Copyright and Commerce:
The DMCA, Trusted Systems, and the Stabilization of Distribution

Tarleton Gillespie
Science and Technology Studies, Cornell University

appeared in *The Information Society*, (v20n4, Sept. 2004): 239-54.

Abstract: The Digital Millennium Copyright Act has been criticized for granting too much power to copyright holders, offering them new technological controls that may harm the public interest. But, by considering this exclusively as a copyright issue, we overlook how the DMCA anticipates a technological and commercial infrastructure for regulating not only copying, but every facet of the purchase and use of cultural goods. In upholding the law in Universal v. Reimerdes, the courts not only stabilized these market-friendly arrangements in cultural distribution; they extended these arrangements into realms as diverse as encryption research and journalism, with consequences for the very production of knowledge.

Keywords: copyright, DMCA, trusted system, law, DeCSS, intellectual property, journalism, encryption.

Controversy has raged in the courts, in academic circles, online, and in public discourse, about the intersection of copyright law and the Internet. A three-hundred-year-old legal doctrine designed to regulate the distribution of printed materials, and since extended to cover not only books but also music, art, advertising, film, and computer software, now faces significant transformations in the very mechanics and economics of the distribution of all cultural goods. At the same moment, those industries most invested in copyright have an increased sense of urgency because of rising stakes in the so-called knowledge economy. Will the Net prompt the renovation of copyright law and the proliferation of new techniques of cultural production that can exceed traditional copyright's limited imagination? Or will it require the imposition of even more stringent versions of the law, to compensate for the absence of those material and economic constraints that have always been endemic to physical manufacture and exchange?

Or, are these the wrong questions?

The flashpoints of this dispute thus far have certainly been the passage of the Digital Millennium Copyright Act (DMCA) in 1998 and the 1999 lawsuit brought and won by the record industry against the Napster peer-to-peer file trading system, eventually resolved in 2001. Napster and P2P file-trading flaunted the established economic relations of the music industry, implicit in and bolstered by a traditional understanding of copyright law. Its dismantling by the courts, persuaded by the arguments made by legal advocates of the powerful culture industries, seemed to suggest that the corporate view of copyright (more, stronger, faster) was tipping the scales against the amorphous values of public interest and open distribution copyright claims to serve. In the shadow of the Napster showdown, the DMCA appeared to be a similar project, to strengthen copyright to the benefit of corporations.

But despite its name and the way it has been described by both proponents and detractors, I will argue here that the DMCA is only nominally about copyright. While it was put in place on the rhetorical shoulders of a panic about digital piracy, its reach over the production and distribution of culture goes well beyond the traditional bounds of copyright law, to make possible a massive technological and commercial system that will limit not only copying, but will regulate every facet of the purchase and use of cultural goods. Premised more on computer security statutes, it is based on a very different sense of priorities than does copyright. This distinction has been largely overlooked in the court decisions and in the public debate, yet it has far more fundamental consequences, not only for whether I can trade music online or duplicate a DVD, but for the very production of knowledge inside of intricate systems of informal and explicit, institutional and technological controls. By considering this and related cases exclusively in the light of copyright, we have asked the wrong questions, and have overlooked the more dramatic shifts occurring at the nexus of intellectual property law, the culture industries, and the Net.

The Digital Millennium Copyright Act

The language of the U.S. Constitution, which merely authorizes Congress to design more specific copyright laws, also announces its priorities:

> Congress shall have power... to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries... (U.S. Constitution, art. I, § 8, cl. 8)

The book or work of art or computer program you create, by mandate of the law, belongs exclusively to you; you have legal recourse against those who attempt to duplicate, distribute, or perform that work without permission.[1] But rather than basing this privilege on some natural right of authors as such, or on the inviolate character of property, copyright is articulated in terms of social and intellectual progress. It is to the public's benefit when people share what they know, as others may build on that knowledge. At its foundation, "intellectual property" is a means to an end, not an end in itself. As Matt Jackson reminds us, "one cannot overemphasize that the constitutional purpose of copyright is to stimulate content creation for the public's benefit, not to create a private property right based on a moral notion of ownership." (Jackson, 2001, p. 613)

To build a cultural distribution system on the metaphor of "property" itself is a debatable strategy; in many ways, intellectual property does not circulate the way material property does. To further assume that this metaphor will facilitate intellectual progress requires another very particular leap in faith; as Julie Cohen notes, "a model that attempts to relate 'property' to 'progress' must consider the public-good nature of creative and informational works, and cannot assume equivalency between private wealth and social gain." (Cohen, 1998b, p. 560) The Framers of the Constitution, in championing vibrant public discourse, aimed to put this monopoly in the service of the people. Their chief concern was that this legally enforced monopoly is acutely vulnerable to a form of commercial exploitation damaging not just to competitors and customers, but to the entire culture, since the commodity in question is information and knowledge. To avoid this, American lawmakers and courts have since built in additional limitations, aiming to further restrain the power granted to authors and owners, and pass some of that power back to the public at large.

With the rise of the Net, the already unsteady balance inherent in copyright (private vs. public, individual ownership vs. social progress) seemed, quite visibly and dramatically, to explode. Most in the culture industries argued that the ease of network distribution and the perfection of digital reproduction meant that copyright restrictions needed to be even more rigorously enforced.[2] Others thought copyright could shift from a law of property to a kind of contract law for managing relationships between content providers and consumers.[3] And still others believed that copyright could be discarded altogether.[4]

But when the U.S. government began to consider how copyright law should apply to the new information medium,[5] it preferred the corporate view, and introduced a startling new twist. Under the aegis of the Clinton-sponsored "National Information Infrastructure Task Force," a working group on intellectual property was charged with determining what changes if any would be necessary in the context of this new medium. Among their proposals was an "anti-circumvention" statute; if a copyright owner were to distribute a digital work with some kind of technological barrier built in (i.e. password security, watermarking, encryption, anti-copying codes, etc.) it should be illegal for a user to gain unauthorized access by breaking that barrier. Furthermore, it should be illegal to make or distribute a tool that facilitates such a breach. Their justification spoke of a mounting "arms race" between beleaguered copyright owners and wily hackers:

> The ease of infringement and the difficulty of detection and enforcement will cause copyright owners to look to technology, as well as the law, for protection of their works. However, it is clear that technology can be used to defeat any protection that technology may provide. The Working Group finds that legal protection alone will not be adequate to provide incentive to authors to create and to disseminate works to the public. Similarly, technological protection likely will not be effective unless the law also provides some protection for the technological processes and systems used to prevent or restrict unauthorized uses of copyrighted works. ("White Paper," Information Infrastructure Task Force, 1995)

After some Congressional wrangling and its reappearance in a WIPO treaty, the anti-circumvention proposal became the Digital Millennium Copyright Act in 1998.[6]

The DMCA arguably represents the most dramatic change in copyright law in U.S. history; but it is not without precedent. In certain ways, it mirrors current arrangements in the regulation and protection of computer software, where early efforts to apply copyright have been replaced by contract law in the form of "shrinkwrap" licenses. These licenses grant control of both the software in the abstract and the particular copy purchased, and dictating largely at the owner's whim what the user is and is not permitted to do.[7] But the move in both doctrines shifts copyright law's traditional attention to "use" of the "work" (a legal abstraction that pointed to something beyond each individual manuscript or recording, to the creation itself) to regulating "access" to a specific "artifact": this DVD, that book, this copy of the software. Some in the legal community have described the DMCA as "paracopyright" so as to emphasize that it not so much an alteration or expansion of the copyright doctrine, but rather a companion law that straddles it, staking claim on different though overlapping legal territory.[8] But even this is misleading, for the DMCA shares neither the logic nor the strategy of copyright; instead, it anticipates a new technological regime where control depends on the tight coupling of technology and law, each sharing the task of regulation not only copying, but access, use, and purchase.

Universal v. Reimerdes

The home video market had been a decade-long boom for the major movie studios (despite early efforts to sue the VCR into copyright oblivion); by the 1990s, Hollywood hoped to revitalize that market with the power of digital technologies. The goal was, at least at first, to improve on the picture and sound quality of VHS and add the durability and navigational features of the DVD disc format. But the broader aspiration was not just digital movies, but digital transmission. The industry hoped they could soon outdo the "pay-per-view" services of the cable industry by delivering their films online.

But the ease of distribution the Net offered and the quality of reproduction afforded by digital tools were more than enough to reawaken old fears of copyright infringement, and Hollywood waited until they had a solution: the Content Scramble System (CSS). CSS is an encryption algorithm that scatters the digital data of the film around the surface of the DVD. For authorized playback, the necessary algorithm key is built into DVD players so that the machines can read the encrypted disc, recover the scattered data, and display the film.

It is important to recognize that this technique is a lock, rather than a block. Instead of recognizing and prohibiting certain uses, it prohibits access, until access can be granted under controlled circumstances. The difference is an important one. Encryption here is not itself a copy protection, at least not directly.[9] Instead, films are protected from reproduction by ensuring that DVD players do not allow copying, and ensuring that the DVDs can only be played on these authorized machines.

In a sense, this has been the strategy of the movie industry since its inception. While the music industry sells its music once, and uses copyright to control unauthorized re-distribution, the movie industry controls distribution through access boundaries: the ticket counter, the velvet rope, the theater door. This depends as much on arrangements with associated industries as on copyright law. Studios prevent piracy in the theater not only by prosecuting the sale of the bootlegs, but also by delegating responsibility to theater owners to patrol ticketed audiences for illicit video cameras. I use the term "delegate" deliberately, to invoke Bruno Latour's conception of technology as a delegation of human tasks to nonhuman actors. Just as we can either put a hydraulic piston on a door to close it, or hire a doorman to serve the same function, the movie studios have an array of tactics, human and otherwise, by which they can keep that theater "door" closed. And just as Latour suggests we choose strategically between different tactics, preferring the hydraulic piston over the doorman for cost and reliability, the control of DVD use imposed by the CSS encryption is a preferable choice either to the vagaries of human responsibility, or, importantly, the limitations of copyright's exclusive focus on use. (Latour, 1988)

And access control is not just for copy protection; by controlling access to the theater rather than reproduction of the work, the movie industry has developed ways to monetize each viewing experience, rather than possession: seeing a film in the theater requires purchasing a ticket for each viewing; seeing it again requires a second payment. Under this arrangement, ancillary markets can be based on layers of access (second-run theaters, exhibition on airplanes, hotel pay-per-view, video rental, video purchase, subscription cable, commercial television broadcast), with fewer restrictions and cheaper prices at each level. Control of copying only protects future sales; control of access protects future sales and regulates the current sale as well.

As with the arrival of Napster, Hollywood's trouble would come from the community of independent designers who have embraced the Net as both technical playground and libertarian

experiment. DeCSS, an application so tiny it can be written in as few as 434 characters and printed on a T-shirt,[10] is an application that removes ("De") the protective encryption ("CSS") from a DVD and stores the film in its linear, unencrypted form. DeCSS does not work by cracking the CSS algorithm; it is simply a digital key ring that opens the DVDs the way they were supposed to be opened, but not by those devices authorized to open them.

When the story of DeCSS is told, the starting point is typically Jon Johansen, part of a team of Norwegian hackers called the "Masters of Reverse Engineering" (MoRE), who designed DeCSS and first posted it online. The story might just as easily begin with XingDVD Player, an authorized DVD player designed by RealNetworks. RealNetworks failed to encrypt the algorithmic key that opens CSS and plays the DVD. When Johansen's crew discovered this, they were able to extract the hidden key from it; once they had one key, they were able to make educated guesses and identify 170 more.[11]

The story the film industry would subsequently tell, of merciless and unethical hacker pirates hell-bent on stealing their valuable intellectual property and trading it Napster-style with the masses, while not exactly false *per se* is a particular take on the situation. Another would be that the film industry forced hardware designers to collude with them, to keep users from enjoying certain uses of their works; when one of their partners mistakenly violated the agreement, some users with the technical know-how found the opportunity and created a tool that did permit the uses they desired. To stop this the studios turned to a law, which they had themselves helped to create, that would brace their technological-financial ramparts with legal consequences. The technological arms race described by Congress is underway, though the moral clarity of the battle lines may be more ambiguous than first suggested.

In November of 1999, the Motion Picture Association of America (MPAA) demanded that Johansen remove the application from his site; he did.[12] But DeCSS had already been mirrored on websites around the world. In January of 2000, the MPAA sued three of the more prominent websites, (*Universal City Studios et. al. v. Shawn Reimerdes et. al.*, 82 F. Supp 2d 21, 111 F. Supp. 2d 346 [S.D.N.Y. 2000]; the decision was appealed by the defendants, and affirmed on appeal; *Universal City Studios et. al. v. Eric Corley*, 273 F. 2d 429 [2001]) requesting an injunction prohibiting them from posting the application, and charging them with violating the DMCA.[13] The argument made by the movie studios, and that proved persuasive to the court, was straightforward: DeCSS was a device designed to circumvent a technological protection, and posting it on a website was "providing" it. The defendants attempted to address the law itself: first claiming that they fell under one of its exceptions, then questioning the law's implications and thus its constitutionality.

The Copyright Concern: Fair Use and the DMCA

For some of the same social and intellectual reasons that undergird copyright doctrine, limited use of a copyrighted work is sometimes seen as worthwhile even when it is ideologically undesirable for the copyright owner. A book critic should be able to quote from the book even if he is going to tear the book to shreds; a journalist should be able to quote from a corporate mission statement even if the report is condemning that corporation. Copyright holders should not be able to squelch such "fair" uses, either by withholding permission or by charging so much as to make the work practically unavailable.

The law specifies certain conditions under which fair use may apply, ones that resonate with the principles of intellectual progress behind copyright itself: "for purposes such as

criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research"[14] (17 U.S.C. §§ 107). Within these general boundaries, particular uses are judged to be "fair" or not according to four criteria: the purpose and character of the use, the nature of the original work, the amount used, and the impact on the market for the original. The courts are left with a great deal of leeway in weighing these four factors, which means fair use has traditionally been difficult to specify as a practical guideline for users; nevertheless, it is an important counterbalance to copyright power.

The defendants in the DeCSS case, facing the task of challenging a "copyright" statute, attempted to criticize the law for squelching the guaranteed rights of fair use.[15] This has proven a successful strategy in some copyright battles (e.g., *Sony v. Universal*) and unsuccessful in others (e.g., *A&M v. Napster*). Here they would have to argue that important fair uses have been rendered technologically unavailable by CSS encryption, that DeCSS allowed exactly the kinds of uses protected by the fair use doctrine, and that the DMCA was being deployed to stifle those uses by criminalizing the application. But precisely because the DMCA is a law of access and commerce masquerading as a copyright law, this counterargument failed, in revealing ways.

The DMCA's prohibition of circumvention is in two parts: restriction of the act of circumventing, and restriction of tools that facilitate circumvention: one restriction on conduct, one on the instrument. In addition, rather than a simple ban on circumvention of any kind, the law creates a two-tiered restriction, distinguishing between circumvention for the purposes of unauthorized access, and circumvention for the purposes of unauthorized copying. Within the scope of the DMCA, the first is illegal, but the second is not. Since unauthorized copying would already violate existing copyright law, lawmakers did not want the DMCA to impose an additional penalty. However, the part of the statute restricting circumvention tools does not distinguish according to purpose. Therefore, as Figure 1 suggests, three of four circumvention behaviors envisioned by the law are rendered illegal by the DMCA:

Circumvention for the purposes of unauthorized access: **ILLEGAL**	Circumvention for the purposes of unauthorized copying: **LEGAL**
Tools that aid in circumvention for the purposes of unauthorized access **ILLEGAL**	Tools that aid in circumvention for the purposes of unauthorized copying **ILLEGAL**

Figure 1. The two-tiered prohibition of circumvention in the DMCA

The problem is almost too obvious. Circumvention for the sake of copying is legal, but a tool that helps do so is not. Copying is illegal except when it is fair. So the fair user who wants to reproduce a work that is encrypted, and doesn't happen to be a skilled hacker, is out of luck; presumably, tools to help him would be unavailable. The court even admitted that the law grants the tech-savvy a right it withholds from the rest of us: "The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted

works without the technical means of doing so is a matter for Congress, unless Congress' decision contravenes the Constitution..." (111 F. Supp. 2d 346 [S.D.N.Y. 2000], p. 45) Which, the court decided, it did not.

Building Trust

Just as digital technology seems to facilitate the reproduction and distribution of the intellectual property, it also facilitates new forms of technological intervention that are more specific, flexible, and invisible. Well before these lawsuits, the culture industries had already been seeking technological solutions should the legal ones fail. What they seem to be aspiring to is something more vast than just stronger statutes, copy protection systems, and watermarks; they are slowly building the material infrastructure and digital standards, as well as the social, commercial, and legal pre-conditions, for the rise of digital rights management (DRM), or a "trusted system".[16]

Imagine that your "stereo" is a small, hand-held device. It stores, organizes, and plays songs you have purchased in digital form. (Perhaps it is an all-purpose media device: DVD and MP3 player, e-book display, cell phone, wireless web browser, PDA, portable game console, everything but the virtual kitchen sink.) It interfaces with your home entertainment system to play music through your expensive speakers, snaps into your dashboard to play in your car, and pumps tunes through your titanium headphones. To purchase music, you link it to your personal computer to download from your favorite website, or to a kiosk at the mall, or even to a friend's player. This device would offer the ultimate in convenience, audio fidelity... and digital commerce.

The "trusted" part of this system is that this device obeys rules established by the copyright owner when they first make the song available, "digital rights" that would now travel with the work itself. The music is encrypted, and marked with tags that indicate not only its title and artist and such, but its owner, its cost to play or to transfer, its duration of usability, and the account to which such fees are to be paid. These digital "tags" can provide almost any kind of information, including any kind of re-articulated copyright specifications; they can also be flexibly redesigned as the culture industry comes up with new ways to carve up the distribution and use of their product. Trusted devices would "precisely interpret" (Stefik, 1997, p. 140) these digital tags and act accordingly.

Let me quote at length the description of one such system; the comments come from George Freidman, CEO of InfraWorks, and one-time intelligence and security expert for the U.S. military during Operation Desert Storm:

> The InTether system consists of a packager, used by the originator of a file, and a receiver, used by the recipient. The packager enables a publisher, record label, movie studio -- or, for that matter, a law firm, doctor's office, bank or anyone else who wants information security -- to impose a set of restrictions on almost any digital file...
>
> Using the packaging software, the originator can determine how many times the recipient can view or play the file; whether the recipient can alter it and send it to others; the identity of permissible recipients (determined by ID numbers and passwords); whether the file can be printed freely, once, or never; how long the

> file can be viewed or played (in hours and minutes); the date on which the file can first be opened; and the date on which, if the originator wishes, the file will self-destruct and vanish from the recipient's hard drive...
>
> ... From the perspective of the user, the Infraworks software is almost invisible, except that when viewing or playing an InTethered document the consumer will not be able to use certain commands -- typically, the "copy," "print," "cut," "paste" and "save as" commands.
>
> ...The receiver is anchored to the C drive, where it cannot be moved or copied, and it is "cloaked" to render it invisible to the Windows operating system... Although the InTether system does involve cryptography -- InTethered files are encrypted, and the receiver contains the key to decrypt them -- the receiver does much more than that. It places "system-level controls on what you can do that are persistent," Friedman says, effectively overriding the operating system...
>
> "We're fairly deep in the operating system," he says, "so we see what's going on and we either permit or deny it from happening in relation... to the files under our control." (Parloff, 2001)

The rhetoric is classic command-and-control, a far cry from the delicate balance of copyright; it should come as no surprise that the design of this technology has been developed by military security experts. The device, and the entire system, aspires to be a "black box" in the most Latour-ian sense: the "assembly of disorderly and unreliable allies is thus slowly turned into something that closely resembles an organized whole... It is made up of many more parts and it is handled by a much more complex commercial network, but it acts as one piece." (Latour, 1987, pp. 130-131) The user would, ideally, be completely unaware and completely regulated by this system.

These trusted systems would perfectly contain copying. Devices would refuse to output to other devices that were not compliant with these protocols and rules, that were deemed "untrustworthy". This, Lawrence Lessig argues, is a fundamentally different way to enforce law: "What copyright seeks to do using the threat of law and the push of norms, trusted systems do through the code. Copyright orders others to respect the rights of the copyright holder before using his property. Trusted systems give access only if rights are respected in the first place." (1999, p. 130) This system would not require a monolithic system of authority to oversee the production of every device; it would, like the Net, depend only on shared or translatable protocols, so that a network of networks could function together as a system to ensure that the rules are comprehensive and inviolate.

With a trusted system, each transfer, and potentially each use, would accrue charges, which would find their way back to the copyright owner; this would require some form of remote billing or e-cash system not quite in place yet. This system of exchange could extend well past the original point of sale; you might buy a copy of a song from me, or pay a smaller fee to "borrow" it from me, at which point the copy on my device would be disabled temporarily as long as you "had" it. Sales could be for a limited duration, an extended music rental, or for a set number of plays; the device could destroy the song after the authorized period, unless you assented to pay more. The "accountant inside" (Stefik, 1996, p. 241) would log all sales and

transfers, and accumulate them into a monthly bill payable to the record company. "Digital property can be anywhere on the planet without the knowledge of its creators and still make money for them whenever it is used or copied." (Stefik 1996, p. 235)

The trusted system, though regularly justified as a specific response to the threat of online piracy, is much more. It allows for an incredibly subtle and complex parsing of use into any manner of monetizable parts; and it provides a tool that will act as clerk, distributor, broker, and police, all in one. Geoffrey Nunberg has remarked how commercial industries, looking to best transform culture into commodity, often work towards the "morselization" (1996, pp. 120-123) of culture; the flow of ideas and expression is endlessly subdivided into discrete portions -- books, songs, movies, clips, sequences -- so that they may be monetized in individual transactions. This, he argues, is not a cultural logic, but rather a strictly commercial one. The trusted system is a morselizer of newfound capacity; it can divide the same materials into all manner of discrete packages (song, album, number of listens, time period), offering multiple forms of commercial transaction to suit the liking of the user. All of these forms, of course, aspire toward what some see as a rapidly-developing "pay-per-view society", (Mosco, 1988) one where digital technology offers ever more subtle and specific means of commodifying every bit of expression, and every practice involved with it. "Though information has been a commodity from the earliest days of capitalism, the new technology deepens and extends opportunities for selling information by transcending the boundaries that space and time impose on the packaging and repackaging of information in a marketable form." (Mosco, 1988, p. 8) To the extent that such commercial arrangements can, in certain cases, offer economicall equitable services to many, they may have some benefit; however, when a "pay-per-view" arrangement is pursued solely for its commercial value and efficiency, and other cultural needs are overlooked, we risk leaving to the market precisely those aspects of public life we already know are badly served by it.

So what is necessary to make this trusted system work? Certainly the technological apparatus and the necessary protocols must be designed, though this is no small task, and the public must be convinced and/or required to adopt it. This technology clearly has not only a number of parts, but a number of supplemental components, such as e-cash, each of which has some kinks still to work out. But the technology itself, robust as it might be, cannot regulate behavior by itself. As John Law has argued, complex technological systems require "heterogeneous engineering" (Law, 1987), the simultaneous reworking not only of technical artifacts, but also legal, economic, and cultural arrangements to match. The law is a crucial element in this network of arrangements.

While it might be useful to recognize here that these "artifacts have politics" (Winner, 1980), Law's attention to heterogeneity is a useful reminder that material constraints are insufficient as perfect mechanisms of regulation. Low bridges may regulate the passage of people in busses. But it is easy to overlook, as Winner does, that this is both because it is difficult to get under them and because it is illegal for the driver to demolish them as he passes. Material permanence is both a technological and a legal accomplishment, for both the bridge and the trusted system.

The death knell of the trusted system is, of course, the ability to circumvent the built-in rules: "the physical integrity, communications integrity, and the behavioral integrity of a repository are the foundations of a trusted system. A repository is designed with the ability to detect tampering and communications errors and to ensure certified behavior." (Stefik, 1996, p. 240) The system must be designed to withstand attack. If the user can break the encryption, or

trick the system into dumping unprotected copies onto their computer, or pry open and re-wire the device, or re-program the system not to charge for copies, the system will be leaky. And if a hacker can develop a tool to do these things and pass it around on the Net, the entire system will disintegrate.

In its protection against unauthorized circumvention, the DMCA does much more than protect digital copyright; it will be the guardian at the gates of the trusted system, ready to patrol the boundaries of this massive control mechanism. And by emphasizing access rather than copying, it can sanction violations of the trusted system that have nothing to do with copying, but are rather about accessing materials without following the proper channels, i.e. paying for it, and following the rules prescribed by that commercial relationship. CSS and the trusted system proscribe behavior in intense detail and design other behaviors out of existence, and then depend on the law to ensure that consumers use the system as recommended, risking the threat of criminal penalty if they attempt otherwise. But there is still another step necessary before the system is complete.

Beyond Copyright

The most effective way to keep users from copying DVDs is, of course, that DVD players have no record button. Copy protection here is the technological absence of the very possibility of copying. This may seem like an obvious point, but it is merely the tip of this iceberg. CSS encryption is a proprietary lock that forces manufacturers to license the key; since there's only one place to get this key, the studios can demand that manufacturers enforce whatever limits they desire, a king's ransom for their own films they hold hostage and paid, in the end, by the public.

For the CSS encryption system to work, the film industry had to establish an agreement with manufacturers to compel them to restrict the design of their tools. And with encryption, the studio had a decided advantage in setting the terms of this arrangement. Unlike the failed attempt to hold VCR manufacturers legally responsible for user copyright infringement, (see *Sony v. Universal)* or the music industry's botched attempts to get manufacturers to voluntarily agree to restrictions,[17] the studios could simply lock up their content; manufacturers had no choice but to license the key. In this sense CSS serves as a yoke, built by the movie studios, with which to rein in the manufacturers of DVD players and DVD software, so as to enforce the CSS license.

The CSS license, implemented and overseen by the DVD Copy Control Association, maps out an arrangement that any manufacturer of DVD players must agree to and submit to its terms.[18] And it is overwhelmingly about proper hardware copy control; the structural plans for a trusted device. Section 6.2, which take up four-fifths of the 43-page agreement, spell out what precautions the designer of DVD players or applications must take in order to prevent two things: (1) the digital output of the film in a way that would allow duplication, and (2) the playing of regional DVD discs outside of the appropriate locale. These precautions include:

- incorporating copy control signals, such as automatic gain control, in any analog output signal (to, say, a television);
- refusing to deliver a high definition analog signal unless the DVD was already encoded as such;

- only delivering a digital output stream to three authorized formats, (IEEE 1394, USB, and DVI) each of which is equipped with "digital transmission copy protection," and not until they have been further authorized by the studios;
- refusing to play recorded media that indicates that it was never to be copied, or CSS scrambled material stored on a DVD-R;
- scrambling the CSS key inside the workings of the software as it is passed from portions of the system that authenticate to portions that decrypt, to avoid its discovery by hackers;
- ensuring that the controls on regional playback are "closely coupled" with the authentication process, to thwart attempts to re-engineer them;
- actively frustrating attempts to defeat copy protection, to discover the CSS keys, or to discover CSS algorithm info, by encrypting this information, building it into physical architecture, protecting the flows between modules, and self-monitoring the integrity of the system so that modifications will make the entire system fail.

Licensees must agree not only to these terms, but also to make any changes the DVD-CCA requests in light of new circumstances; manufacturers must even agree to surprise spot checks to ensure compliance.

This technologically-enforced licensing scheme is the most egregious intervention into the distribution of cultural expression; by locking up their DVDs, the movie studios can ask almost anything of the hardware manufacturers, who can only obtain the key (necessary to even produce a DVD player) if they agree to every demand. Note, again, that nothing in the DMCA says that "circumvention" should refer only to circumventing the technological controls that specifically prevent copying, or access barriers designed as a yes or no restriction. There's nothing to prevent the culture industries from eventually imposing micro-limitations not only on copying, but on nearly all features of the use. One example that already exists is "regional coding"; each DVD and each DVD player is encoded as being specific to a certain region of the world; DVD players can only play discs from their region. This has little to do with piracy, and everything to do with the studios maintaining a release schedule that debuts films at different times in different countries, and at different prices. Another example is the inability to skip past trailers, ads, or copyright messages at the start of the DVD. Circumvention of either of these restrictions has no copyright implications; it would, however, be a violation of the DMCA.

Protecting CSS

At the time the suit was brought, there were no authorized DVD player applications for the Linux operating system; Linux users could not play DVDs on their computers, discs they had purchased and therefore had authorization to use. Here is a personal use restricted by the business strategy of the film industry, and ensured by the CSS access control. The defendants claimed that the development and distribution of DeCSS was part of a development effort to design a DVD player for the Linux operating system, and that a legitimate tool was being squelched by the stipulations of the DMCA.

Admittedly, the claim that DeCSS was part of a Linux project was probably more in the grey area between accurate and convenient. But what is important here is not the validity of the defense, but the principles by which it was rejected. In the preliminary injunction, Judge Kaplan dismissed the Linux defense when he stated that, "although defendants contended at oral argument that DeCSS was not designed primarily to circumvent CSS, that argument is

exceptionally unpersuasive." (82 F. Supp 2d 21 [S.D.N.Y. 2000], p. 12) This is not what they argued, of course; it was precisely to circumvent CSS. The court rejected the argument by saying that the question was not about use at all. In Judge Kaplan's eyes, even if DeCSS was for playing DVDs on Linux machines, to do so still entailed circumvention of CSS without authorization, violating the DMCA.

Fair use gets hamstrung between access controls and hardware restrictions; there is simply no place for its consideration. The question ignored is not whether DeCSS developers circumvented to infringe, but whether they circumvented to infringe fairly. The law stopped them from circumventing, because they were circumventing for access; the lack of Linux players kept them from making fair use of DVDs. And the law seems uninterested in regulating these interventions; indeed, legislators cannot even see the problem. Consider how responsibility is subtly abrogated inside of this statement, from Judge Kaplan's DeCSS injunction: "In consequence, even though the fair use doctrine permits limited copying of copyrighted works in appropriate circumstances, the CSS encryption of DVD movies, coupled with the characteristics of licensed DVD players, limits such uses absent circumvention of CSS." (111 F. Supp. 2d 346 [S.D.N.Y. 2000], p. 73) What is described as "the characteristics of licensed DVD players" is treated as a natural phenomenon, as if DVD players sprout from the ground without record buttons. In fact, each of those characteristics is explicitly mandated inside of the CSS license. By hiding the system of control inside the technology, not in the CSS encryption scheme but in the hardware itself, the content providers avoid judicial scrutiny, in the glorious name of preventing piracy and ensuring the continued strength of the American economy.

It is clear, then, why it was so important to the movie studios that the courts ensure the security of the CSS algorithm. The threat was not that copyrights would be infringed, but that DeCSS would undermine the power of the license to bind this coalition of content, hardware, and software manufacturers. The designers of DeCSS were not so much pirates as they were upstart manufacturers. Their efforts to participate in the display of movies, outside of the licensing agreement, made them a threat to the studios, the forced collusion with manufacturers, and the profit streams it hoped to generate.[19] What is clear is that a trusted system requires not only a massive technological system, and a law to protect its borders, but also a carefully choreographed arrangement of cooperating and ideologically coherent industries, who are willing -- or compelled -- to produce this technological system according to certain principles, and to submit to legal consequences if they violate that arrangement.

Certifying Related Institutions: Encryption Research

The CSS license compels DVD player manufacturers to adhere to and bolster the trusted system, shoring up the cracks through which intellectual property might slip. The courts have proven willing to certify an arrangement that borders not only on being a trusted system, but also a "trust" in a very different legal sense. But, I would argue, the implications of the application of the DMCA in this case are even more insidious. Not only does the *Universal v. Reimerdes* decision work to certify established manufacturers over upstarts unwilling to agree to Hollywood's rules; it also, in every moment, leans on and borrows from the authority of related institutions to prop up this system of trust: rhetorically associating proper use of cultural goods with other socially legitimate activities, and piracy with illegitimate ones, until a stable matrix of right and wrong is constructed. And in doing so, the decision reifies the existing hierarchy inside

of those institutions as well, by granting them greater legal standing in this context, and an ideological authority in a broader sense.

Congress established certain exceptions to the DMCA's restriction on access circumvention, some regarding only the act of circumventing, others covering both the act and the provision of the necessary tool. With the limited range of these exceptions, the defendants turned to three that might indemnify the provision of a decryption tool like DeCSS: (1) reverse engineering of a lawfully obtained work for the sake of achieving interoperability with other applications; (2) security testing of computers and networks, with authorization of the owner or operator; (3) encryption research that is dedicated to discovering flaws and vulnerabilities of encryption technologies. Again, these might not be the most convincing claims, and may be largely opportunistic defenses; but, again, the significant question here is how the court decided to answer them.

The court rejected the idea that the DeCSS designers were engaged in security testing or reverse engineering with little fanfare; but rebuking the claim that DeCSS was the product of encryption research required a bit more finesse. The defendants argued that, in developing DeCSS, Johansen and his colleagues were studying the CSS protection scheme and looking for its flaws. In a literal sense, this is what they were doing; and barring more official venues, the distribution of the tool over the Net might be seen as a kind of "publication" effort to make their research known. However, the court claimed that the research was not performed in "good faith," as required by the DMCA:

> In determining whether one is engaged in good faith encryption research, the Court is instructed to consider factors including whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement, whether the person in question is engaged in legitimate study of or work in encryption, and whether the results of the research are communicated in a timely fashion to the copyright owner. (82 F. Supp 2d 21 [S.D.N.Y. 2000], p. 17)

That the DeCSS designers are not academically authorized researchers, did not publish what they found in peer-refereed journals, and were not working with the industry, was sufficient proof for the court that their efforts are not "research," and need not enjoy protection from the legal restrictions.

This is not to say that Johansen and company were somehow grossly misunderstood by the court; it is to point out how, even beyond the kind of circulation of copyrighted work being subtly privileged or marginalized by this law, the law envisions a similar distinction between legitimate and illegitimate information distribution in the world of research as well. By building into the DMCA an exception, not for all encryption research writ large, but for a particular kind of encryption research, the law and the courts privilege a particular definition of what counts as research, and relegate other forms to the margins. Academic-based encryption research, which is both institutionally bound and has historically enjoyed a cozy relationship with the computer industry, stands in as the most legitimate form. Excluded is not only amateur hacking, which has often been justified as a kind of tinkering that makes computer systems stronger; also excluded are alternative development systems based less on institutional hierarchy and more on distributed, public, and collaborative work.

Ironically, the most prominent of these is the development of Linux itself, giving credence to the claim that the development of DeCSS as a Linux DVD player may have been conceived as parallel to the design of Linux itself, depending on the same network-based interactions, but deemed unfit as "good faith" encryption research by the courts. What could be a Net-based shift in the very nature of technology research and development is slowed by a decision that de-legitimates new versions in a reach for the authority of the old.[20]

Certifying Related Institutions: Journalism

In appealing the preliminary injunction, the defendants added a fourth tactic to their legal strategy, one that proved the most promising in invoking a compelling legal principle, and forced the greatest caveat by the courts to the censure of DeCSS. Yet it too looked to a related institution -- this time journalism -- for authority, one that had not yet been anticipated in the DMCA. In response, the court found that it had to clarify journalism itself in order to close off this loophole, drawing its own distinction between legitimate and illegitimate forms of news. And in doing so, not surprisingly, the court managed to privilege existing forms of journalism, to the potential detriment of what may be new Net-based alternatives.

In April of 2000, the MPAA was forced to amend their New York complaint in response to the actions of one defendant, Emmanuel Goldstein, also known as Eric Corley. Corley, publisher of 2600, a hacker magazine in both print and online formats, had provided DeCSS on his site. He was one of the three named in the New York lawsuit; after the initial injunction, he was compelled to remove the application from his site, or face criminal penalties. Unlike the other defendants, who complied fully with the initial judgment, Corley removed the application but urged his readers to "mirror" it, i.e. to post it on their own sites, and submit the URL to him. He compiled on the 2600 site a list of links to sites that offered the application, adding new links when they appeared and deleting those that became unavailable. His stated goal was to challenge the rules being imposed on the Net, and the institutions developing a position of power for themselves over the medium; he dubbed his methods "electronic civil disobedience".[21] (111 F. Supp. 2d 346 [S.D.N.Y. 2000], p. 1) This move forced the MPAA to sue not only the "provision" of DeCSS, but also linking to other sites that provided it as well. And by extending the lawsuit to include the act of linking, the MPAA opened up the case to a new defense: freedom of speech. While Corley's list of links did clearly help his readers locate copies of DeCSS, the extent of his action was now entirely in words -- albeit, words that do something.

The particular rights of citizens to disseminate information, often even in the face of potential or real harm to others, have been assured and reassured by American legislation and jurisprudence over the course of the nation's history, though by no means consistently. These rights have especially been assured for journalists; the Framers were adamant that the press be all but immune from government intervention or censorship. And the justification for these special protections is a long-standing belief that journalism is the ultimate protector of democratic life.

Whether or not Corley could claim to deserve protection under the First Amendment, the defense hoped to demonstrate the value of linking itself to the practices of journalism. And to bolster this argument, they attempted to not only characterize hyperlinking as crucial to online journalism, but to posit the Net as finally achieving the fundamental values journalism had always sought. In an amicus brief signed by eight news organizations and associations, Net journalists argued that freedom of the press involves a commitment to giving their readers not

just information, but the tools to make informed decisions on their own; hyperlinking is characterized as a crucial element for fulfilling that mission:

> Hyperlinks enhance online news reporting. The rapid access to layers of supplementary information allows journalists to add depth and context to their stories, making them more meaningful and useful to readers. Links allow the journalist to direct readers to the journalist's primary source material, lending credibility to the report and empowering the reader to investigate independently. (*Universal v. Corley* 273 F. 2d 429 [2001] -- "Online News Association, et. al.: Brief of Amici Curiae in Support of Appellants and Reversal of the Judgment Below," Jan 26, 2001)

By drawing on the now iconic descriptions of the Web and its expressive promise, the journalists could link the medium to the fundamentals of journalism and the freedoms protected by the First Amendment.

In his August 17, 2000 injunction, Judge Kaplan ruled that linking to a site offering DeCSS was tantamount to "providing" the application, and therefore enjoined Corley from posting links to DeCSS mirror sites. But he fretted about the potential "chilling effect" of his ruling, and sought a more subtle intervention that would minimize that chill in contexts where it might be most debilitating to democratic society. His solution depends on a principle of intent; and it builds a distinction precisely along the lines defined by the journalist amicus, reaffirming a particular understanding of journalism and thereby, as with encryption research, re-establishing rules of distribution that privilege certain forms and participants over others.

The court designed three criteria (modeled loosely on the rules regarding defamation of character) for determining liability when a website links to a site offering a circumvention tool illegal under the DMCA:

> there may be no injunction against, nor liability for, linking to a site containing circumvention technology, the offering of which is unlawful under the DMCA, absent clear and convincing evidence that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology. (82 F. Supp 2d 346 [S.D.N.Y. 2000], p. 79)

Some sites will link in order to facilitate the dissemination of DeCSS and similar tools. The court argues that 2600 is one of those sites. But others will do so for other reasons, mainly informational, like a link from CNN.com or The New York Times. The distinction depends on the intent to distribute. Two links, each to the same site offering an illegal tool, may be judged differently by the law, all depending on why they link. As MPAA lawyer Charles Sims put it in an interview with the New York Times, "'When the Times does an article about the drug situation in Manhattan, and mentions that drugs are available on the corner of 85th Street and Amsterdam, that is different than people who are engaged in trafficking in drugs by sending people to buy drugs at different corners,' Sims said. 'The difference is intent, among other things.'"[22] (Kaplan, 2000) Sims attempts to render the intent distinction obvious and righteous, valorizing credentialed journalists and condemning drug traffickers.

But the distinction is not so neat, since the practices appear to be, and claim to be, almost identical. How can intent be proven? Judge Kaplan points to two details that convince him that the intent behind Corley's linking was to distribute rather than to inform. First, before the initial injunction, he had been providing the application himself, which made him already an actual distributor. Second, the page of links explicitly encouraged other sites to mirror the DeCSS application precisely because it would be difficult for the MPAA and the courts to block its circulation. This was enough to convince Judge Kaplan that, at heart, Corley wanted to facilitate the piracy of DVD movies, despite the fact that Corley had painted himself as a journalist.

The problem here is not how this decision applies to Corley, but rather the implications for which cases even see the inside of a courtroom in the future. How do you judge intent when the evidence is not so clear? Will it be tempting to rely on what we know of the speaker, rather than what is said, to divine intent, e.g. CNN is a news institution, thus their intent is journalistic; Corley is a hacker, thus his intent is to distribute? Determining intent is always a game of interpretation, of course, but this is precisely why the risk is so great that judges could be tempted to take contextual factors into account: judging the speech not for what it intended, but for who said it and who they appear to be. Which publications will feel most assured that they can demonstrate benign, journalistic intent if put under the court's scrutiny, and which might back off from linking to sites they see as having some kind of social value, worried that they will be penalized under this revision of the statute? A site like 2600 is much more likely to shy away from linking to a site offering DeCSS or the like, regardless of its intent or its politics within the copyright debate. And, even if jurists continue to restrict their analysis of intent only to the explicit written context of the links in question, which publications will risk (and can afford) a costly lawsuit to test their resolve?

In the end, the distinction set forth by Judge Kaplan for determining linking liability will rely not so much on intent, but on the <u>appearance</u> of intent. Those sites that most clearly signify "journalism" in their design and ideological posture, most defensible as an arm of the legitimate press, will likely feel the safest in posting such links; they will be those that are either online portions of already well-established print or broadcast journalism, or those that most closely emulate the same forms and conventions. In particular, the decision privileges a certain kind of speech -- institutional, dispassionate, and "objective," a mannerism of traditional journalism that has been roundly criticized[23] -- and penalizes speech that does not appear journalistic in this way: the activist, subjective, politicized speech of 2600, for example. On the other hand, forms of information dissemination that do not closely adhere to the traditional conventions of journalism will be at greater risk, i.e. precisely those forms that have been vying with traditional journalism as legitimate alternatives.

Rules make choices about which institutions and practices of expression and distribution will be privileged and which will be restricted. Yochai Benkler puts it this way:

> Many people in society engage in information production. They produce and exchange symbols for a variety of reasons, and using a variety of strategies to appropriate the benefits of their production... The core point to understand about property rights in information is that they have different effects on these different strategies, such that changes in the institutional content of property rights can help some of these strategies at the expense of others. In particular, increases in the scope and reach of property rights benefit commercial producers who sell information goods, at the expense of noncommercial producers and producers

> who appropriate the benefits of their production by means other than sale of rights... In other words, when Congress passes a statute like the Digital Millennium Copyright Act... it is making a choice among types of information producers. (Benkler, 2000)

And,

> ...this type of social choice between different mixes of information production is decidedly political. (Benkler, 2002)

Similarly, the intent distinction privileges established forms of journalism, shutting down alternatives. And it does so way in a way that intervenes now and restrains the possibility of future change; current sites that cannot clearly perform their journalistic intent will be most wary about providing certain kinds of information, and future sites may think twice before even pursuing the role of the press unless they are willing to adopt the classic markings of journalism.

Where we draw the line between what is and is not journalism grants legal protections and cultural authority to some websites and not to others, offering some the right to distribute information as an official arm of a democratically principled and respect profession, relegating others to the status of chat, gossip, propaganda, minutiae. And that line is drawn in the multitude of moments where those rights and authorities are awarded or withheld, such as court cases, like this one. Judge Kaplan's intent distinction, rather than identifying a difference, will help produce one. It will have consequences for what kinds of information dissemination can flourish on the Net, granting traditional journalism greater protection and rhetorical authority than those new forms that do not as easily fit into the characterization of journalism the court composed here, and squelching the real potential of the Net: to innovate on the very forms journalism takes and the sites in which it is produced.

The DMCA itself returns the power of distribution to the hands of the movie studios, the kind of culture providers that copyright law privileges; the DeCSS injunction returns the power the distribute the means of distribution to the traditional press, the kind of information providers that First Amendment law privileges. This intent distinction is, admittedly, a small decision in the scope of all things that shape journalism, or encryption research. It may never appear in a case again. But it is the kind of small gesture towards reaffirming the institutional and marginalizing the alternative that, recurring many times over in countless small decisions, together forms a matrix of forces privileging certain organizations and obstructing others.

A Regime of Arrangement

In the *Universal v. Reimerdes* decision, the courts were willing to give up the messy work of adjudicating copyright, despite the Congressional mandate that has long required it of them. The DMCA has managed to shift copyright from a Constitutional guideline arbitrating the balance between proper and improper use, to a sanction strengthening technological controls of both copying and access designed and implemented by copyright owners. A technological system, encrypted DVDs, was given the legal teeth that the studios had requested and received from Congress in the DMCA. Hollywood could encrypt their films and demand that hardware manufacturers and software designers enforce their preferred uses; Congress would ensure that the system remain secure by prosecuting hackers, discouraging circumventors, and shutting down the channels by which decryption tools might circulate.

The sleight of hand here is that the protection of copyright, the fears of piracy, and the articulation of the Net as a fundamentally unsafe space for cultural expression, all have helped usher in a legally-sanctioned, technologically-enforced collusion of corporate content providers and hardware and software manufacturers, who can together dictate not only the range of possible uses of cultural expression, but also how, when, and to what extent they will be charged for them. And along with that, a series of related institutions are stabilized and lashed together, whose own conservative distinctions between legitimate and illegitimate forms are held fast and mapped onto the copyright dispute, naturalizing and reinforcing the distinction being made, and closing out all manner of upstart alternatives in the process.

If Mark Rose called modern copyright a shift from a "regime of regulation" to a "regime of property," (Rose, 1993, pp. 9-30) I might mark this new approach as a "regime of arrangement": the arrangement of distribution systems through material and legal constraints, the arrangement of allied institutions through technologically-enforced licenses and ideological linkages, and the arrangement of use through a network of restrictions and of facilitations, to dovetail ever more perfectly with commercial interests. Even when hardware manufacturers, for the sake of ensuring that their devices appeal to consumers, might resist the restrictions preferred by copyright owners (as they did in rejecting the SDMI plans proposed by the music industry) , they are now compelled by the CSS encryption to either accept the terms of the arrangement or get out the game altogether.

What is lost are the venues in which the public interest side of copyright could effectively balance the interests of copyright owners, who can only envision the value of discourse through a lens of their own commercial survival and success. What is missing is a reminder that rules about "information" regulate cultural expression, social participation, and the production of knowledge.[24] The possibility that not only the act of expression, but the act of circulation, could be a valuable element of social participation and learning is obscured, shrouded by a system entrusted only to sell, deliver, and collect.[25]

Most of all, as Jessica Litman has pointed out, it is Congress who has abrogated their responsibility to raise the question of public interest. Perhaps this should not come as a surprise; as Jessica Litman has pointed out, Congressional apathy is endemic to the history of copyright legislation more broadly. (Litman, 2001) What was, inside of a legal arena, a positive assertion of rights and values regarding cultural expression, is handed to technologists and private corporations to decide for themselves and hardwire in. (Reidenberg, 1998; Lessig, 1999) What was a question of the rights of citizens becomes a question of the preferences of consumers, as imagined by producers. And lawmakers, who might still have an opportunity to demand that this shift include a debate about people's rights, seem debilitated by the technological sheen the debate has taken on. Consider how the following comment, from the House of Representatives discussions of the DMCA before its implementation, first acknowledges the risks of the pay-per-view society, then reveals a sense of futility about turning the inevitable tide of technological "progress":

> The growth and development of the Internet has already had a significant positive impact on the access of American students, researchers, consumers, and the public at large to informational resources that help them in their efforts to learn, acquire new skills, broaden their perspectives, entertain themselves, and become more active and informed citizens. A plethora of information, most of it embodied in materials subject to copyright protection, is available to individuals, often for free,

> that just a few years ago could have been located and acquired only through the expenditure of considerable time, resources, and money...
>
> Still, the Committee [on Commerce] is concerned that marketplace realities may someday dictate a different outcome, resulting in less access, rather than more, to copyrighted materials that are important to education, scholarship, and other socially vital endeavors. This result could flow from a confluence of factors, including the elimination of print or other hard-copy versions, the permanent encryption of all electronic copies, and the adoption of business models that depend on restricting distribution and availability, rather than upon maximizing it. (HR 105-551, part 2, July 22, 1998, 35-36)

The language is telling: "marketplace realities" might cause the benefits of the Net for wide dissemination of information and debate to diminish, because of "the elimination of" alternatives and "the adoption of business models that depend on restricting distribution". Treating these changes as marketplace "realities" erases the responsibility of Congress to regulate the market, something it has been less and less willing to do in recent years; even in light of a foreseeable and potentially tragic shift, Congress sees itself as only able to adjust to these changes rather than orchestrate preferred alternatives. And the industry has been adamant in encouraging this hands-off approach to regulation; a recent joint statement from the record, computer, and software industries, worried that future Congressional intervention could actually demand that copy and access controls include public interest caveats, proclaimed that

> How companies satisfy consumer expectations is a business decision that should be driven by the dynamics of the marketplace, and should not be legislated or regulated... The role of government, if needed at all, should be limited to enforcing compliance with voluntarily developed functional specifications reflecting consensus among affected interests. If government pursues the imposition of technical mandates, technology and record companies may act to ensure such rules neither prejudice nor ignore their interests.[26]

It is the DMCA that facilitates the adoption of these very business models, that hands over authority to technologies and licenses designed by copyright owners rather than by government; Congress is creating this world and giving it the authority of law, even as they claim they are merely watching it happen. In their sullen myopia, Congress even believes that the Net brings us information that "just a few years ago could have been located and acquired only through the expenditure of considerable time, resources, and money," forgetting that much of this information was and is available in public libraries, a quiet reminder of a moment when the government was more than willing to design public institutions to permit the availability of free information regardless of the interests of publishers.

The legislature and the courts have consistently argued that strengthening copyright is the best and only way to pursue the public interest in cultural expression; the exceptions balanced inside of fair use, long squeezed, have dissolved in the shift from use to access, from infringement to circumvention, from policing to encryption, from law to license. It has become nearly unthinkable that the public interest should be served in any way other than ensuring that authors are also owners. The question of whether any of this is justified under the Constitutional

authority of the copyright doctrine has nearly disappeared inside the skirmishes over code and circumvention. And in statutes like the DMCA, this logic is used not just to tip the copyright scales towards corporate owners, but is powerfully deployed to construct and stabilize particular arrangements of cultural distribution that work hand in hand with these interests, and too often against the public welfare.

References

Barlow, John Perry. 1996. Selling wine without bottles: The economy of mind on the global net. In *High noon on the electronic frontier: Conceptual issues in cyberspace*, ed. Peter Ludlow. Cambridge, MA: MIT Press. 9-34.

Bell, Tom. 1998. Fair use vs. fared use: The impact of automated rights management on copyright's fair use doctrine. *North Carolina Law Review* 76: 557-619.

Benkler, Yochai. 2000. From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. *Federal Communications Law Journal* 52: 561-79.

Benkler, Yochai. 2002. Intellectual property and the organization of information production. *International Review of Law and Economics* 22: 81-107.

Black, Max. 1983. *The prevalence of humbug and other essays*. Ithaca, NY: Cornell University Press.

Bordo, Susan. 1987. *The flight to objectivity: Essays on cartesianism and culture*. Albany, NY: State University of New York Press.

Branscomb, Anne. 1986. Law and culture in the information society. *Information Society* 4(4): 279-311.

Brown, Janelle. 2000. Is the SDMI boycott backfiring? *Salon*, October 3. http://dir.salon.com/tech/feature/2000/10/03/hacksdmi_fallout/index.html (accessed February 5, 2004)

Brown, Janelle. 2000. SDMI cracked! *Salon*, October 12. http://dir.salon.com/tech/log/2000/10/12/sdmi_hacked/index.html (accessed February 5, 2004)

Burk, Dan. 2002. Anti-circumvention misuse. *UCLA Law Review* 50: 1095-1140; available at the Social Science Research Network Electronic Paper Collection, http://ssrn.com/abstract_id=320961 (accessed February 5, 2004)

Burke, Lynn. 2000. Teen hacker's home raided. *Wired News*, January 25. http://www.wired.com/news/business/0,1367,33889,00.html (accessed February 5, 2004)

Chon, Margaret. 2000. Paracopyright and the digital divide: Anti-circumvention provisions and control over digital information. Paper presented at "Copyright's Balance in an Internet World," University of Dayton School of Law Symposium, November 17-18, 2000.

Cisneros, Oscar. 1999. Watershed for digital music. *Wired News*, June 28. http://www.wired.com/news/technology/0,1282,20455,00.html (accessed February 5, 2004)

Cohen, Julie. 1998a. Copyright and the jurisprudence of self-help. *Berkeley Technology Law Journal* 13: 1089-1143.

Cohen, Julie. 1998b. Lochner in cyberspace: The new economic orthodoxy of rights management. *Michigan Law Review* 97:462-563.

Cohen, Julie. 1996. A right to read anonymously: A closer look at copyright management in cyberspace. *Connecticut Law Review* 28: 981-1039.

Daston, Lorraine. 1992. Objectivity and the escape from perspective. *Social Studies of Science* 22:597-618.

Daston, Lorraine and Galison, Peter. 1992. The image of objectivity. *Representations* 40: 81-128.

DVD-cracking teen acquitted. AP in *Wired News*, January 7. http://www.wired.com/news/politics/0,1283,57107,00.html (accessed February 5, 2004)

Dyson, Esther. 1995a. Intellectual property in the net. Electronic Frontier Foundation, August 3. http://www.eff.org/IP/ip_on_the_net.html (accessed February 5, 2004)

Dyson, Esther. 1995b. Intellectual value. *Wired* 3(7): 136-141, 182-184.

Festa, Paul and Junnarkar, Sandeep. 1998. RIAA taking on music downloads. *CNet*, December 15. http://news.com.com/2100-1023_3-219110.html (accessed February 5, 2004)

Gans, Herbert. 1979. *Deciding what's news: A study of CBS Evening News, NBC Nightly News, Newsweek, and Time*, 1st ed. New York: Pantheon Books.

Ginsburg, Jane. 2001. Copyright and control over new technologies of dissemination. *Columbia Law Review* 101: 1613-1647.

Ginsburg, Jane. 2003. From having copies to experiencing works: Development of an access right in U.S. copyright law. In *U.S. intellectual property: Law and policy*, ed. Hugh Hansen. London: Sweet & Maxwell. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493 (accessed February 5, 2004)

Gitlin, Todd. 1980. *The whole world is watching: Mass media in the making and unmaking the new left*. Berkeley: University of California Press.

Halbert, Debora.1999. *Intellectual property in the information age: The politics of expanding ownership rights*. Westport, Conn.: Quorum Press.

Howe, Jeff. 2000. DVD hackers take a hit in NY. *Wired News*, January 21. http://www.wired.com/news/politics/0,1283,33816,00.html (accessed February 5, 2004)

Jackson, Matt. 2001. Using technology to circumvent the law: The DMCA's push to privatize copyright. *Hastings Communications and Entertainment Law Journal* 23: 607-46.

Kaplan, Carl. 2001. Does an anti-piracy plan quash the First Amendment? *New York Times*, April 27. http://www.nytimes.com/2001/04/27/technology/27CYBERLAW.html (accessed February 5, 2004)

Kaplan, Carl. 2000. Is linking illegal? *New York Times*, June 16. http://archive.nytimes.com/library/tech/00/06/cyber/cyberlaw/16law.html (accessed February 5, 2004)

Katz, Jon, 2000. Analysis: The Digital Millennium Copyright Act. posted to Slashdot.com March 6, 2000.

'Landmark' accord on copyrights. AP in *Wired News*, January 14. available at http://www.wired.com/news/politics/0,1283,57205,00.html (accessed February 5, 2004)

Latour, Bruno. 1987. *Science in action: How to follow scientists and engineers through society.* Cambridge, Mass.: Harvard University Press.

Latour, Bruno (a.k.a. Jim Johnson). 1988. Mixing humans and nonhumans together: The sociology of a door-closer. *Social Problems* 35: 298-310.

Law, John. 1987. Technology and heterogeneous engineering: The case of portuguese expansion, In *The social construction of technological systems: New directions in the sociology and history of technology*, eds.,Wiebe Bijker, Thomas Hughes, and Trevor Pinch. Cambridge, MA: MIT Press. 111-134.

Lemley, Mark. 1999. Beyond preemption: The law and policy of intellectual property licensing. *California Law Review* 87: 111, 119-121.

Lemley, Mark. 1995. Intellectual property and shrinkwrap licenses. *Southern California Law Review* 68: 1239-1292.

Lessig, Lawrence. 1999. *Code, and other laws of cyberspace*. New York: Basic Books.

Lessig, Lawrence. 2001. *The future of ideas: The fate of the commons in a connected world*. New York: Random House.

Litman, Jessica. 2001. *Digital copyright: Protecting intellectual property on the internet.* Amherst, N.Y.: Prometheus Books.

Litman, Jessica. 1996. Revising copyright law for the Information age. *Oregon Law Review* 75: 19-46.

Litman, Jessica, 1998. The tale that Article 2B tells. *Berkeley Technology Law Journal* 13: 931-943.

Longino, Helen. 1990. *Science as social knowledge: Values and objectivity in scientific inquiry*. Princeton, NJ: Princeton University Press.

Loren, Lydia Pallas. 1997. Redefining the market failure approach to fair use in an era of copyright permission systems. *Journal of Intellectual Property Law* 5: 1-58.

Lyman, Peter. 1998. The Article 2B debate and the sociology of the information age. *Berkeley Technology Law Journal* 13: 1063-108.

Megill, Allan. ed. 1994. *Rethinking objectivity*. Durham, NC: Duke University Press.

Mosco, Vincent. 1988. Introduction: Information in the pay-per society. In *The political economy of information*, eds. Vincent Mosco and Janet Wasko. Madison, WI: University of Wisconsin Press. 3-26.

National Research Council (U.S.). Committee on Intellectual Property Rights in the Emerging Information Infrastructure, and National Research Council (U.S.). Computer Science and Telecommunications Board. 2000. *The digital dilemma: Intellectual property in the information age*. Washington, D.C.: National Academy Press.

Netanel, Neil. 2000. From the dead sea scrolls to the digital millennium; Recent developments in copyright law. *Texas Intellectual Property Journal* 9: 19-63.

Nimmer, David. 2000. A riff on fair use in the Digital Millennium Copyright Act. *University of Pennsylvania Law Review* 148: 673-742.

Nimmer, David, Brown, Elliot, and Frischling, Gary. 1999. The metamorphosis of contract into expand. *California Law Review* 87: 17-77.

Nunberg, Geoffrey. 1996. Farewell to the information age. In *The future of the book*, ed. Geoffrey Nunberg. Berkeley: University of California Press.

Oakes, Chris. 1999. SDMI on SDMI: A better MP3? *Wired News*, July 8. http://www.wired.com/news/politics/0,1283,20601,00.html (accessed February 5, 2004)

Parloff, Roger. 2001. Copy this! Can 'military' technology beat digital piracy? *Inside.com*, March 12. (no longer available online)

Patrizio, Andy. 1999. DVD piracy: It can be done. *Wired News*, November 1. http://www.wired.com/news/technology/0,1282,32249,00.html (accessed February 5, 2004)

Patrizio, Andy. 1999. Why the DVD hack was a cinch. *Wired News*, November 2. http://www.wired.com/news/technology/0,1282,32263,00.html (accessed February 5, 2004)

Patry, William. 1995. *The fair use privilege in copyright law*, 2nd ed. Washington, D.C.: Bureau of National Affairs.

Ratto, Matt. 2003. *The power of openness: The hybrid work of Linux free/open source kernel developers*. Dissertation, Communication Department, University of California, San Diego.

Reidenberg, Joel. 1998. Lex informatica: The formulation of information policy rules through technology. *Texas Law Review* 76(3): 553-584.

Rose, Mark. 1993. *Authors and owners: The invention of copyright*. Cambridge, MA: Harvard University Press.

Samuelson, Pamela. 1996. The copyright grab. *Wired* 4(1): 134-138, 188, 190-191.

Samuelson, Pamela. 1999a. Intellectual property and contract law for the information age: The impact of Article 2B of the Uniform Commercial Code on the future of information and commerce. *California Law Review* 87: 1-.

Samuelson, Pamela. 1999b. Intellectual property and the digital economy: Why the anti-circumvention regulations need to be revised. *Berkeley Technology Law Journal* 14: 519-66.

Samuelson, Pamela. 1994. Legally speaking: The NII Intellectual Property Report. *Communications of the ACM* 37(12): 21-27.

Samuelson, Pamela. 1997. The U.S. digital agenda at WIPO. *Virginia Journal of International Law* 37: 369-390.

Schudson, Michael. 1978. *Discovering the news: A social history of american newspapers*. New York: Basic Books.

Schudson, Michael. 2000. The domain of journalism studies around the globe. *Journalism* 1(1): 55-59.

Schudson, Michael. 1995. *The power of news*. Cambridge, MA: Harvard University Press.

Stefik, Mark. 1996. Letting loose the light: Igniting commerce in electronic publication. In *Internet dreams: Archetypes, myths, and metaphors*, ed. Mark Stefik, Cambridge, MA: MIT Press. 219-254.

Stefik, Mark. 1997. Shifting the possible: How trusted systems and digital property rights challenge us to rethink digital publishing. *Berkeley Technology Law Journal* 12(1): 137-59.

Sullivan, Jennifer. 1998. Music industry to take on MP3. *Wired News*, December 12. http://www.wired.com/news/business/0,1367,16794,00.html (accessed February 5, 2004)

Sullivan, Jennifer. 1998. RIAA unveils anti-MP3 plan. *Wired News*, December 15. http://www.wired.com/news/culture/0,1284,16853,00.html (accessed February 5, 2004)

Touretzky, David. 2000. "Gallery of CSS descramblers." available: http://www.cs.cmu.edu/~dst/DeCSS/Gallery/ (accessed February 5, 2004)

Wilen, John. 2000. DVD suit defendant pushes legal envelope. *USA Today*, August 25. (no longer available online)

Winner, Langdon. 1980. Do artifacts have politics? *Daedalus* 109(1): 121-36.

Zimmerman, Diane. 2001. Adrift in the Digital Millennium Copyright Act: The sequel. *Dayton Law Review* 26(2): 279-92.

- - - - - - - - - -

A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004 (9th Cir., 2001).

Business Software Alliance, Computer Systems Policy Project, and Recording Industry Association of America. 2003. Technology and record company policy principles. issued January 14, 2003.

Digital Millennium Copyright Act of 1998 (DMCA); Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. 512 and in various sections of Chapter 12 of Title 17 of the U.S.C.).

Information Infrastructure Task Force, 1995. Intellectual property and the national information infrastructure: The report of the working group on intellectual property rights. ("White Paper") Washington, D.C.

Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 435, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984).

Universal City Studios v. Reimerdes, 111 F.Supp.2d 294, 326 [S.D.N.Y. 2000]

NOTES

[1] Current copyright law is a deeply complicated affair whose myriad details cannot be explained here because of space constraints. For those who want a primer on copyright law as it stands, check the U.S. Copyright Office's "Copyright Basics" (http://www.copyright.gov/circs/circ1.html). The current statutes are available at "Legal Information Institute" of Cornell University's Law School (http://www.law.cornell.edu/topics/copyright.html)

[2] See also Ginsburg, 2001; Ginsburg, 2003. For an argument that anticipates this concern well before the rise of the web, see Branscomb, 1986.

[3] See Dyson 1995a and 1995b.

[4] See, for example, Barlow 1996.

[5] There were earlier government discussions of copyright and digital information, some of which reached quite different conclusions than the NII working group; The now defunct Office of Technology Assessment issued two reports, in 1985 and 1994, that focused not on the risk of piracy but on the potential for new forms of authorship ushered in by the Net. The reports speculated that copyright might not even be up to the job of accommodating all of these changes. See the discussion in Halbert, 1999, pp. 28-33**.**

[6] A number of legal scholars have examined the White Paper and its implications for copyright; see Burk, 2002; Cohen 1996; Ginsburg, 2000; Ginsburg, 2003; Katz, 2000; Litman, 1996; Litman, 2001, especially chapters 11 and 12; Netanel 2000; Nimmer, D 2000; Samuelson, 1994, 1996, 1999b; Zimmerman, 2001.

[7] A debate about the implications of this body of law, especially around the controversial Article 2B proposed for the Uniform Commercial Code (UCC), has focused on whether the details of a legally-enforceable contract will be permitted to impose itself over and above the rules of copyright when the commodity in question is information; the courts have fallen on both sides of the issue. For discussions of this, see Lemley, 1995 and 1999; Nimmer, D, 1999; Samuelson, 1999a; and the Fall 1998 special issue of the Berkeley Technology Law Journal (13:3) devoted to the topic, including Cohen, 1998a; Litman, 1998; Lyman, 1998.

[8] For the idea of "paracopyright, see Burk, 2002; Chon, 2000; National Research Council, 2000.

[9] If someone were hoping to duplicate Hollywood DVDs on a massive scale and sell them cheaply, they could easily do so; they would merely have to reproduce the data on the DVD verbatim, press it onto a blank DVD, and sell it. The pirated copy would be encrypted, exactly as the original was; anyone who bought this black market disc could watch it on their licensed DVD player.

[10] A number of creative versions of the tiny application are collected at David Touretzky's "Gallery of CSS Descramblers". See Touretzky, 2000.

[11] For details, see Patrizio, 1999a; Patrizio, 1999b; Burke, 2000; Howe, 2000.

[12] Johansen was indicted in January 2002, and faced up to two years in prison. But in January of 2003, he was acquitted of all charges. See "DVD-Cracking Teen Acquitted", 2003.

[13] The DVD CCA also sued 72 websites in a California court for providing the application; the charge there was trade secret violation: the sites distributing the application knew or should know that the tool was built around stolen property, namely the decryption key lifted from XingDVD. This lawsuit stalled and then waited for a resolution in the NY case.

[14] For more on fair use, see Bell, 1998; Loren, 1997; Nimmer, D, 2000; Patry, 1995.

[15] The DMCA includes an explicit stipulation intended to ensure that its legal domain would not impinge on fair use protections: "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." See the Digital Millennium Copyright Act, 1201[c][1].

[16] The description of such "trusted systems" is drawn primarily from Mark Stefik, who has described them in the context of legal debates and inside the world of digital publishing; but similar plans crop up in press and industry reports, and some elements are beginning to appear in announcements about the two digital music subscription services, Pressplay and MusicNet, since established by the major record companies, and the more recent and somewhat less restrictive system established by Apple. See Stefik, 1996 and 1997.

[17] See Brown, 2000a; Brown, 2000b; Cisneros, 1999; Festa, 1998; Oakes, 1999; Sullivan, 1998a; Sullivan, 1998b.

[18] "CSS Specifications, Version 1.1" available at <http://www.dvdcca.org/css/>; accessed January 18, 2003.

[19] Dan Burk argues that, considering the cases brought under the DMCA, that the law has overwhelmingly been used by one business to shut out upstart competitors; often the plaintiffs are not even the relevant copyright holders, as in *RealNetworks v. Streambox*. See Burk, 2002.

[20] For a discussion of the Linux challenge to traditional arrangements of research and design, see Ratto, 2003.

[21] See also Wilen, 2000; Kaplan, 2001.

[22] In the online version of this article, there was a link to a site offering the DeCSS application; that article has since disappeared in the labyrinth of the New York Times website.
[23] For discussions of the concept of objectivity in journalism, see Schudson, 1978; Schudson, 1995; Schudson, 2000; Gans, 1979; Gitlin, 1980. For discussions of objectivity in the sciences, see Black, 1983; Bordo, 1987; Daston, 1992; Daston and Galison, Longino, 1990; Megill, 1994.
[24] Many thanks to one of this journal's anonymous reviewers for suggesting that this argument be linked to a broader range of "information regulation from the consumer standpoint as well as from the policy standpoint." This issue will be addressed more fully in another essay.
[25] See also Lessig, 1999; Lessig, 2001; Litman, 2001.
[26] Business Software Alliance, Computer Systems Policy Project, and Recording Industry Association of America, "Technology and Record Company Policy Principles"; issued January 14, 2003. See also "'Landmark' Accord on Copyrights", AP, in Wired News, January 14, 2003. http://www.wired.com/news/digiwood/0,1412,57211,00.html