new device called the Internet that was a giant copying machine. One of the conclusions of the green paper was that the best policy was to hold the service provider liable. That phrase awakened a sleeping giant. The telecom industry never paid attention to the topic before. At the same time, the copyright community introduced a bill called the NII Protection Act that made all temporary copies illegal. (McCullagh, 2001)

In this case, the temporary copies mentioned refers to even cached and buffered copies of copy-protected content. However, caching audio and video files is the primary means by which these files are made available online. Web browser caches hold copies of previously-viewed content, such as web pages, as well as audio and video clips. These cached or buffered copies typically serve as a staging areas of sorts, with only the content that has changed being downloaded from their respective sites with each new request. Caching is a quicker and more efficient way to access frequently needed content than having to download every single image, word, and multimedia file associated with the page(s) each time. (Techencyclopedia, 2004)

Because ISPs understandably did not want to be held legally liable for copyrighted works or even the cached copies of these works, they were forced to negotiate what is now known as the DMCA with lobbyists from content-producing industries. Under the DMCA, distributing or rebroadcasting copyrighted materials in any way was a felony, as was disabling any DRM technical measures wrapping these copyrighted works. Although this may not initially seem nefarious, the scope of the DMCA has since been expanded considerably. Duetsch stresses that,

> The content community would like . . .to have the service provider block infringing sites that are not located on our network and to use digital rights management tools to stop peer-to-peer transmissions. . . .Their strategy right now is to use DRM bills as a way to reopen the DMCA and to get remedies through forcing technologies on other industries. (McCullagh, 2002)

This notion of mandating DRM has been a constant refrain from the MPAA, the RIAA, and the Software & Information Industry Association (SIIA). From the late 1990s to the present day, steps are being taken technically and legislatively to turn current and emerging technologies into these rigid, trusted systems--regardless of the desires of students, faculty, and end-users of these technologies. Yet, can we blame the content-producing industry? As audio, video, and text becomes increasingly divorced from the physical wrappers that long contained it, widespread piracy continues on a scale previously unimagined. We have seen this manifest itself more and more over the years, with products like Napster, Gnutella, Kazaa, and the now-defunct Aimster, making it relatively easy to transfer text, audio, and video to anywhere, from anywhere. As a result, lawsuits by embattled content producers and copyright holders are an almost daily subject on the evening news.

Will these lawsuits eventually take care of the problem of illegal file trading, or will a different solution be necessary? How will these lawsuits and the current mindset of DRM and trusted systems at all costs affect computer-mediated learning? In his interview with Royle (2003), Fred Von Lohmann, Senior Intellectual Property lawyer for the Electronic Frontier Foundation, argues that the entertainment industry has "made it clear that they will sue any company that uses or offers general-purpose P2P tools." Lohmann also asserts that copyright law

> has been built on the premise that you go after the guy who actually breaks the law. . . .no one ever suggested that Ford should be liable for every bank robbery committed with one of its cars. Yet the entertainment industries appear to want to let all the bank robbers run free and only punish the car makers. It makes you wonder whether the fight is actually about piracy, or if it's instead about asserting control over new technologies. (Royle, 2003)

The end result, according to Lohmann and others, is total control over "culture, radio, television, literature, music, art, information" (Royle, 2003) and knowledge by content producers, regardless of what we hope to accomplish with students in terms of computer-mediated learning.

Institutionally, this control has been stealthily slipping into the electronic classroom, by way of seemingly benign software that many students have become accustomed to using. Windows Media Player (WMP) is a prime example of this. It is the standard audio / video player that comes bundled with any version of the Windows operating system and, as such, has rapidly become pervasive in higher education. Yet, WMP may well pose serious privacy and security concerns, both individually and institutionally (Festa, 2002). According to computer privacy and security expert Richard Smith and others, WMP 8 had the following capability: Each time a DVD was played on a computer, WMP contacted a central Microsoft server to get information for the DVD. When this contact was made, the server was given an "electronic fingerprint" which identified the DVD being accessed and a cookie which "uniquely identifies a particular WMP player" (Smith, 2002). WMP also built a database on the hard drive of the host system, of all DVDs accessed. Additionally, there did not appear to be any option to stop it from "phoning home" when a DVD movie was viewed, or clearing out the DVD movie database on the hard drive.

The Microsoft privacy policy for WMP did not disclose that the software contacts central servers to get this information, nor did it disclose what kind of tracking Microsoft used, what purpose it served, or how cookies were and are used by WMP in this regard. Although it is difficult to determine if these covert forms of DRM exist in the current versions of WMP, clearly such actions represent a technology of control that has little business being in our classrooms.

Educators also are beginning to see the negative consequences of the DMCA as they affect our pedagogical decisions. These consequences have manifested in a variety of ways, in a variety of disciplines:

- If a computer science instructor wants to demonstrate to students how the Content Scrambling System (CSS) used in commercials DVDs works by writing a relatively simple program to allow these DVDs to play on Linux-based systems, doing so would potentially be a violation of the DMCA, and has been the subject of an on-going series of lawsuits initiated by the MPAA. (Borland, 2004)
- If that same instructor wants to examine how Internet content filtering systems such as Net Nanny or Cybersitter work by reverse engineering the programs to see how and when they under-block and over-block web sites, doing so would potentially be a violation of the DMCA. (Leydon, 2003)
- If an instructor in electronics and computer technology wants to demonstrate how hardware modification chips function, by way of a project involving adding such a chip to a proprietary system such as Microsoft's Xbox (for the purposes of installing open source software on the system), doing so would potentially be a violation of the DMCA. (Fahey, 2004)
- If a specialist in encryption technology were to find gaps in copy protection standards used in commercial electronic books eBooks, and then presented those findings at a research conference here in the United States, doing so would potentially be a violation of the DMCA. This exact scenario occurred with when Russian

> encryption specialist Dmitri Skylarov presented such findings about DRM technology used to protect Adobe eBook content, a derivative of the PDF format. Skylarov was arrested immediately after his presentation, and was jailed for over two months as the Justice Department attempted to build an ultimately unsuccessful case against him. (Dvorak, 2001)

In short, many seemingly innocuous pedagogical and research activities could now be violations of the DMCA, and could--as in the case of Dmitri Skylarov--result in arrest and prosecution. Fair use and/or educational use would not necessarily be a strong enough shield to protect the academic freedom of the instructor or potentially even the institution itself from a DMCA-based legal assault. Such consequences could have a chilling effect on future research in these and other areas, perhaps even leading to academic conventions and conferences in these areas being held outside the U.S. to avoid potential prosecutorial efforts in the future.

DRM: Classrooms of the Future?

How do technologists deal with a rapidly "wrapperless" society, a society where content is no longer bound by physical media? Kurzweil (1999) and others debated this very issue over a decade ago. He stated:

> We are used to paying for the knowledge content of products so long as it is integrated into something with mass. We recognize that a $300 software product is physically identical to a few $2 floppy disks, and thus we are primarily paying for the information contained therein. We are aware (or should be) that the manufactured cost of a compact disc recording is less than 50¢ (depending on volume), and that again we are paying for the (musical) information. It is, after all, the information we are after. We obtain no pleasure from the discs themselves. (Kurzweil, 1999, p. 300)

Barlow agrees, referring to it as a simple problem with a complex solution. He states, "If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we [content producers] protect it?" (1999, p. 318-319) Unfortunately, the answer is simple: They cannot digitally protect it in the manner in which they have been accustomed. I believe that time is at an end. Existing patent and copyright laws are at best ill-equipped for the nuances associated with emerging technologies. Barlow goes on to assert that most technology "is detaching itself from the physical plane, where property law of all sorts has always found definition. . . .Even the physical/digital bottle to which we've become accustomed--floppy disks, CD-ROMs, and other discrete, shrink-wrappable bit-packages--will disappear" (Barlow, 1999, p.319).

Additionally, even Larry Ellison, mercurial CEO of Oracle, agrees. Years ago in Cringely's *Triumph of the Nerds: The Rise of Accidental Empires* documentary about the birth of the personal computer industry in America, Ellison predicted the death--and utter impracticality--of the wrapper. He stated:

> Me going down to the store and buying Windows, I've got to get into my car drive down to a store buy a cardboard box full of bits you know encoded on a piece of plastic CD-ROM and you bring it home and read a manual to install this thing--you must be kidding you know, put the stuff on the net--it's bits, don't put bits in cardboard, cardboard in trucks, trucks to stores, me go to the store, you know, pick the stuff out, it's insane. (Cringely, 1995)

Ellison espouses the same wrapperless society as Barlow, Kurzweil, and others did before him. This wrapperless society seems not only logical but likely inevitable, particularly with broadband Internet access gradually displacing narrow band analog modems across the country. The distribution mechanism is there. Unfortunately, this distribution mechanism also represents the worst nightmare of our traditional content providers for audio, video, and text.

How, then, do content-producing industries deal with many of their products not having standardized file formats, standardized DRM, or even a standardized distribution method? This is the situation the RIAA has been in for some time now, pre- and post-Napster. This is the situation in which the MPAA is currently immersed, battling a host of nimble peer-to-peer services such as Gnutella, Freeway, and others that cannot be easily sued. This is the situation the publishing industry dreads, but cannot avoid. For all three industries, all of which have numerous products and services entwined into the fabric of computer-mediated learning and by default technology literacy, the question remains: How do we continue to profit when the distribution mechanisms relied on for so long are becoming less and less relevant to more and more people? There is no easy answer, of course, and it is certainly a monumental issue. Fundamental changes in content distribution will likely be necessary, along with a further consolidation within the respective content-producing industries. Yet, many of these changes--particularly those that involve confusing and restricting DRM rights models--will undoubtedly affect literacy and our students' collective ability to create, innovate, and think critically.

For example, take the hypothetical scenario suggested by Tim O'Reilly at a panel discussion titled *The Near Future of Digital Rights Management*. O'Reilly is the founder and president of The O'Reilly Network, a publishing company focused on technology and software-related texts and course materials. At this panel, O'Reilly posited that the near future of DRM could well be one where piracy prevention is the primary goal, with all other communication, collaboration, and pedagogical considerations falling a distant second. O'Reilly asks:

> What if there was a law that said you couldn't browse the Internet with any device that could be attached to a printer? . . .maybe content providers want to make sure they get page hits from people reading their mate-

> rial. If you print [their material] and give it to a friend, [they] wouldn't be able to track it to get credit for that additional reader. (Steinberg, 2003)

O'Reilly suggests that while most publishers would not care about tracking and getting credit for the additional reader (presumably to charge higher advertising rates), in the near future some publishers might care, and their solution to this problem is to lobby Congress to pass additional laws regulating information and communication technologies. He continues, and suggests the following scenarios:

> Imagine a law that says it's illegal to produce a device that can both display content in a browser and connect to a printer. Now there's someone concrete to sue if the law is broken. Imagine the law says more than that. Suppose it said that your device has to check in with some central authority on a regular basis. This is so that if a device can browse the Internet and later finds a way to connect it to a printer, then the web browsing capabilities can be disabled by this central authority. You would be buying a device because it could perform certain functions--but later these functions can be disabled [remotely] by someone without your permission. (Steinberg, 2003)

Admittedly, trying to imagine O'Reilly's hypothetical situation as reality may seem a bit of a stretch. The implications of having a significant amount of online content being essentially locked away from any device capable of generating hardcopy would be antithetical to teaching and learning with technology.

Unfortunately, O'Reilly's scenario is not too far off from proposed legislation such as the Consumer Broadband and Digital Television Protection Act (CBDTPA). If this bill became law, Princeton University professor Ed Felton argues it would "prohibit the manufacture or distribution of 'digital media devices,' unless those devices include government-approved copy restriction technology" (Felton, 2003). What is a digital media device, according to the CBDTPA? Unless specifically stated as being exempt, a digital media device could be any hardware or software device that reproduces works in digital form; converts copyrighted works in digital form into a form whereby the images and sounds are visible or audible; or retrieves or accesses copyrighted works in digital form and transfers or makes available for transfer such works to hardware or software described in subparagraph (B) (Felton, 2003). Based on this definition, Felton compiled what he refers to as a "hit list" of current devices that would be illegal under the CBDTPA, would necessarily be pulled from the shelves of stores, and removed from computer labs and computer-mediated learning environments, then eventually replaced by "trusted system" versions deemed CBDTPA-compliant. Examples of such prohibited digital media devices could well include:

- Cockpit voice recorders: Newer versions of these use digital storage, rather than tape
- Hearing aids: These devices convert copyrighted works in digital form (say, a track played from a CD) into a form whereby the sounds are audible
- Scanners: These peripherals can duplicate copyrighted images and digitally store them
- Zip drives: These are capable of digitally transferring and storing copyrighted works

Felton's list currently details numerous products and devices commonly used in different industries--particularly in education institutions--that would technically be illegal if the CBDTPA becomes law. While actually confiscating and disposing of every such device would be a logistical impossibility, not to mention a huge drain on federal and state resources, Felton's list demonstrates that O'Reilly's hypothetical scenario could actually represent the near future of DRM.

That is, if the CBDTPA passed, or if newer legislative efforts such as Orrin Hatch's Inducing Infringment of Copyrights (INDUCE, or IICA) Act passed, and if even a smaller-scale crackdown on "digital media devices" (as defined by the CBDTPA) were to occur, the impact on teaching and learning with technology would be felt far and wide. Institutions of Higher education, many of which are already reeling from deep cuts in state funding, would scramble to comply. Existing computer labs would have to be physically and systematically reconfigured, as systems with CD-RW drives, Zip drives, scanners, and related hardware and software deemed illegal would removed from the lab or uninstalled from the computers, or otherwise rendered inoperable for the sake of compliance. New methods for digital storage and file transfer would have to be created and implemented, to ensure no student is duplicating, sending, or receiving copyrighted materials. DRM-based technologies would have to be incorporated into mail servers, to prevent illegally duplicated email attachments. PowerPoint would have to incorporate some form of DRM, to prevent the insertion of copyrighted images, audio, and video into presentations. The same would apply for web publishing software, such as Dreamweaver. The ability to educate our students in computer-mediated learning environments would open to reinterpretation, based on dictates from the content-producing industry.

Conclusion

Technological change is rarely easy, and the growing pains associated with how digital media is replicated and distributed will almost certainly continue to be hotly contested issues for years to come. The needs of the content producing industry are all too often in direct contradiction with the legitimate, fair use needs of honest consumers of this content. This attempted control of how we use technologies to access information, by Microsoft, by the MPAA, by the RIAA, or by similarly large institutions, flies in the face of traditional notions of computer-mediated learning. In the name of fighting piracy, the policies and technologies of control are vying to alter the social

and cultural contexts we have come to expect from teaching and learning with technology.

As faculty and working professionals in technological industries, I believe we should collectively have a greater, more prominent voice in determining how the digital media technologies we use to teach and learn evolve. The problem is that we are not currently exercising that voice. Affiliation with digital media advocacy groups such as the Electronic Frontier Foundation (EFF), the Center for Democracy & Technology (CDT), Computer Professionals for Social Responsibility (CPSR), and DigitalConsumer.org should be actively promoted and encouraged within our respective disciplines, at our conferences, and in our institutions. These organizations actively lobby and litigate to protect current digital rights such as space-shifting, time-shifting, and format-shifting digital content, fair use, and first sale that we have all come to rely on for years inside and outside the classroom. I believe our professional organizations should also move to take official stances against pending legislation that seeks to control access to or distribution of digital media, much as how organizations in other disciplines frequently do, such as the American Library Association's stances against the DMCA and USA PATRIOT Act (Clark, 2004). If we opt not to promote stronger ties to these and similar organizations, and if we instead opt to remain passive in the face of far-reaching DRM technologies and policies, we may soon be faced with an unfortunate reality. All emerging digital media technologies and tools, however potentially useful to computer-mediated discourse and pedagogy, might one day have to be officially sanctioned by legal departments of the content producing industry prior to be released to us, the technologists that use them.

References

Barlow, J. (1999). The Economy of Ideas: A Framework for Rethinking Patents and Copyrights in the Digital Age. In V. Vitanza (Ed.), *CyberReader* (pp. 299 - 319). New York, NY: Allyn and Bacon.

Borland, J. (2004, January 22). Hollywood group drops DVD-copying case. Retrieved September 8, 2004, from http://news.com.com/Hollywood+group+drops+DVD-copying+case/2100-1025_3-5145809.html

Cesarini, P. (2003). Digital Rights Management: Coming Soon to a Class Near You. National Association of Industrial Technology, 2003 Annual Conference Proceedings.

Clark, L. (2004, June 29). ALA Supports Supreme Court Decision on Child Online Protection Act. Retrieved September 3, 2004, from http://www.ala.org/ala/pr2004/june2004/COPASupremect.htm

Cringely, R. (1995). Triumph of the Nerds: The Transcripts, part III. Retrieved October 5, 2004, from http://www.pbs.org/nerds/part3.html

Dvorak, J. (2001, July 23). The Skylarov Gambit. Retrieved September 3, 2004 from http://www.pcmag.com/article2/0,1759,25446,00.asp

Fahey, R. (2004, September 4). USA: Jail sentence and fine for mod chip retailer. Retrieved August 20, 2004 from http://www.gamesindustry.biz/content_page.php?section_name=pub&aid=1502

Felton, E. (2003, February 9). Freedom to Tinker. Retrieved January 3, 2004, from http://www.freedom-to-tinker.com

The Information Society Project. (2003, November 24). Introduction: the Transition to Digital. Retrieved January 10, 2004, from http://www.nyls.edu/pages/1511.asp

Kurzweil, R. (1999). The Future of Libraries. In V. Vitanza (Ed.), *CyberReader* (pp. 291-303). New York, NY: Allyn and Bacon.

Leydon, J. (2003, April 10). DMCA strikes again in N2H2 filtering list. Retrieved September 2, 2004 from http://www.theregister.co.uk/2003/04/10/dmca_strikes_again_in_n2h2/

Maier, M. (2002, April). Technophobia Over the Years. Retrieved July 14, 2002 from http://www.business2.com/articles/mag/0,1640,39436,FF.html

McCullagh, D. (2001, October 15). RIAA Wants to Hack your PC. Retrieved December 15, 2003, from http://wired.com/news/conflict/0,2100,47552,00.html

McCullagh, D. (2002, August 27). Verizon's Copyright Campaign. Retrieved January 13, 2003, from http://news.com.com/2102-1082-955417.html

Planet eBook. Ebooks Glossary. Retrieved Feb 2, 2003, from http://www.planetebook.com/mainpage.asp?webpageid=70

Rosenblatt, B., Trippe, B., & Mooney, S. (2002). *Digital Rights Management: Business and Technology*. New York: M&T Books.

Royle, B. (2003, January 8). Interview with Fred Von Lohmann. Retrieved November 20, 2003, from http://techfocus.org

Smith, R. (2002, February 20). Serious Privacy Problem in Windows Media Player for Windows XP. Retrieved December 3, 2003, from http://www.computerbytesman.com/privacy/wmp8dvd.htm

Sorkin, A. (2003, May 4). Software Bullet Sought to Kill Music Piracy. Retrieved January 4, 2003, from http://64.225.202.40/mediadefender/press%20about%20MD/nytimes_5_8_03_pg1.htm

Stefik, M. (1996). *Letting Loose the Light: Igniting Commerce in Electronic Publication*. Internet Dreams: Archetypes, Myths, and Metaphors. Cambridge, Massachusetts, MIT Press. 219-253.

Steinberg, D. (2003, October 10). The Near Future of Digital Rights Management. Retrieved October 23, 2003, from http://www.oreillynet.com/pub/a/mac/2002/10/03/drm.html

Strong, W. (1999). *The Copyright Book: a practical guide.* Cambridge: MIT Press.

TechEncyclopedia. Retrieved October 3, 2004 from http://www.techweb.com/encyclopedia/