

Survival of Fair Use
Kenneth Berland
November 2004

The advancement of digital technology is beginning to make a world without analog tools possible. No videotape, no paper, no phonographs. A world of all digital content and hardware will further challenge the existing common law and statutory doctrines of copyright infringement and fair use. Courts have previously been capable of including new hardware in the old framework of copyright utilizing the “staple item of commerce” doctrine¹, but the battle has quickly shifted to software and its myriad implications.² This Paper argues that this shift is temporary, and irreconcilable, that the real battle for an effective and just copyright regime in the United States will be fought within the realm of hardware. Further, controls over the specifications for and production of networking and computing hardware will most likely emanate from all three branches of government³—each fighting to alter the balance of copyright.

Before the advent of digital technologies there existed a merger of the form and substance of copyright protected works. A book is at once a work protected by copyright

¹ See *Sony Corp. of Am. v. Universal Studios, Inc.*, 464 U.S. 417, 426 (1984) [hereinafter *Betamax*] (“if deemed sufficient as a basis for liability, would expand the theory beyond precedent and arguably beyond judicial management.”).

² See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154 (9th Cir. 2004); *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002)

and the only practical method of viewing that copy.⁴ A book can, in effect, play itself back. The current frictions in copyright stem from the versatility of the personal computer (PC) and its ability to both present copyrighted works to the user and copy those works. The PC is both a reader and duplicator, as if one could rip a book in two and at once have two copies of the work. The PC simultaneously allows access and duplication.

This Paper will first survey the underpinnings of copyright in both law and policy. Attention will be paid to the delicate balance that copyright seeks to strike and whether or not any period of time can be located that best expressed that balance. It will then explore some of the hardware based technological developments that present the greatest risks to an optimum balance in the law. Finally, it will present some policy prescriptions that could help guide courts in the future when deciding these issues. Namely, that regulators (courts, Congress and arms of the Executive) should be aware of analog's eventual extinction and should mandate that the fair uses available in the analog world be preserved in an all digital one.

³ In fact, the Executive and Judicial branches have already mandated hardware specifications and it is possible that a recent FCC order could be challenged in the courts. *See* Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rulemaking, 18 F.C.C.R. 23,550 (2003) (creating hardware specifications preventing ATSC demodulators from digitally outputting specified copyrighted and flagged content). Further, courts have in the past created rules effecting hardware. *See, e.g.,* Universal City Studios, Inc. v. Sony Corp. of Am., 659 F.2d 963, 977 (1981) (finding "no Congressional intent to create a blanket home use exception to copyright protection and that home videorecording does not constitute fair use" and instructing the district court to "fashion appropriate relief."), *overruled by, Sony*, 464 U.S. 417 (1984).

Background

Most sources, whether they be the Constitution, courts, commentators or outlaws⁵, agree that copyright ultimately seeks to balance the rights of authors and the public. The Framers sought to increase the Nation's creative output by granting authors a limited monopoly to their works.⁶ Comments can be found that recognize this delicate balance even while obviously skewing the balance in one direction or the other – “The sole interest of the United States and the primary object in conferring the monopoly lie in the general benefits derived by the public from the labors of authors.”⁷ or – “[copyright] may also provide greater incentive for American and other authors to create and disseminate their work in the United States.”⁸ Finally, Nimmer informs us that the Framers believed copyright to be a right created *per se* in the public interest:

[T]he authorization to grant to individual authors the limited monopoly of copyright is predicated upon the dual premises that the public benefits from the creative activities of authors, and that the copyright monopoly is a necessary condition to the full realization of such creative activities. Implicit in this rationale is the assumption that in the ab-

⁴ See U.S. Copyright Office, Summary, The Digital Millennium Copyright Act of 1998, available at <http://www.copyright.gov/legislation/dmca.pdf> (Dec. 1998). Distinctions between copy protection and access were, until recently, not applicable. When all works are goods, access is possession. *Id.* (noting, “section 1201 does not prohibit the act of circumventing a technological measure that prevents copying. By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited.”).

⁵ See Anonymous (Beale Screamer), *Mad as Hell about the DMCA*, at <http://www.spinnaker.com/crypt/drm/freeme/Philosophy> (last visited Nov. 15, 2004) (including this statement of purpose inside a source code distribution that disables Digital Rights Management software created by the Microsoft Corporation to “give people the tools to regain the rights that have existed for centuries with respect to copyright, and are now in danger of being taken away in a most uncompromising manner.”).

⁶ See U.S. CONST. art. I, § 8.

⁷ *Fox Film Corp. v. Doyal*, 286 U.S. 123, 127 (1932), *accord*, *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 429 (1984).

⁸ *Eldred v. Ashcroft*, 537 U.S. 186, 188 (2003) (upholding the constitutionality of the Sonny Bono Copyright Term Extension Act, Pub. L. 105-298, 112 Stat. 2,827 (codified in scattered sections of 17 U.S.C. (1998))).

sence of such public benefit, the grant of a copyright monopoly to individuals would be unjustified.⁹

If there ever existed a Golden Age of copyright balance it is certainly not now. Not according to either content creators¹⁰ or advocates for the public interest. Perhaps, however, the time between the 1909 Copyright Act and the 1976 Copyright Act can be cited as a period in which the challenges of today's world did not exist or were extant in a more manageable form. The current set of threats to the system emanate from the inherent qualities of digital media and its various capacities for duplication, namely: 1) no loss of quality, 2) minimal or negligible cost, 3) anonymity and 4) uneducated use.¹¹ To some, these qualities make copyright law a dead letter,¹² to others, the plastic nature of digital realms merely necessitates change in regulatory methods if they are to be successful.¹³

To these previously noted qualities of digital media must be added the relative ease with which computers can be made to do the things they do. Here I am talking about the general diffusion of knowledge regarding the ability to make computers operate—and have them make copies. The qualities of computer code that make them so powerful in

⁹ 1 Nimmer on Copyright, §1.03 (2004).

¹⁰ See Todd Longwell, *Copy machines*, Hollywood Reporter.com, at http://www.hollywoodreporter.com/thr/film/feature_display.jsp?vnu_content_id=1000682867 (October 22, 2004) (noting that if audiences continue to make copies of feature films during public exhibitions and make them available for downloading on the internet, “these products that we call movies will not be made.”).

¹¹ See Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet*, Berkeley Technology Law Journal Online, at <http://www.law.berkeley.edu/journals/btlj/articles/vol112/Schlachter/html/reader.html> (1997).

¹² See id.

¹³ See Lawrence Lessig, *Law of the Horse: What Cyber Law Might Teach*, 113 HARV. L. REV. 501, 524 (1999) (noting “[t]he nature of the Net, we were told, would make copyright controls impossible. Copyright was dead. ... But why exactly? ... Why couldn't we imagine a different code [copyright law], one that better protected intellectual property?”).

the hands of content creators are the same qualities that empower copyright infringers. Computers allow infringers to automate their attacks¹⁴ and use the operating system against the copy protection mechanism employed. The most serious of these tools is open source software.¹⁵ Open source software reveals the internal organization of a computer's operation to all those who can understand the logic of the code in which it is written. By many accounts, it will not be possible to regulate this trend into non-existence.¹⁶

Lawrence Lessig postulates the following about networked digital environments:

[W]hile particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regulability. To see just how, we should think more broadly about the question of regulation. What does it mean to say that someone is 'regulated'? How is that regulation achieved? What are its modalities?¹⁷

He offers four, inclusive, realms in which this regulation can take place: norms, markets, law and "code".¹⁸ Lessig's view is, generally, that code is the law of the internet—that it enforces property rights beyond those sanctioned by law. Code is private law¹⁹. Lessig's view of code is expansive and, for the purposes of this discussion, too

¹⁴ See, e.g., RSA Laboratories, *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4*, RSA Technical Notes and Reports, at <http://www.rsasecurity.com/rsalabs/node.asp?id=2009> (last visited November 15, 2004) (describing how the encryption of 802.11 wireless networks should be considered "broken" and "to plan remedial actions as necessary to mitigate the attendant risks.").

¹⁵ See, generally, Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 BERKELEY TECH. L.J. 759, 767 (1999) (noting, "to the extent that code remains open, it is harder for government to regulate; to the extent it is closed, it is easier.").

¹⁶ A Google search for "pry cold dead hands linux" returns nearly 2,000 results expressing the authors' contention that "[I]f someone wanted to take away the Linux [open software] box on my desk and replace it with something that ran command.com [Windows], they would have to pry it out of my cold dead hands." Steve Borho, *Re: <OT> Linux jobs*, redhat-list, at <http://www.redhat.com/archives/redhat-list/1999-January/msg00907.html> (Jan. 25, 1999).

¹⁷ Lessig, *supra* note 13, at 506.

¹⁸ *Id.* at 507.

¹⁹ See, generally, Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

broad. He fails properly to differentiate software layers from those of hardware. His discussion wrongly lumps together such things as routers (hardware) and web browser design (software). Two examples of how these types of code regulate will help to illuminate this point.

Linksys is a company that builds networking hardware.²⁰ Their design for the wrt54g, an 802.11g wireless access point and router, utilized software licensed under the GNU GPL²¹, and this helped them get their product to market more quickly. To comply with the GPL, Linksys must make their modified source code available.²² This is the tradeoff that Richard Stallman, the author of the GPL, imagined, and it sometimes requires legal effort to enforce the provisions of the license.²³ The point is, Linksys brands its products as personal routers, not as self-contained computer platforms, upon which users can execute programs arbitrarily.²⁴ Linksys chose a particularly weak method of enforcing this desire—software. Their regulation of the wrt54g’s architecture told users not

²⁰ Their web presence is <http://www.linksys.com/>

²¹ GNU is an acronym for “GNU’s Not UNIX.” GPL is the GNU “General Public License.” See Richard Stallman, *The GNU Manifesto*, at <http://www.gnu.org/gnu/manifesto.html> (last visited November 15, 2004) (describing Stallman’s views on the nature of software and freedom); *The GNU General Public License*, Free Software Foundation, at <http://www.gnu.org/copyleft/gpl.html> (last visited Nov. 15, 2004).

²² Linksys, GPL Code Center, at <http://www.linksys.com/support/gpl.asp> (last visited Nov. 15, 2004).

²³ See Jim Rendon, *Linksys routers caught up in open source dispute*, SearchNetworking.com, at http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci932666,00.html (Oct. 20, 2003).

²⁴ See Rob Flickenger, *Is Linksys shirking the GPL? (Maybe not.)*, O’Reilly Networking, at <http://www.oreillynet.com/pub/wlg/3580> (Jul. 29, 2003).

what programs it would run, but *what kinds* of programs, i.e., small, self-contained and *probably* routing applications.²⁵

A second and more successful story involves a company called Microsoft. Microsoft wanted to get into the console gaming business, but didn't know how to make consoles. Their solution was to disguise personal computers as gaming consoles. They called it the Xbox. Microsoft didn't think this would fool anyone unless they were somehow stopped from utilizing the machine as a PC. They realized what Linksys did not and chose to regulate its console through its hardware, its basic input-output system (BIOS). The BIOS "provides low-level communication, operation and configuration to the hardware of a system,"²⁶ it is the glue between the software and the hardware. The BIOS instructions are contained in computer chips that are either difficult or impossible to modify.²⁷ Consequently, users of the Microsoft console need to purchase a modified BIOS (mod-chip) and install it themselves if they wish to use the console as a regular PC.²⁸

These two examples reveal something about the effectiveness of regulation implemented in both software and hardware. Both can be circumvented, but circumvention of the hardware layer requires either more, or replacement, hardware. In the Xbox exam-

²⁵ See OpenWrt Homepage, at <http://www.openwrt.org/> (last visited Nov. 15, 2004) (noting "OpenWrt is a linux distribution for the Linksys WRT54G. ... For users this means the ability to custom tune features, removing unwanted packages to make room for other packages and for developers this means being able to focus on packages without having to test and release an entire firmware.")

²⁶ Wikipedia, the free encyclopedia, *BIOS*, at <http://en.wikipedia.org/wiki/Bios> (last visited Nov. 15, 2004).

²⁷ See id.

ple, the modified hardware is transported in interstate commerce and is more easily regulated. In the Linksys example, software, i.e. digital files, are all that is necessary. This data can be traded in so many different forms that regulation of it is not very effective.²⁹ Software *runs* on hardware. When seeking to limit what can be done in software, one needs to regulate the hardware.³⁰

Hardware Protection Technologies - Older Technologies

Serial Copy Protection

Digital technologies suitable for consumer use, *viz* Audio Compact Discs, were first perfected in the early 1980's and standardized by Phillips and Sony through the publication of the "Red Book"³¹. This was quickly followed by the introduction of digital audio tape (DAT) in 1987³² and the Sony Mini-Disc³³ in 1992. These technologies were the first to give consumers the power to produce "copies of copies ... that would be virtually

²⁸ See, e.g., Xbox Linux Project, *FAQ*, at <http://www.xbox-linux.org/FAQ> (last visited Nov. 15, 2004) (informing that if a user wishes to use the game console as a PC a hardware modification is necessary).

²⁹ For example, the DeCSS software that circumvents the film industry's DVD encryption technique can be accessed throughout the internet. A Google.com search for "DeCSS source download" on November 15, 2004 yielded about 51,900 results.

³⁰ This same kind of weak software regulation can be seen in other products. the TiVo, a digital video recorder, and the mediaMVP, a set-top box for viewing PC based multimedia on a television. See JEFF KEEGAN, *HACKING TiVo: THE EXPANSION, ENHANCEMENT AND DEVELOPMENT STARTER KIT WITH CD-ROM* (CD-ROM ed., 2003); MediaMVP Media Center Homepage, at <http://mvpmmc.sourceforge.net/idx.php?pg=main> (last visited Nov. 15, 2004) ("mvpmmc is a media player for the Hauppauge MediaMVP. It is a total replacement for the Hauppauge software, and can be booted onto the MediaMVP via tftp").

³¹ Hans Fantel, *SOUND; As More Companies Make Compact Disks, Flaws Increase*, N.Y. TIMES, Sept. 25, 1998, at B1 (blaming flaws in compact discs to deviation from the Red Book).

³² Wikipedia, the free encyclopedia, *Digital Audio Tape*, at http://en.wikipedia.org/wiki/Digital_Audio_Tape (last visited Nov. 17, 2004).

³³ Wikipedia, the free encyclopedia, *MiniDisc*, at <http://en.wikipedia.org/wiki/Minidisc> (last visited Nov. 17, 2004).

indistinguishable from the original.”³⁴ The fears in 1992 were the same as today—that these “capabilities could significantly decrease consumer demand for commercially pre-recorded music products because there would be significantly more illegal ‘perfect’ copies in circulation.”³⁵ The clout of the music and consumer electronics industry, combined with their threats to sue any manufacturer who produced a device capable of producing perfect copies, prompted Congress to pass the Audio Home Recording Act of 1992 (AHRA).³⁶

The AHRA subjects any manufacturer or importer to penalties for trafficking in digital audio equipment that does not inherently prohibit the making of serial digital copies, that is, digital copies of copies. An AHRA compliant DAT or Mini-Disc recorder can digitally copy music *once*; all subsequent serial copies will be analog copies and, therefore, slightly degraded. The AHRA has been law for over ten years, has it worked?

No.³⁷ In many ways it is a failure. Firstly, neither the Mini-Disc nor the DAT format ever succeeded in the same way the CD has. Secondly, consumers have learned to use PC’s to make serial digital copies. Thirdly, the AHRA was accompanied by a complex royalty system that inflated the price of DAT and Mini-Disc media³⁸, complicating

³⁴ H.R. REP. 102-873(II), 1992 WL 236754 at *2 (1992) (considering The Audio Home Recording Act of 1992).

³⁵ *Id.*

³⁶ Pub. L. 102-563, 106 Stat. 4,237 (codified in scattered sections of 17 U.S.C. (1992)).

³⁷ See June M. Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 486-87 (2004) (noting that most commentators consider the AHRA a failure).

³⁸ See 17 USC §§ 1003-7.

the analysis of why these media never became as popular as the CD. Do consumers prefer making copies with PC's because the media is cheaper or because the strictures of the AHRA are too burdensome? Lastly, and most importantly, the fear of runaway serial copying from a single digital master has proven to be overblown. Analog and degraded digital copies³⁹ have proven sufficient for consumer tastes. Further, if every digital master is duplicated and degraded across only three or four generations, resulting in tolerable copies, the business models currently employed by most content producers would still need massive restructuring.

Automatic Gain Control (Macrovision)

If you have a DVD player, a VCR and a television lacking video inputs, you may have attempted to watch a DVD “through” your VCR—by attaching the video output from the DVD player to your VCR’s video input and then tuning your television to channel 3 or 4 to watch the program. If you do this with a recent vintage DVD player, you will be sorely disappointed as the output will be somewhat degraded and unpleasing to watch. What you will have discovered is Macrovision, a hardware control mandated by the Digital Millennium Copyright Act (DMCA).⁴⁰

³⁹ Here, I mean MPEG-1/2 Audio Layer 3 or mp3's which are clearly degraded from the original yet threaten to be the format by which most music is listened to.

⁴⁰ Pub. L. 105-304, 112 Stat. 2,860 (codified in scattered sections of 17 U.S.C., specifically 17 U.S.C. § 1201(k) (1998)).

The Macrovision⁴¹ system has two components; a copy-protection signal that is either placed on pre-recorded tapes or inserted into the video signal by a DVD player and an extra video cassette recorder “feature” called automatic gain control (AGC).⁴² AGC was originally included in VCRs to optimize picture quality. The Macrovision signal confuses AGC, causing it to chase the signal up and down in an attempt to equalize it, this causes the picture to grow light and dark, effectively rendering it un-watchable.

One obvious point from the example above is that this hardware control makes even some *legal* activities impermissible. Watching DVDs on an older television is certainly not copyright infringement, yet this technology makes it impossible or, at the least, un-enjoyable.⁴³ Secondly, making decent, viewable, copies of DVDs and pre-recorded tapes is also burdened by Macrovision, upsetting the fair use balance in the direction of copyright holders.

Macrovision was easily implemented and AGC was actually present in most VCRs before the DMCA mandated that it be. Studios were already using Macrovision to

⁴¹ Although Macrovision is the *nom de guerre* for this system, it is not the only one nor is it the only acceptable one:

Despite this general ‘no mandate’ rule, section 1201(k) does mandate an affirmative response for one particular type of technology: within 18 months of enactment, all analog videocassette recorders must be designed to conform to certain defined technologies, commonly known as Macrovision, currently in use for preventing unauthorized copying of analog videocassettes and certain analog signals. The provision prohibits rightholders from applying these specified technologies to free television and basic and extended basic tier cable broadcasts.

U.S. Copyright Office, *supra* note 4.

⁴² See Besek, *supra* note 37 at 457; 17 U.S.C. § 1201(k) (2003); Antti Paarlahti, *Macrovision FAQ*, § 3.1, at http://www.repairfaq.org/filipg/LINK/F_MacroVision1.html (last visited Nov. 15, 2004).

protect their pre-recorded content before all VCRs had the circuitry that guaranteed it would work. Macrovision helps us to define the amount of signal degradation that consumers are willing to accept in analog copies of digital works. Anecdotally, it appears to be a success, while the burden to those seeking fair-use is minimal since Macrovision can be disabled in a variety of ways including the purchase of an inexpensive signal filter.⁴⁴

Newer Technologies

Broadcast Flag

As part of a ten year effort to transform television into a digitally broadcast medium⁴⁵, the Federal Communications Commission (FCC) and major broadcasters have recently agreed upon a hardware based scheme to prevent the digital reproduction of broadcast digital content.⁴⁶ This has come to be known as the Broadcast Flag.⁴⁷ The Flag is extremely similar to the Serial Copy Protection scheme set forth above. The flag is a digital marker honored by hardware that presents a would-be infringer with an extra hurdle. This hurdle could variously be the inability to transfer, record, copy or share pro-

⁴³ Like the anti-circumvention provisions of the DMCA, 17 U.S.C. § 1201, 17 U.S.C. § 1201(k) overreaches. The court noted so in *Skylink*, and so did some commentators, that fair use becomes illegal. *See infra*, note 57.

⁴⁴ *See, e.g.* the Sima "Copy This" stabilizer, \$64, at <http://www.bgsales.com/video-stabilizer/sima-copythis.html> (last visited Nov. 15, 2004).

⁴⁵ *See generally*, Advanced Television Systems and their Impact Upon the Existing Television Broadcast Service, Fourth Further Notice of Proposed Rule Making and Third Notice of Inquiry, 10 F.C.C.R. 10,540 (1995).

⁴⁶ *See* Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rule-making, 18 F.C.C.R. 23,550 (2003); 47 C.F.R. § 73.9008 (2004).

⁴⁷ Redistribution Control Descriptor set forth in ATSC Standard A/65B or "ATSC flag" or "flag" also works.

tected content. For example a TiVo or ReplayTV⁴⁸ user would be unable to transfer protected content to a device outside of her home network, e.g., to a friend.

In theory, the Flag provides levels of protection similar to that of Macrovision technologies. However, in reality, the balance is shifted even further toward the side of copyright holders. Where Macrovision merely limits fair-users to degraded copies, the Flag and its associated technologies threaten to deny fair use altogether. The Flag could deny access to news and other programming that is already in the public domain, removing altogether the notion of fair use in the all-digital realm.⁴⁹ Although not all news can be re-broadcast under fair use,⁵⁰ FCC Commissioners worried aloud about the possible abuses of the Broadcast Flag:

I understand the arguments of those who caution that precluding the flag for news and information could entail some difficult and sensitive decisions about what constitutes news and public information and what does not. Even if we are confronted with some difficult decisions, I would rather attempt the difficult than deny the free flow of news and information the widest possible dissemination.⁵¹

The Broadcast Flag, in its current administrative law incarnation, also presents several thorny issues that were noted by the Commission but, perhaps negligently, not considered a bar to implementation. First, does the FCC have the power to mandate a

⁴⁸ These are both digital video recorders utilizing a hard disk and electronic programming guide.

⁴⁹ *See supra*, note 46 at 23,616 (“I dissent in part, first, because the Commission does not preclude the use of the flag for news or for content that is already in the public domain.”) (Statement of Commissioner Michael J. Copps Approving in Part, Dissenting in Part).

⁵⁰ *See Harper & Row Publishers, Inc. v. Nation Ent’ps.*, 471 U.S. 539 (1985); *Cf. Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977).

⁵¹ *See supra*, note 46 at 23,617; *Accord, id.* at 23,621 (Statement of Commissioner Jonathan S. Adelstein Approving in Part, Dissenting in Part) (noting the order “could restrict the free flow of news or public affairs programming”).

broad requirement on all equipment capable of demodulating digital television signals?⁵² Previous restrictions have been implemented by Congressional legislation and have the power law. It is unclear whether the power of the FCC, which certainly includes the power to regulate broadcasters, extends to receivers, which pose only an indirect threat to the ability of the Commission to fulfill its duties.⁵³ Secondly, whether or not analog copies made in violation of the broadcast flag would violate the DMCA is an unsettled issue and one the Commissioners sought to avoid.⁵⁴ Obviously, the Broadcast Flag presents some dangerous challenges to fair use.

More recently, the FCC began approving various hardware implementations of the broadcast flag specification.⁵⁵ More than ten schemes were approved that, in their sophis-

⁵² Commissioner Abernathy questioned this power in her Separate Statement:

Finally, I have previously expressed concerns about whether we have jurisdiction to adopt a broadcast flag solution, or whether this is an issue best left for Congress. As a general rule, the Commission should be wary of adopting significant new regulations where Congress has not spoken. On balance, though, I believe that given the broad congressional direction to promote the transition to digital broadcasting, a critical part of that obligation involves protection of content that is transmitted via free over-the-air broadcasting. I am hopeful that any court review of this decision can occur before the effective date of our rules.

Id. at 23,614 (Separate Statement of Commissioner Kathleen Q. Abernathy).

⁵³ Also relevant, perhaps, is the explicit and repeated use of the word “transmission” in Title I of the Communications Act. 47 U.S.C. § 152(a) (2004).

⁵⁴ *See supra*, note 46 at 23,620 (Statement of Commissioner Jonathan S. Adelstein Approving in Part, Dissenting in Part) (noting, “Given the possibility that the Digital Millennium Copyright Act might apply, content protection technologies have the potential to override lawful uses of digital content.”).

⁵⁵ *See* Digital Output Protection Technology and Recording Method Certifications, Order, 19 F.C.C.R. 15,876 (2004).

tication and security, make prior protection methods look quaint in comparison.⁵⁶ Although there exists some promising case law on point, limiting the ability of technology to protect intellectual property through the DMCA and contract, if the current crop of protections schemes become the norm, it might make fair use or other judicially allowed copyright doctrine so difficult to implement that copyright does, indeed, become an area governed solely by contract.⁵⁷

Digital Rights Management (DRM) and Trusted Computing

DRM and trusted computing are the next generation of digital content protection. DRM seeks to control both access and duplication of content through contractual relations and technology. It allows copyright holders to monetize their content through sub-

⁵⁶ A typical Broadcast Flag scheme is “Digital Transmission Content Protection” (DTCP) created by Hitachi, Ltd., Intel Corporation, Matsushita Electrical Industrial, Co., Ltd., Sony Corporation and Toshiba Corporation. “DTCP uses authentication, key exchange techniques, and content encryption as part of its protection system. Under this system, a connected device must first verify through the exchange of keys that another connected device is ‘authentic,’ meaning also DTCP-compliant, before sharing protected information.” *Id.* (footnote omitted).

⁵⁷ Although Lessig warned of copyright being conducted through contract in the future, *see* Lessig *supra* note 13 at 529 (noting that trusted systems are private law) two recent decisions have reinforced fair use and dealt a blow to the use of the DMCA in creating new rights for copyright holders. In *Chamberlain Grp. v. Skylink Techs.*, 381 F.3d 1178 (Fed. Cir. 2004), the court held:

The anticircumvention provisions convey no additional property rights in and of themselves; they simply provide property owners with new ways to secure their property. Like all property owners taking legitimate steps to protect their property, however, copyright owners relying on the anticircumvention provisions remain bound by all other relevant bodies of law.

Also in *Lexmark Int’l Inc., Static Control Components, Inc.*, --- F.3d ----, No. 03-5400 (6th Cir., Oct. 26, 2004), the court vindicated the fair use rights of a replacement parts manufacturer who duplicated code to facilitate the creation of replacement printer ink cartridges. The court appears to deny copyright to those schemes that do not eventually “create any protected expression”. *Id.* at 17. Only code that eventually results in a “video or audio manifestation generated by the code’s execution” is eligible for copyright protection. *Id.* Yet, ominously, the court suggests that Lexmark’s lack of encryption and Static Control’s easy access to the code might be a controlling factor. *Id.*

scription, limited time purchases, video on demand and pay-per-view revenue models.⁵⁸ Any digital media can be protected in this fashion. Even text can be protected through the disabling of copy, paste and save functions.⁵⁹

Of course, these DRM schemes depend upon the security of the underlying hardware. If the computer user can successfully monitor or emulate the internal functioning of the computer, the unprotected digital content can be copied from memory or accessed in an intermediate form—attacks the original programmer had not anticipated.⁶⁰ The problem is, with “low-level access, end users can attack the digital file itself, intercept digital information as a program executes (through an emulator or debugger), or access the end result (through screen or audio capture programs).”⁶¹

Trusted Computing, in theory, solves this problem. The concept seeks to transport software-like control to the hardware based internals of the computer, creating walls between the user and key elements of the hardware. It necessitates physically sealed hard-

⁵⁸ See Microsoft, *Windows Media Digital Rights Management*, at <http://www.microsoft.com/windows/windowsmedia/drm/default.aspx> noting (last visited Nov. 15, 2004) (“Scenarios The following scenarios demonstrate just a few of the innovative business models and acquisition scenarios that Windows Media DRM can enable. Direct License Acquisition, Indirect License Acquisition, Subscription Services, Purchase and Download Single Tracks, Rental Services, Video-on-Demand and Pay-Per-View”).

⁵⁹ See Peter Sayer, *Government, Microsoft haggle over documentation*, InfoWorld, at [http://www.infoworld.com/article/04/10/11/HNmshaggle_1.html](http://www.infoworld.com/article/04/10/11/HNmshaggle_1.html?source=rss&url=http://www.infoworld.com/article/04/10/11/HNmshaggle_1.html) (Oct. 11, 2004) (“...Microsoft, asked to open up and document the interfaces to its communication protocols for licensees, has chosen to issue the documentation in a rights-protected file format called MHT, readable only with its own Web browser, Internet Explorer. This means licensees can neither annotate nor effectively search the information, according to the plaintiffs.”).

⁶⁰ See, e.g. Paul Thurrott, *Hacker Breaks DRM, Microsoft Looks Into Legal Action*, Windows IT Pro, at <http://www.winnetmag.com/Article/ArticleID/23000/23000.html> (Oct. 23, 2001); Anonymous, *supra* note 5.

⁶¹ Ryan Roemer, *Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 2003 UCLA J. OF L. & TECH. 8 (2003). Note that screen capture and audio capture are, generally, digital copies, so long as the data is obtained before it is processed by a digital to analog converter.

ware, immune to hacks conducted with soldering irons and jumper wire as well as traditional software hacking. Trusted Computing removes a portion of the computer from the user's control. It has many people worried.⁶² However, because the Napster model requires only a single, unprotected, copy of a work to become available through the network, query whether all computing must be subject to licensing restrictions, in addition to access to component parts and the microprocessors that make computing possible; lest one user construct a machine unrestricted by trusted computing regimes with which to make illegal copies.⁶³

Conclusion & Policy prescription

Preservation of Analog Holes

As digital methods displace even more of the analog world it becomes important that courts and regulators preserve the ability of the public to make fair use of copyrighted material. In the trusted computing and DRM environment outlined above, consumers might try to record news or share a political program only to be thwarted by the underly-

⁶² See Richard Stallman, *Can You Trust Your Computer?* in FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN (2002), available at <http://www.gnu.org/philosophy/can-you-trust.html>:

The technical idea underlying treacherous [trusted] computing is that the computer includes a digital encryption and signature device, and the keys are kept secret from you. Proprietary programs will use this device to control which other programs you can run, which documents or data you can access, and what programs you can pass them to. These programs will continually download new authorization rules through the Internet, and impose those rules automatically on your work. If you don't allow your computer to obtain the new rules periodically from the Internet, some capabilities will automatically cease to function.

Id.

⁶³ See *supra*, note 61.

ing technology. Few consumers would be aware of their rights when their video recorder informs them, perhaps through a pop-up, that “You are not allowed to perform this action.” When awareness of a right wanes, so does its practice. Rights atrophy without exercise. Courts and regulators should press devices makers to enable analog duplication where digital reproduction has been disabled.

In the Macrovision example, many fair users would be hard-pressed to locate the cause of their poorly recorded copy. Equipment manufacturers should be pressured to inform the consumer about the copy protection features of the devices they sell. Disclosure through the interface itself or in printed material packaged with the device would enable consumers and the public more fully to understand and exercise their rights.

Circumvention Devices

Technology to combat illegal copying has much more momentum than does technology to enable fair use. Companies are currently experimenting with a system that blocks video camcorders from recording projected feature films.⁶⁴ Technology also exists that allows for recording devices to recognize the title and artist of the song they have recorded or are recording.⁶⁵ With a small expansion of wireless networks it is not difficult to imagine an environment where all recording devices contact copyright holders, e.g. the Motion Picture Association of America or the Recording Industry Association of Amer-

⁶⁴ See Sarah McBride, *The Hunt For Movie Pirates*, WALL ST. J., Apr. 12, 2004, at B1.

ica, to identify the material they are about to record and obtain permission. In this possible world, audio recorders refuse to duplicate copyrighted songs and camcorders refuse to record from television screens.

In the face of this threat, courts and regulators should be vigilant in providing that circumvention devices that enable fair use remain available. This should involve preserving the holding of the *Betamax* case and promoting the idea of substantial, non-infringing uses. Courts and regulators should also seek to tailor technologically based copyright protection schemes to ensure that they merely make copying more difficult, not impossible. A user should be aware of her actions—not merely sold tools that are unable to perform them. Courts should be aware that if the copyright holders have their way, e.g. if DeCSS were never made available, no critic would today be able to grab a DVD screenshot to comment on the work.

⁶⁵ See Relatable, *TRM: The Universal Barcode for Music and Media from Relatable*, at <http://www.relatable.com/tech/trm.html> (last visited Nov. 8, 2004) (describing that TRM “recognizes the song ... because it interprets [sic] the kind of audio information that humans actually hear.”).