



Electronic Countermeasures To Copyright Infringement on the Internet: Law and Technology

by

Joseph D. Schleimer, Esq.

Journal of Internet Law, November, 2001

Literally *billions* of copyright infringements have taken place over the Internet through the so-called file sharing systems. Legal efforts to shut down Napster and its imitators have begun to have an impact, but even as one system is shut down many others spring up, some of them in offshore locations beyond the reach of the U.S Courts. Our legal system does not seem to be up to the task of dealing with this problem over the long run, so it is inevitable that copyright owners will explore more direct, technological methods of striking back at infringers.

Because they involve a massive uploading and downloading among strangers, the peer-to-peer file exchanges are the perfect vector for computer viruses. For the same reason, these systems are vulnerable to electronic countermeasures that can jam, inhibit, block, investigate and document on-line copyright infringement.

State and Federal anti-hacking statutes were enacted before copyright infringement on the Internet became a serious problem. Those statutes are so overbroad they unintentionally restrict the implementation of legitimate electronic countermeasures. As a result, some of the most effective potential counterattack technologies are arguably illegal. Other countermeasures are merely technical violations of the anti-hacking laws but should ultimately be held legal under the common law doctrines of justification and abatement.

The Technology of Electronic Countermeasures

The major file-sharing systems, such as Gnutella and Napster, provide content

by scanning the hard drives of their users, posting the users' files on an index, and making those files available for uploading at the request of other users. Thus, before Napster was shut down, every time a Napster user logged onto the system to download free music, the music files on the downloader's computer were simultaneously posted, indexed and uploaded to other users.

Although euphemistically referred to as file sharing,⁴ this process constitutes an infringement of copyright. See, *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Under some circumstances, it could be prosecuted as a *criminal* copyright infringement under the No Electronic Theft (NET) Act of 1997. See, "[Criminal Prosecution of On-Line 'File Sharing'](#)" by Joseph D. Schleimer, Esq. and Kenneth D. Freundlich, Esq. (*Journal of Internet Law*, August, 2001)

By definition, peer-to-peer file-sharing systems are wide open, so anyone can post files. Once a file is downloaded to another user, the file-sharing software will detect it on the downloader's hard drive, index it, and re-post it for uploading to other users. In this fashion, a popular file (such as a recent hit song) can form a daisy chain of high-quality digital copies across cyberspace.

A Napster virus or Gnutella virus disguised as a popular music file and posted on the file-sharing services could exploit this daisy chain and be transmitted to millions of computers with breathtaking speed. The emergence of such viruses on the file-sharing systems would obviously deter infringement. However, releasing a malicious computer virus onto the Internet is a felony under both State and Federal law. See, 18 U.S.C. ' 1030(a)(5); California Penal Code ' 502(c)(8). See, also, New York Penal Law ' 156.27; Michigan Stat. ' 28.529(5)(b), (7)(2); 18 Pennsylvania Cons. Stat. ' 3933(A)(1), (B).

Moreover, using a virus to combat copyright infringement would inevitably cause severe injury to innocent third parties. Before it was shut down, more than 70 million users downloaded music through Napster, and millions of them used computers at work or school, or downloaded the files to their parents' computers at home. Thus, a Napster virus could wreak havoc on millions of computers owned by innocent third parties.

Surgical electronic countermeasures are feasible because the file-sharing systems are open and accessible to the public. Moreover, these systems operate in plain sight, so it should be legal to use reasonable electronic countermeasures, especially against systems like Napster and Aimster that brazenly promote mass copyright infringements.

The creators of Napster recognized from the start that their system had to acquire a massive user base to provide content. Once a large number of users had logged on, Napster publicized the comprehensiveness of the content to attract millions of additional users. For this strategy to work, the Napster Web Site had to

be highly publicized and accessible to the general public. Thus, anyone could log onto Napster, browse the system, and observe thousands of copyrighted songs being infringed.

This open architecture means that electronic countermeasures can be implemented on Napster-style systems without any unauthorized entry to the system. This is legally a very important factor because most of the anti-hacking laws focus primarily on preventing computer trespass. See, e.g., New York Penal Law ' 156.10; Washington Rev. Code ' 9A.52.110.

Because of the public nature of their activities, the individual users of Napster- and Gnutella-type systems should have no reasonable expectation of privacy. The songs on Napster were all posted by users, each of whom made a general offer to the public to open up his or her personal hard drive and upload files to strangers. The publicly acknowledged purpose of these transactions was the mutual and reciprocal infringement of copyrighted material. In that context, no privacy-in-fact existed. For the same reason, no intrusion was necessary to enter the hard drives of millions of Napster users.

Since access is consensual and therefore should be legal *per se*, the next step in determining legality requires a critical analysis of the functionality of the particular electronic countermeasures used.

CEASE-AND-DESIST PROGRAMS

The object of a cease-and-desist program is merely to deliver an electronic message to online infringers. These files would be posted on the peer-to-peer indices masquerading as desirable content, such as a current hit song. The would-be infringer downloads the decoy song voluntarily and eagerly opens it in the expectation of hearing music. Instead, the file contains, for example, an authoritarian voice that accuses the downloader of criminal and civil copyright infringement and demands that he or she immediately cease and desist. (The voice can also deliver a paternalistic lecture about how downloading bootleg material risks infecting the infringer's computer with a virus.)

Delivery of such a message should not violate any anti-hacking law because the downloader voluntarily brought the file into his or her system and because the cease-and-desist file does not engage in data collection, nor inflict any damage. Such communications should be *per se* immune under the litigation privilege, as well as protected by the First Amendment.

Some anti-hacking statutes contain specific references to "self replicating" and "self propagating" programs as part of an effort to define a computer virus. See, e.g., California Penal Code ' 502(b)(10). In fact, most viruses propagate themselves by accessing the victim's communications software and emailing copies of the virus to

every person in the victim's address book. The recipients of this poisoned email open the file and inadvertently unleash the virus, which then accesses the recipient's address books and propagates itself again. In this fashion, many viruses have spread globally at great speed.

Decoy files should not include a self-replicating function, because that might legally classify them as viruses. In fact, they don't need to self-replicate because, once the decoy has been downloaded, every time the user logs back onto a file-sharing system, the software will index, post, and offer the decoy file to other users, still masquerading as a hit song. Other users, hoping to get a free copy of the song, will copy it to their hard drive. The decoy will then deliver the cease-and-desist message to them, and from that point forward they will post it each time they log onto the system.

This should propagate the decoy through the file-sharing system but should not violate any hacking statutes because each replication of the decoy file occurs only as the result of two users (uploader and downloader) mutually attempting to infringe a copyright.

"SNITCH" PROGRAMS

A Snitch program also could be distributed as a decoy file. Once inside the downloader's computer, the snitch would actively collect information, such as the infringer's name and address, a list of infringed material found on the local hard drive, and the IP addresses of recipients of infringing uploads. The snitch, and its cache of incriminating information, could be retrieved each time the infringer logs onto a file-sharing system and thereby posts the snitch (decoy) file back onto the system.

The snitch would remain resident on the infringer's computer, making updated reports on infringing activities each time the infringer logs onto the file-sharing system. Because of the daisy-chain effect, the infringer would pass the snitch to other infringers. Incriminating information collected by the snitch program could be used to generate cease-and-desist letters from private lawyers or as the basis for civil lawsuits or criminal referrals.

The use of information-gathering decoys might result in legal challenges under the data theft provisions of the state and federal anti-hacking statutes. See, e.g., 18 U.S.C. ' 1030(a)(2)(C); California Penal Code ' 502(c)(2); New York Penal Law ' 156.10; Michigan Stat. ' 28.529(5).

The most likely context for such a legal challenge would be a motion to suppress. Could information from a snitch be used to demonstrate probable cause for issuance of a search warrant, to seize a computer or arrest an infringer? Would data gathered by a snitch program be admissible as evidence in a prosecution for

copyright infringement?

Criminal defendants will argue that the information was obtained through an illegal search. The prosecution would respond by proving that the infringer had posted the snitch file (and its cache of incriminating information) on the World Wide Web as part of a voluntary and unprompted attempt to engage in further copyright infringement in plain sight. The outcome of this debate should not affect admissibility because information gathering by the snitch program constitutes, at most, a private search, not state action, and neither the Fourth Amendment nor the exclusionary rule applies. See, *United States v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652 (1984)(evidence admissible because intrusion by Federal Express employees was a private action); *United States v. Hall*, 142 F.3d 988, (7th Cir. 1998)(computer evidence seized by private technician held admissible).

The same rule of admissibility should apply in civil proceedings, so long as the party conducting the private search has probable cause to seize incriminating evidence. See, e.g., *Ecker v. Raging Waters Group, Inc.* (2001) 87 Cal.App.4th 1320, 105 Cal.Rptr.2d 320 (security guards had probable cause to seize videotape). Since only persons actively involved in on-line copyright infringement would receive the snitch in their computers, probable cause should always be present.

Including a snitch program in legal copies of music files or other copyrighted material is ill-advised. The Copyright Act expressly authorizes circumvention of snitch software when it has been improperly included in lawfully acquired copyrighted material. See, 17 U.S.C. ' 1201(i). Under the same statute, if the file containing the snitch software was obtained illegally (i.e., if it has been pirated), the circumventer of the snitch program might even be subject to liability for the act of circumvention. See, 17 U.S.C. ' 1201(i)(1)(D)

One interesting collateral effect of snitch programs is, they may trigger virus alarms. The cumulative effect of false virus alarms might, however, reinforce the perception that illegal downloading entails a high risk of viral infection. Indeed, this chilling effect might be one of the most effective electronic countermeasures available.

ELECTRONIC TAGGANTS

A snitch program could not distinguish between legal and illegal files located on a target computer in the absence of some identifying mark that conclusively establishes that a particular file is illegal. Copyright owners could partially overcome this problem by posting decoy files which contain unique taggants. The presence of a taggant in a file proves that it had, at some point, been copied from an illegal file-sharing system. The owner of a copyright has a statutory privilege to insert identification information in digital copies to monitor infringement. 17 U.S.C. ' ' 1002, 1202.

MASS DECOY POSTINGS

Web sites guilty of chronic copyright infringement could be flooded with decoy files, thus forcing users to download numerous decoys to obtain the real music files. After numerous decoys have been posted, the daisy chain effect of the file-sharing system would replicate them even further, and the decoys could ultimately bury the real files. The burden of wading through the decoys, and being constantly bombarded with annoying cease and desist messages from the voice, should drive infringers away from the illegal sites.

Web site operators may challenge this tactic based on anti-hacking statutes that outlaw denial-of-service attacks. See, e.g., California Penal Code ' 502(c)(5). Such legal challenges could be launched in civil proceedings, as many of the anti-hacking statutes have clauses specifically creating a private cause of action. See, e.g., 18 U.S.C. ' 1030(g); California Penal Code ' 502(e); Georgia Code ' 16-9-93(g); Nevada Rev. Stat. ' 205.511; Oklahoma Stat. tit. 21, ' 1955(c); Virginia Code ' 18-2-152.12; Vermont Stat. tit. 13, ' 4106; West Virginia Code ' 61-3C-16.

In any such civil proceeding, it would be significant whether the Web site operator had encouraged, tolerated or had knowledge of the use of the site for copyright infringement. If the Web site operator had been warned that the system was being used for infringement, but failed to comply with the notice-and-take-down procedures under the Copyright Act (17 U.S.C. ' 512), a civil lawsuit against the subsequent use of decoy flooding would not have much legitimacy.

"HANDSHAKE" PROGRAMS

The most deserving targets for electronic countermeasures are the individual computers that upload copyrighted files through the peer-to-peer systems. Without this posting of copyrighted material, no infringements could take place. The copyright owner has a keen interest in taking down particular files which infringe particular copyrights. Hence, the ability to attack specific infringing files is very desirable, from the copyright owners= standpoint.

In the peer-to-peer systems, downloaders are simultaneously uploaders, so a decoy file, once resident on the user=s computer, could block the uploading of specific copyrighted materials. This would require a massive use of decoys to make sure that all or most of the persons who are posting the targeted upload files receive such a Ablocking@ program into their system.

A more direct approach would be to identify specific infringing files posted on a file-sharing system, initiate an upload of those particular files, and during the Ahandshake@ (when the uploader=s computer is introducing itself), insert a program into the uploader=s computer that blocks copying of the infringing file, deletes it, or replaces it with a cease-and-desist or decoy program. The technological feasibility of

such an offensive measure depends on the existence of vulnerabilities in the receiving system.

Such functions might be challenged under the Aalteration@ and Adamage@ proscriptions in the anti-hacking statutes. See, e.g., 18 U.S.C. ' 1030(a)(5); California Penal Code ' 502(c)(4); New York Penal Law ' 156.20, .26. However, because it was an offer to illegally upload which attracted the handshake counterattack, anyone filing such a legal challenge automatically subjects himself or herself to a countersuit for copyright infringement.

This kind of proactive electronic countermeasure should be legally justified because it targets specific files being used to infringe specific copyrights, and blocking specific acts of infringement is the only impact.

JUSTIFICATION AND ABATEMENT

Because of the overbreadth of the anti-hacking statutes, the legality of using certain electronic countermeasures may depend on the common law defenses of justification and abatement. Justification is based on the traditional right to defend property. This doctrine, developed in much simpler times, has not changed much over the generations, so many of the legal authorities are quite old. For example, in *Richardson v. Anthony*, 12 Vt. 273 (1840), the defendant entered plaintiff's property to recover possession of some heifers and was sued for trespass. The Vermont Supreme Court held that the defendant was justified in Abreaking the close@ to recover his cattle, even though the property owner had refused entry.

Some courts find recapture legally permissible under an implied-in-law *consent* to trespass. See, e.g., *Madden v. Brown*, 8 A.D. 454, 40 N.Y.S. 714 (1896)(A[W]here a person places the goods of another upon his own premises, he gives to the owner of them an *implied license* to enter for the purpose of taking them.)(Emphasis added)

This implied consent doctrine could be very important in the context of electronic countermeasures because most anti-hacking statutes are couched in terms of banning the unauthorized entry into a computer system. If the law deems a computer invasion (to protect intellectual property) to be under an implied license to enter, then the anti-hacking statute is not violated.

Justification defenses have always been limited to the use of reasonable force, and the defense is strongest when the property owner is in Ahot pursuit@ of the stolen goods. Thus, in *State v. Dooley*, 121 Mo. 591 (1894), the court held that the defendants were entitled to a jury instruction on the right of recapture of property when, after a hot pursuit on horseback, they brandished a Winchester rifle to recover some horses. Under the circumstances, the jury could have found this limited show of force was reasonable, so a justification instruction should have been given.

As the U.S. Supreme Court stated in *Davis v. United States*, 328 U.S. 582, 591, 66 S.Ct. 1256, 1260 (1946):

A[A]n owner of property, who seeks to take it from one who is unlawfully in possession, has long been recognized to have greater leeway than he would have but for his right to possession. The claim of ownership will even justify a trespass and warrant steps otherwise unlawful.@

The common law remedy of abatement, which should be available on the theory that online infringers (and some incorrigible Web site operators) are maintaining a nuisance, complements the doctrine of justification. Abatement may trigger a self-help right to peaceably enter private property and abate the nuisance. See, e.g., California Civil Code ' 3502 (1872), which codified the common law right of abatement:

AA person injured by a private nuisance may abate it by removing, or, if necessary, destroying the thing which constitutes the nuisance, without committing a breach of the peace, or doing unnecessary injury.@

APPENDIX

The Anti-Hacking Statutes

The State and Federal Aanti-hacking@ statutes were enacted to combat a wave of criminal hacking and malicious virus releases beginning in the mid-1980s. The statutory proscriptions vary widely from jurisdiction to jurisdiction, but typical clauses prohibit (a) unauthorized Aaccessing@ of private computer systems; (b) theft of data or software; (c) dissemination of viruses; (d) reckless or malicious alteration or destruction; (e) intrusion into government computers; (f) trafficking in passwords; (g) denial of service attacks; (h) misappropriation of services; and (i) use of computers in fraud, theft or extortion.

FEDERAL ANTI-HACKING STATUTE

The Federal anti-hacking statute, 18 U.S.C. ' 1030, contains the following provisions relevant to the use of anti-infringement countermeasures:

A(a) WhoeverB

....

(2) Intentionally accesses a computer without authorization or exceeds

authorized access, and thereby obtains

....

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

...

(4) knowingly and with intent to defraud accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

....

shall be punished as provided in subsection (c) of this section.

STATE ANTI-HACKING STATUTES

The California statute is a typical state anti-hacking law and typically overbroad. California Penal Code ' 502 states, in relevant part:

A(c) Except as provided in subdivision (h) [exempting acts done within the scope of employment], any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes

use of any data from a computer, computer system, or computer network....

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user or a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces a computer contaminant into any computer, computer system, or computer network....@

The statute also contains the following pertinent definition:

A>Computer contaminant= means any set of computer instructions that are designed to modify, damage, destroy, record or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.@

Many anti-hacking statutes include clauses establishing Along arm@jurisdiction over hackers who access forum state computers from across state lines. See, e.g., Arizona Rev. Stat. ' 13-2316B; Connecticut Gen. Stat. ' 53a-261; Georgia Code ' 16-9-94(4); Kentucky Rev. Stat. 434.860; Mississippi Code ' 97-45-11(b); New Hampshire Rev. Stat. 638:19(III); Virginia Code ' 18.2-152.10(4); West Virginia Code ' 61-3C-20.

California Penal Code ' 502(j) is typical of these long arm statutes:

AFor purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.@

Anti-infringement countermeasures cannot be limited to a particular state, so (in the absence of Federal preemption) any legal analysis of electronic countermeasures must take into account all of the state anti-hacking laws. For the readers= convenience, here are the relevant citations:

Alabama Code ' ' 13-8-101 to 103

Alaska Stat. ' ' 11.46.200, .484, .740, .990

Arizona Rev. Stat. ' ' 13-1801, -2301, -2316.02, -2316

Arkansas Code Ann. ' ' 5-41-101 to -104, -107, -108

California Penal Code ' ' 502-502.01

Colorado Rev. Stat. ' ' 18-5.5-101 to -102

Connecticut Gen. Stat. ' ' 53a-250 to -262

Delaware Code tit. 11, ' ' 932-939

Florida Stat. ' ' 815.01 et seq.

Georgia Code ' ' 16-9-90 et seq.

Hawaii Rev. Stat. ' ' 708-890 et seq.

Idaho Code ' ' 18-2201 to -2202

720 Illinois Comp. Stat. ' ' 5/16D-1 to -7

Indiana Code ' ' 35-42-2-3, *amended by* 2001 Ind. Acts 1644, -43-1-4,
amended by 2001 Ind. Acts 180

Iowa Code ' ' 702.1A, .14, 714.1, 714E.1, 716.6B

Kansas Stat. ' ' 21-3748, 3755

Kentucky Rev. Stat. ' ' 434.840, .845, .850, .855, .860

Louisiana Rev. Stat. ' ' 14:73.1 - .6

Maine Rev. Stat. tit. 17, ' ' 431-433

Maryland Code art. 27, ' ' 146, 555C

Massachusetts Laws ch. 266, ' 120F

Michigan Stat. ' ' 28.529(1) - (7)

Minnesota Stat. ' ' 609.87 - .891

Mississippi Code ' ' 97-45-1, 3, 5, 7, 9, 11, 13

Missouri Rev. Stat. ' ' 556.063, 569.095, .097, .099

Montana Code ' ' 45-6-310 et seq.

Nebraska Rev. Stat. ' ' 28-1341 et seq.

Nevada Rev. Stat. ' ' 205.473 - .498, .505-509, .511, .513

New Hampshire Rev. Stat. ' ' 638:16 et seq.

New Jersey Stat. ' ' 2C:20-23 et seq.

New Mexico Stat. ' ' 30-45-1 et seq.

New York Penal Law ' ' 156.05 et. seq.

North Carolina Gen. Stat. ' ' 14-453 et seq.

North Dakota Cent. Code ' 12.1 et seq.

Ohio Rev. Code ' ' 2913.01, .04

Oklahoma Stat. tit. 21, ' ' 21-1951 et seq.

Oregon Rev. Stat. ' ' 164.125, .377

18 Pennsylvania Cons. Stat. ' 3933

Rhode Island Gen. Laws ' 11-52-1 to -7

South Carolina Code ' ' 16-16-10 to -30

South Dakota Codified Laws ' ' 43-43B-1 to -8

Tennessee Code ' ' 39-14-601 to -603

Texas Penal Code ' ' 33.01 - .04, 39-14-603

Utah Code Ann. ' ' 76-6-701 to -705

Vermont Stat. tit. 13, ' ' 4101-4107

Virginia Code ' ' 18.2-152.1 - .15

Washington Rev. Code ' ' 9A-52-110 to -130

West Virginia Code ' ' 61-3C-1 to -21

Wisconsin Stat. ' ' 947.0125, 943.70

Wyoming Stat. ' ' 6-3-501 to 505

[HOME](#)

