VIGILANTES V. PIRATES

THE RUMBLE OVER PEER-TO-PEER TECHNOLOGY HITS THE HOUSE FLOOR*

As new file transfer technologies rise in the wake of Napster's demise, Congress considers a bill that would enable copyright owners to use self-help measures to impair piracy of their works over online peer-to-peer networks. This iBrief evaluates the need for the proposed act and its implications for privacy and fair use.

Overview

On July 25, 2002, the Berman Bill[1] was tossed into the congressional pool, but despite its rather meteoric implications for privacy, the bill caught little public attention outside the circling policy-hawks of the tech community. Hailed by some as a congressional call for a "posse of copyright vigilantes,"[2] the bi-partisan "Hollywood Hacking Bill"[3] erects a safe harbor for copyright owners to engage in self-enforcement of their copyrights by disabling, interfering with, or impairing the distribution of copyrighted materials via popular peer-to-peer (P2P) transfer systems like Music City, KaZaA, and other Napster progeny.[4]

Congressman Howard L. Berman, the lead sponsor of the bill, was the immediate subject of press scrutiny. His 26th district of California consisting of North Hollywood, San Fernando, and other prime areas in Los Angeles, is home to giants of the entertainment industry who have substantially funded his re-election war chest.[5] While some critics are resigned to the fact that

---

* Special thanks to Chris McGettigan and David Barkai for their helpful tutorials in P2P networks.

[1] *See* H.R. 5211, 107th Cong. (2002), *available at* http://thomas.loc.gov/cgi-bin/query/D?c107:2:./temp/~c107UFnOAA (July 25, 2002). The bill has sometimes been more formally dubbed the Peer to Peer Privacy Prevention Act.

[2] Statement by Ellen Stroud, representative of Streamcast Networks, the company that created the Morpheus P2P file sharing technology and operates MusicCity.com. *See* Rebecca Gray, *Berman's Bill Faces Opposition Online*, AVN ONLINE, July, 10, 2002, *at* http://www.avnonline.com/issues/200207/newsarchive/071002_lead.shtml.

[3] Declan McCullagh, *Hollywood Hacking Bill Hits House,* NEWS.COM,July 25, 2002, *at* http://news.com.com/2100-1023-946316.html.

[4] *See* H.R. 5211 at § 514(a).

[5] Congressman Berman's top five contributors are Walt Disney Co., AOL Time Warner, Vivendi Universal, Viacom Inc., and News Corp. *See* opensecrets.org, *Howard L. Berman (D-CA): Top Contributors*, *at*

Berman is indeed representing the interests of *his* district, privacy aficionados are repulsed by the thought of Congress permitting anyone, let alone Hollywood, to interfere with their file sharing pastime. They decry the Berman Bill as "an invitation to online-lawlessness" and "a declaration of cyber warfare on consumers."[6] In fact, there is nothing conceptually wrong with purpose of the Berman Bill: copyright owners should be permitted to protect their legally granted interests by technological means so long as the methods employed do not cause harm. This principle of self-help is well established in our legal tradition in such doctrines as recapture of chattel, repossession, and foreclosure.

Yet, Congress is perhaps too often convinced that the road to re-election is paved with good intentions. Such is the flawed reality of the Berman Bill. While the bill does effectively legitimize the employment of certain methods to disrupt illegal file swapping and limit nonconsensual damage to files and data, if enacted without amendment, the act will throw open the door for a numerous defensible privacy intrusions that will greatly increase the burden of personal computer security and otherwise seriously threaten what's left of the personal in PC.

Problems Posed by P2P Technology

File transfer technology over the Internet may be roughly divided into three categories: client/server communications, hybrid P2P computing, and pure P2P computing.[7] The client/server model exists under the most traditional network technology. Individual computers communicate with central servers that control, coordinate and manage client requests.[8] In such cases, communication between individual computers is indirect and the server operates as a central conduit for information transfers.[9]

Hybrid P2P computing is an initial movement away from the client/server model towards decentralization.[10] Under hybrid technology, a central server may perform some but not all of the

---

http://www.opensecrets.org/politicians/contrib.asp?CID=N00008094&cycle=2002 (last visited Sept. 9, 2002).

[6] Press Release, Streamcast Networks, Streamcast Networks Opposes Congressman Howard L. Berman's Proposal Calling for Posse of Copyright Vigilantes (July 25, 2002), *at* www.streamcastnetworks.com/6_25_02.html.

[7] For an excellent review of P2P technology *see, e.g.,* David Barkai, *Initiatives and Technologies: An Introduction to Peer-to-Peer Computing*, Intel Developer Services, Feb. 2001, *at* http://cedar.intel.com/cgi-bin/ids.dll/content/content.jsp?cntKey=Generic+Editorial%3a%3ap2p_barkai&cntType=IDS_EDITORIAL&catCode=BYM.

[8] *Id.*

[9] *Id.*

[10] *Id.*

functions required under the client/server model.[11] The most notable example of hybrid P2P computing is Napster.[12] Under the technology employed in Napster, a person seeking a particular song would have to initially operate through a centralized Napster server where a directory of all the available files was stored.[13] As soon as the file was located in the directory, the individual computers could initiate a file transfer without additional server assistance.[14] Thus, some functions that were originally performed by the centralized server could now be performed by the individual "peer" computers.

Pure P2P computing is at the farthest end of the spectrum of decentralized communications. In this model, each computer functions independent of a centralized server.[15] The information transfers are autonomous and exercise substantial control over the services they utilize.[16] Pure P2P computing is currently in limited use and is most notably associated with the Freenet Project, a transfer system first proposed in a research paper developed by Ian Clarke at the University of Edinburgh.[17] The Freenet system is designed to permit efficient use of bandwidth, free personal Internet publishing, and most notably, uncensorable dissemination of controversial information.[18]

The practical effects of decentralized P2P file swapping are easy to foresee. A legal attack on one computer is but an attack on one of millions of peer computers. Thus, while the recording industry had a newsworthy victory in enjoining the centralized music giant Napster, filing suit against the millions of users of decentralized P2P technology is entirely impracticable. In a demonstration of free-market entry that would raise a toothy grin from Milton Friedman himself, shortly after Napster's timely demise, the new Morpheus system which further decentralized P2P systems came to popularity on alternative file swapping networks.[19] Morpheus features a "supernode" that automatically moves any index on any server interrupted or disabled,

---

[11] *Id.*
[12] *Id.*
[13] *See* Barkai, *supra* note 7.
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *See* Ian Clarke, A Distributed Decentralized Information Storage and Retrieval System (1999) (research report, University of Edinburgh), *available at* http://freenetproject.org/freenet.pdf.
[18] *See* The Free Network Project, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/WhatIs (last visited Sept. 13, 2002).
[19] Farhad Manjoo, *Sour Notes*, SALON.COM, July 30, 2002, *at* www.salon.com/tech/feature/2002/07/30/file_trading/print.html.

for example, by court injunction, to another location on the web.[20] Therefore, as P2P technology is refined, it has the capability to render copyright owners legally helpless.

To the extent current decentralization technology falls short in preserving the free distribution of copyrighted materials, by nature the Internet has other means with which to frustrate copyright holders and their traditional enforcement mechanisms. For example, though the Federal Wire Act[21] prohibits the operation of Internet sportsbook sites,[22] entering an elusive domain name like www.gambling.com will raise the homepage of the Online Gambling Directory and Casino Guide, providing Americans with links to hundreds of sportsbook sites run offshore from unregulated Caribbean retreats.[23] Information once restricted from public access by statute has also been moved offshore. For instance, at www.publicdata.com.ai, based in Anguilla, you can purchase select voter rolls and criminal files otherwise subject to strict confidentiality limitations.[24]

Regulatory arbitrage, the movement between jurisdictions to take advantage of favorable regulatory systems, is rather troubling and very real in the Internet age, with some traditional systems of regulation being undermined entirely by the free flow of data across national boundaries.[25] However, lawmakers remain unconvinced of the need to upgrade traditional concepts of jurisdiction to rein in the web, rather choosing to resign their dilemmas to imperfections in the resolution of conflict of laws, a greater need for private ordering and other problems that will be mitigated by time and experience with Internet technologies.[26] However, wealthy campaign donors in Congressman Berman's district like the membership of the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) are not so willing to stand idle while their revenues stream untapped through their own

---

[20] The supernode system does, however, contain a degree of centralization that has proved troublesome for Morpheus. Streamcast, the creators of Morpheus, were forced to incorporate a more decentralized system to thwart legal attack. *See Id.*; Brad King, *Morpheus' File Trading Fiasco,* WIRED NEWS, Feb. 28, 2002, *at* http://www.wired.com/news/politics/0,1283,50725,00.html.

[21] 18 U.S.C. § 1084(a), (b) (2000).

[22] *In re* MasterCard Int'l Inc., 132 F.Supp. 2d 468, 480 (E.D. La. 2001).

[23] For links to 3,931 sportsbook related sites *see* The Online Gambling Directory and Casino Guide, *at* http://www.gambling.com/directory/index.cfm (last visited Sept. 13, 2002).

[24] *See* Stewart Taggart, *Fast, Cheap, and Out of Control,* THE INDUSTRY STANDARD, Aug. 14, 2000, *at* http://www.thestandard.com/article/0,1902,17365,00.html?body_page=2.

[25] *See*, e.g., David R. Johnson and David Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[26] For a review of this argument *see, e.g.,* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

cable modems.[27] Since they can no longer enforce their copyrights in America's courtrooms, they have lobbied intensely for the right to take to the streets to reclaim their intangibles.

The Berman Bill

The political response is the Berman Bill, legislation introduced in the house in late July to erect a safe harbor for self-enforcement actions by copyright owners. The act specifically provides that any copyright owner may impair the distribution or reproduction of their copyrighted work on a public P2P file sharing network so long as the copyright owner does not, without consent, impair the integrity of the data residing on the file sharer's computer.[28] The safe harbor is also lost should the copyright owner (i) unreasonably impair the accessibility to the P2P network of any file in which the copyright owner does not have a copyright interest under 17 U.S.C. §106; (ii) cause economic loss to any other P2P file trader; (iii) cause economic loss in excess of $50.00 per impairment; (iv) fail to notify the Department of Justice seven days in advance of the technology employed to impair distribution or reproduction; or (v) fail to notify the file trader, upon request, the reason for an impairment, the impairer's contact information, and the file trader's right of action under the bill.[29] The bill goes on to set out a non-exclusive cause of action for damages, including attorney's fees, to be adjudged against a copyright owner who fails to qualify for the safe harbor protections.[30]

Self-enforcement mechanisms like the Berman Bill are not an unpopular response to traditional legal violations presented in the context of new technology. For example, the Uniform Computer Information Transactions Act ("UCITA"), though sluggish in the adoption and ratification process, provides for the prevention of use and retaking of software after an agreed or material breach of an end-user or licensing agreement.[31] And why should self-enforcement be so objectionable? After all, as discussed *supra*, the Internet suffers from a chronic want of effective enforcement mechanisms and P2P computing has been widely popularized solely because it enables users to thwart the legal interests of copyright holders. Indeed, within the context of music file sharing, it is often more cumbersome to increase decentralization by assigning server

---

[27] *See* opensecrets.org, *supra* note 5.
[28] H.R. 5211 at § 514(a).
[29] *Id.* at § 514(b), (c).
[30] *Id* at § 514(d), (f).
[31] Unif. Computer Info. Transactions Act § 815(a), (b) (2001), *available at* http://www.law.upenn.edu/bll/ulc/ucita/citam99.htm.

functions to peer computers than a central server.[32] Thus P2P technologies are being redesigned, even more inefficiently, to circumvent legal interests.[33]

P2P technology, however, should not be banned because (as Congressman Berman, "a big fan of P2P networks and technology behind them"[34] recognizes) P2P computing possesses significant legitimate applications.[35] Additionally, the principle of technological neutrality, that no technology should gain regulatory preference, has provided the foundation for the expansion of the Internet and its derivative innovations and should be strictly maintained.[36] The Berman safe harbor in no way limits the expansion of P2P computing; rather, it legally enables technology to restrict the types of file transfers that may take place to the benefit of copyright owners.

While the Berman Bill does not specifically identify the anti-piracy technologies that it seeks to legitimize, some of the techniques that could be used are interdiction, redirection, and spoofing.[37] Interdiction, more commonly known as a denial of service ("DoS") attack, occurs when a large volume of file requests are directed at a single peer machine, causing it to slow and effectively arresting the downloading process.[38] Redirection consists of index pollution; meaning that the index of files maintained on a P2P network is contaminated such that requests for copyrighted materials will return undesired, bogus files.[39] Lastly, spoofing involves attaching nodes that contain corrupted content to a P2P network which will slow the downloading process by denying the pirate resources for other downloads.[40] Of these three techniques, only the DoS attacks threaten to seriously impair the distribution of legitimate files because the process floods a particular peer computer with false requests impairing access to other, possibly legitimate, files. Redirection will only frustrate the distribution of legitimate files that look like copyrighted materials, for example, because they have a similar filename. None of these techniques, however, require copyright owners to hack into personal files on a pirate's PC.

---

[32] Interview with Christopher McGettigan, Associate, Almeda County Computer Resource Center, in Virginia Beach, Va. (Aug. 18, 2002).
[33] *See* Manjoo, *supra* note 19.
[34] Press Release, Congressman Howard L. Berman, Berman Introduces Legislation to Foil Peer to Peer Piracy (July 25, 2002), *at* http://www.house.gov/berman/pr072502.htm.
[35] *See, e.g.,* Barkai, *supra* note 7. For a legal argument that it is not the judiciary's practice to ban technologies that have substantial noninfringing uses *see* Expert Report of Professor Lawrence Lessig at 12-13, A&M Records, Inc. v. Napster Inc., 1114 F.Supp. 2d 896 (N.D. Cal. 2000) (No. C 99-5183), *available at* http://cyberlaw.stanford.edu/lessig/content/testimony/nap/napd3.doc.html (last visited Sept. 9, 2002).
[36] *See* Expert Report of Professor Lawrence Lessig at 6.
[37] *See* Gray, *supra* note 2.
[38] *Id.*
[39] *Id.*

If an act of Congress, technologically neutral, can mitigate copyright infringement without significant harm in the form of impairing non-infringing data transfers or privacy intrusions, then what could possibly be the problem? That many tech-savvy privacy aficionados have a general objection to the doctrine of copyright itself is an argument best saved for debate over the passage of the Copyright Act of 1909, in 1909, a time when the issue was seriously considered before Congress.

Nevertheless, the act does fail to prevent significant harm to P2P file traders in a number of ways, foremost by concealing privacy intrusions completely unrelated to the protection of copyright interests. Congressman Berman has assured Americans that the bill does not allow copyright owners to lawfully hack or crack into the personal files of P2P users,[41] and in fact, it does not. But in effect, the act has greatly increased the burden of individuals to prevent the access to and the copying of personal files by crackers from being a common, defensible occurrence. Because the bill fails to specify exactly which techniques may be used to impair piracy, any technology registered with the DOJ (like redirection) that does not alter or impair the integrity of data residing on the file trader's computer is permissible. Importantly, cracking (gaining access to files) alone does not alter or impair the integrity of anything residing on a computer and therefore meets the proposed bill's qualifications as a technique entitled to safe harbor protections. One cannot take any confidence that during the registration process the DOJ will prevent the use of more invasive but statutorily compliant methods (like cracking), because such agency discretion is not provided for in the bill.[42]

Of course, the Berman Bill does not protect cracking to gain access to personal files.[43] Such an act is likely a violation of the Computer Fraud Act[44] and in many other ways qualifies as tortious conduct. Yet, the proposed bill threatens to alter the balance of the acceptability of privacy intrusions. Individuals view the privacy of their PC in the same manner they view the privacy of their home. Technological intrusions by government are met with the greatest skepticism and seen as the equivalent of wire-tapping.[45] An intrusion by non-government

---

[40] *Id.*

[41] Howard L. Berman, *Just Desserts for Scofflaws*, NEWS.COM, July 9, 2002, *at* http://news.com.com/2010-1078-942325.html.

[42] All the bill requires is seven days notification. H.R. 5211, § 514(c). Because there is no discretionary power vested in the DOJ they take on a completely administrative role until abuses are apparent. *See Id.* at § 514(e).

[43] The bill nowhere provides that gaining access to personal files is permitted, it only protects the impairment of the reproduction and distribution of files over a P2P network. *See Id.* at § 514(a).

[44] 18 U.S.C. § 1030(a)(2)(c), (4) (2000).

[45] *See, e.g.,* Heather Jacobson & Rebecca Green, *Computer Crimes,* 39 AM. CRIM. L. REV. 273, 312-314 (2002).

personnel is simply incomprehensible to most and any cracking into a personal system is blanketed as wrong. To legally bless some technological invasions implies, contrary to the current standard, that persons have a right under certain circumstances to essentially be inside another's computer.

The effects play out clearly enough in litigation. For example, suppose a young and promising professor keeps his work on his laptop. Two years later a pharmaceutical giant patents a product that simply could not have been created without bits of information obtained in the professor's personal notes. The professor sues for computer fraud and conversion amongst other causes and appropriately submits his complaint to the court. The pharmaceutical giant denies that it obtained the information by cracking the professor's computer, and alleges that it has been developing such technologies for years and has plenty of evidence to that effect. The only evidence the professor can submit to the court with regards to the accessibility of his developing creation is that some crackers dug around in the professor's computer for a few moments because he uses P2P network software. All the crackers claim that they have been authorized by copyright owners to enforce §106 interests and that their techniques are authorized by the DOJ. Any link between the crackers and the pharmaceutical giant is too tenuous to be substantiated. Unfortunately, our professor may very well lose the case. Since the crackers had a reason to be inside the professor's computer, it is incredibly difficult for the legal system to assign rights, obligations, and liability. Previously, cracking was unquestionably a wrong, now it is a matter of evidence.

In moderation, we hope the professor is neurotic enough to own at least an off-the-shelf firewall system to protect his works, much as we hope to remember to lock the doors at night. Yet, it may be asking too much to convince the American public that there is a reason for someone to be in their unlit house at 2 a.m., or, as this bill permits, legally digging inside their PC. If the Berman Bill is enacted in its current form, P2P file traders will have to trust in the ability of corporations to establish and enforce internal policies with regard to limiting cracking technology, and these, most likely, will fail. Any legal action to follow will be disrupted by the inability of file traders to even generally establish what actions the crackers took while inside their PC where previously, the crackers had no right to be there at all.

An equally troubling proposition of the Berman Bill is that it will allow a copyright owner to obtain a P2P file trader's consent to impair the integrity of any computer data residing on the file trader's computer.[46] Microsoft's XP End-User License Agreement specifies:

---

[46] H.R. 5211 at §514(a).

> Content providers are using the digital rights management technology contained in this product to protect the integrity of their content ("Secure Content") so that their intellectual property, including copyright, in such content is not misappropriated… if you elect to download a license from the Internet which enables your use of Secure Content, Microsoft may, in conjunction with such license, also download onto your computer such security updates that a secure content owner has requested that Microsoft distribute.[47]

These End-User License Agreements have generally been found binding since the Seventh Circuit decision in *ProCD v. Zeidenberg*.[48] However, one could currently argue as to whether consent obtained via click-wrap agreements is sufficient to authorize someone to impair the integrity of computer data.[49] After all, it does shock one's conscience to imagine a PC user permitting another to sift through personal computer files and even delete them at any point in time, especially in light of the fact the deletion may, at great cost to the P2P user, be in error.[50] Yet, now the Berman Bill explicitly suggests permitting such self-inflicted harm if consent is obtained.[51] Should a user download any software, a third-party agreement between that software provider and Microsoft may result in the user downloading unwanted, privacy intrusive files or programs onto her hard drive.

Loading complete software applications on a computer makes the task of monitoring a user's content that much easier for copyright owners. They merely have to pre-install a program, likely in the form of a Trojan, in connection with any other software download that a user has

---

[47] *See also* Ed Foster, *Check the Fine Print*, INFO WORLD, Sept. 13, 2002 (discussing the automatic update features in Microsoft's end user and volume purchaser license agreements), *at* http://www.infoworld.com/articles/op/xml/02/02/11/020211opfoster.xml.

[48] 86 F.3d 1447 (7th Cir.1996). *But see* Klocek v. Gateway, 104 F. Supp. 2d 1332, 1339-40 (D. Kan. 2000) (rejecting license agreement because the purchaser did not consent to the additional terms enclosed in the software box under U.C.C. § 2-207).

[49] *See* SoftMan Prods. Co. v. Adobe Sys. Inc., 171 F. Supp. 2d 1075, 1088 (C.D. Cal. 2001) (recognizing that precedent has found shrinkwrap agreements as generally unconscionable contracts of adhesion); I. Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 338 (D. Mass. 2002) ("To be sure, shrinkwrap and clickwrap license agreements share the defect of any standardized contract -- they are susceptible to the inclusion of terms that border on the unconscionable …"); U.C.C. §2-302; *Cf.* Klocek, 104 F. Supp. at 1339-40 (rejecting license agreement because the purchaser did not consent to the additional terms enclosed in the software box under U.C.C. § 2-207); Arizona Retail Sys. v. Software Link, 831 F.Supp. 759, 765 (D. Ariz. 1993) (same); Step-Saver Data Sys. v. Wyse Tech., 939 F.Supp. 91, 99-103 (3rd Cir. 1991) (same). *But see* Specht v. Netscape Commun. Corp., 150 F.Supp. 2d 585, 594 (S.D. N.Y. 2001) (finding click-wrap agreements generally enforceable); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1148-49 (7th Cir. 1997), *cert. denied,* 522 U.S. 808 (1997) (upholding an arbitration forum clause against purchaser).

[50] *See infra* p.10 (on fair use).

[51] H.R. 5211 at §514(a).

consented to and such will permit them to regularly monitor individual computers.[52] This back door enforcement by copyright owners will likely increase the vulnerability of the computer system to third-party crackers – those not designated to enforce copyright interests – and will easily provide the ability to survey and remove other computer files, whether or not they relate to copyright interests.[53]

Even if one assumes that all copyright owners will use the safe harbor only to the extent necessary to protect their interests, the bill nonetheless threatens to disturb a delicate balance between the interests of copyright and fair use. Under the proposed legislation, copyright owners are specifically empowered to impair the distribution and reproduction of files containing portions of their works regardless of whether such portions are excepted from copyright under the doctrine of fair use.[54] Thus, the Berman Bill may join and work in conjunction with other legislation like the Digital Millennium Copyright Act,[55] the Copyright Term Extension Act,[56] and UCITA in further extending the reaches of copyright protection.[57] Also in this light, the bill threatens to destroy one of the principal benefits of P2P technology, its service as a font of future creation by facilitating the free flow of ideas and speech between persons. To that end, the Berman Bill may be more than bad policy—it may be unconstitutional.[58]

Conclusion

Perhaps it is too early to get too worked up over Hollywood's efforts to consecrate its own anti-piracy efforts. There is little time left in the 107th Congress, likely too short a period for a bill of significant privacy implications, which this act will eventually be discovered as, from making its way out of committee and to the President's desk. When a final self-enforcement bill comes to light, it may limit private action to certain anti-piracy technologies and may (though not likely) not be so supportive of the consensual impairment of files and the impairment of fair use works. Such revisions, however, would surely meet with many objections from the MPAA and RIAA and may render the act useless given the limitations of current impairment technologies. Most certainly, the Berman Bill should not be cast aside as a legislative fluke with great haste; it is likely to rear its head again, if in altered form. So long as peer-to-peer technology continues to

---

[52] Interview with Christopher McGettigan, *supra* note 32.
[53] *Id.*
[54] *See* H.R. 5211 at § 514(a), (b).
[55] Pub. L. No. 105-304, 112 Stat. 2860 (1998).
[56] Pub. L. No. 105-298, 112 Stat. 2827 (1998).
[57] *See, e.g.*, Pamela Samuelson, *Mapping the Digital Public Domain: Threats & Opportunities*, 66 LAW & CONTEMP. PROBS. (forthcoming Winter 2002).

unabatedly burn a hole in the pockets of the motion picture, recording, and software industries with traditional enforcement systems standing by the wayside, privacy buffs can expect to face a bi-partisan Congress willing at least to consider providing a level playing field for this battle over copyrights between vigilantes and pirates.

By: Christopher Fazekas

---

[58] *See, e.g.,* Neil Netanel*, Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1 (2001) (arguing that the DMCA is unconstitutional without some fair use limitations).