When Should Computer Owners Be Liable for Copyright Infringement by Users?

R. Carter Kirkwood†

Computer networks have caused a radical change in the means of disseminating information, a change that will likely be as profound as the changes caused by the telephone and television,¹ and that may even rival the changes caused by the invention of the printing press. Copyright law, which the printing press first made necessary, has "always been closely connected with . . . technological improvements in means of dissemination."² And, as technology has evolved, "[s]uccessive ages have drawn different balances among the interest of the writer in the control and exploitation of his intellectual property, the related interest of the publisher, and the competing interest of society in the untrammeled dissemination of ideas."³ Thus, as the Supreme Court observed, copyright law needs to "strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce."⁴ With the advent of computers, courts need to strike a new balance between the interests of copyright owners and the right of society to use computer networks. To date, in four reported cases, courts have addressed the use of computer networks to reproduce and disseminate copyrighted materials illegally.⁵ A primary question in these cases is which theory of copy-

---

† B.A. 1991, University of California, Los Angeles; J.D. Candidate 1997, The University of Chicago.

¹ See The Internet Survey, The Economist 3, 4 (July 1, 1995).
² Benjamin Kaplan, An Unhurried View Of Copyright vii-viii (Columbia 1967).
³ Id.
⁵ Playboy Enterprises, Inc v Frena, 839 F Supp 1552 (M D Fla 1993) (finding operator of computer bulletin board system ("BBS") liable for direct copyright infringement); Sega Enterprises Ltd v Maphia, 1996 US Dist LEXIS 20385 (N D Cal) (granting summary judgment against BBS owner for contributory infringement); Central Point Software, Inc v Nugent, 903 F Supp 1057 (E D Tex 1995) (finding BBS operator liable for direct infringement); Religious Technology Ctr v Netcom On-Line Communication Servs, Inc, 907 F Supp 1361 (N D Cal 1995) (holding that defendants, a BBS operator and an Internet access provider, were not liable for either direct or vicarious copyright infringement, and that their liability for contributory infringement involved genuine issue of material fact).
right infringement should be used to determine whether the owners of networks are liable.

Many cases of copyright infringement on a computer network involve users who upload ("post") copyrighted information to a computer bulletin board without the copyright owner's permission. Often the user will post this information anonymously in order to avoid liability. The pirated information is then automatically distributed across the network to other computers and is stored on each computer's hard drive. Subsequent users of these computers are able to download the pirated information until the computer automatically removes it.

Computer networks make copyright infringement easier, less expensive, and safer than do other methods of disseminating information. Consequently, copyright infringement is quickly becoming rampant on the Internet. There are two possible ways to minimize this increase in copyright infringement. The first approach would be to reduce or remove the legal impediments to imposing criminal penalties for copyright infringement. Currently, the Copyright Act imposes criminal penalties only if prosecutors can prove that the defendant infringed a copyright "willfully and for purposes of commercial advantage or private financial gain." One of the principal rationales for criminal penalties is that they help deter criminal acts by people who are judgment-proof. It might reasonably be assumed that many of those posting copyrighted materials illegally are judgment-proof (students, for example, who often have little to lose other than

---

6 Messages that are posted on the Internet or any online service company (like America Online, CompuServe or Prodigy) are mixed in with hundreds of thousands of other messages.
7 The network will often distribute the message to thousands of computers, almost all with different owners.
8 Computer owners typically have the computer automatically remove the information after several weeks.
9 Computers are able to make inexpensive, high quality copies of most copyrighted materials. When computers are combined in networks by telecommunication lines, they are able to deliver inexpensively and quickly the copies over long distances. Because most computer network activity is channeled through a common processor or chip such as a "Pentium," it is often difficult to determine who did the actual infringing. Moreover, it is relatively easy to communicate anonymously on computer networks, further complicating any attempts to hold individuals responsible for infringement. See Philip E. Ross, Cops versus robbers in cyberspace, Forbes 134, 134-36 (Sept 9, 1996) (describing methods copyright holders are devising to detect copyright violators on the Internet).
10 See, for example, Eric Braun, The Internet Directory, Version 2.0, #306 (Fawcett Columbine 1998) (newsgroup alt.binaries.pictures.erotica has "gigabytes of copyright violators"). The network will often distribute the message to thousands of computers, most of which are owned by different owners.
11 17 USC § 506(a) (1994).
their computers). Thus, to deter infringement, Congress could make it easier to impose criminal sanctions by either reducing the mens rea requirement or removing the financial gain requirement. However, this solution may have a chilling effect on borderline cases of fair use, and would do little or nothing to solve the problems associated with anonymous users.

The second possible approach to the increase in copyright infringement would be to place a duty on computer owners, who can monitor and control the activities of their users, to prevent copyright infringement. This solution builds on the recognized concepts of vicarious and contributory infringement and rests upon a similar rationale. In this context, as in the case of vicarious infringement, the owner "has the power to police carefully the conduct of its [invitee]; [imposing liability] will simply encourage it to do so, thus placing responsibility where it can and should be effectively exercised."

However, holding computer owners liable for contributory and vicarious infringement could make owners liable for most, if not all, copyright infringement on their systems, depending on how each theory's requirements are interpreted. Therefore it is necessary to define relevant limits for both theories of liability. Imposing overly broad liability on computer owners would force them to monitor every single piece of information, or "message," posted on their systems. Since there are more than one hundred thousand new postings each day on the Internet, and since complete monitoring would require that every message be read in its entirety, to require computer owners to monitor every message would be extremely expensive. Such a requirement would threaten to undermine the greatest advantage of computer networks—that they provide inexpensive mass communication by automating the tasks of copying and distributing information. Furthermore, an expensive monitoring requirement would impede both development of the Internet and information distribu-

---

13 Indeed, at least one court has urged Congress to consider expanding criminal liability for copyright infringement. See United States v LaMacchia, 871 F Supp 535, 545 (D Mass 1994) (Criminal penalties should attach to multiple willful infringements even without a commercial motive.).

14 A fair use defense is sometimes recognized by courts when the challenged use of copyrighted material is limited, non-commercial and incidental. "Fair use" is a somewhat vague term, and courts have applied it on a case-by-case basis. The nature and scope of the fair use defense is relatively complicated and is beyond the scope of this Comment. Melville B. Nimmer and David Nimmer, Nimmer on Copyright § 13.05 (Matthew Bender 1996).

15 Shapiro, Bernstein & Co v H.L. Green Co, 316 F2d 304, 308 (2d Cir 1963).

tion on it. A better solution would be a rule that only requires computer owners to monitor for patterns or significant amounts of infringement, substantially reducing their monitoring costs while protecting copyright owners against significant infringement.

This Comment argues that courts can achieve the appropriate balance between the rights of copyright owners and the interests of society by applying the vicarious and contributory infringement standards to computer owners. Part I describes the common features of major computer networks, defines specialized terms, and discusses the impact of several software programs on infringement. Part II describes the current law of copyright infringement and explains the standards courts apply to determine direct, vicarious, and contributory infringement. Part III examines computer network infringement cases. Finally, Part IV argues that computer owners should not be held liable for direct infringement when their users post pirated material. Instead, computer owners should be held liable for vicarious and contributory infringement because these standards achieve the best balance between copyright protection and information dissemination. Vicarious infringement is appropriate for computer owners running bulletin board software because they resemble dance hall owners, who have traditionally been held vicariously liable for infringement by musicians who play in the owners’ halls. Contributory infringement is appropriate when computer owners have constructive knowledge of copyright violations because such liability will encourage computer owners to monitor the activity of their users.

I. THE PROCESS OF COMPUTER NETWORK COMMUNICATION

A. Description of Computer Networks

A computer network is made up of three primary building blocks: computers, software, and telecommunication lines. Most networks consist of "server" computers, where information is stored, reproduced, and controlled, and "client" computers, that customers use to "dial into" or access the information on the servers. Software both enables a computer to function and permits the computer owner to control how that computer is used. Finally, telecommunication lines connect computers and make it possible to transfer information from one computer to another.  

17 Telecommunication lines range from twisted pair copper phone lines provided by local telephone companies to high capacity fiber-optic lines leased from long-distance telephone companies. See Nicholas Negroponte, Being Digital 22-23 (Vintage Books
Three primary kinds of computer networks are available to the public. First, a bulletin board system ("BBS") is generally a single "server" computer connected to several modems that allow users to dial in. Each BBS uses different hardware and software configurations that reflect the BBS operator's preferences. Most BBSs allow users to communicate via e-mail and computer bulletin boards. For general information about BBSs, see Howard Rheingold, The Virtual Community: Homesteading on the Electronic Frontier 8-9, 131-44 (Harper Perennial 1993); ACLU, 929 F Supp at 832-34.

Second, online service companies are national networks of "server" computers, each with a proprietary system that users can access only by subscription. Online service companies contract with information providers for much of the information carried on their networks and then make that information available to subscribers.

Third, the Internet is a vast network of hundreds of thousands of "server" and "client" computers that use a common software protocol. Nobody "owns" the Internet; rather, it consists of computers owned by individuals, universities, government agencies and corporations. Generally, users access the Internet through "access providers." The Internet, which has grown explosively during the last five years, currently has over twenty million users.

B. Computer Owners

The term "computer owner," for the purposes of this Comment, includes anyone who controls the information that is placed on a computer. Thus, the term encompasses not only the

---

1996); Peter Coy, Please Hold for New Technology, Business Week 82 (Apr 8, 1996).
18 Each BBS uses different hardware and software configurations that reflect the BBS operator's preferences. Most BBSs allow users to communicate via e-mail and computer bulletin boards. For general information about BBSs, see Howard Rheingold, The Virtual Community: Homesteading on the Electronic Frontier 8-9, 131-44 (Harper Perennial 1993); ACLU, 929 F Supp at 832-34.
19 Online service companies include America Online ("AOL"), Prodigy, and CompuServe.
20 See Mary Meeker and Chris DePuy, the Internet Report § 3 at 2 (Harper Business 1996).
21 See Rheingold, The Virtual Community at 277 (cited in note 18).
22 ACLU, 929 F Supp at 832.
23 Id (noting that "[n]o single entity—academic, corporate, governmental, or nonprofit—administers the Internet").
24 Some companies specialize solely in providing consumers dial-up access to the Internet. Individuals may also access the Internet through online service companies, as well as school- and employer-provided computers directly connected to the Internet. See id at 832-34.
25 Between 1990 and 1996, the Internet evolved from an academic research tool to the foundation of the information superhighway. During this time, it grew from less than one million users to more than twenty million users. See Meeker and DePuy, the Internet Report § 3 at 16 (cited in note 20). See also ACLU, 929 F Supp at 831 ("In all, reasonable estimates are that as many as forty million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to two hundred million users by the year 1999."). The Internet has grown quickly because it is a simple and inexpensive way to create a computer network.
legal owners of computers, but also possessors of computers, system operators, BBSs, online service companies, and Internet access providers. These "computer owners" can control a user's actions because they have the power to exclude any user from accessing their computers.

C. Software

There are three important types of software employed in computer networks which are relevant for this Comment: system and network software, computer bulletin board software, and software that enables pseudonymity and anonymity.

1. System and network software.

System and network software enables computer owners to monitor and exert control over the actions of users. A system administrator—usually either the computer owner or his agent—is the individual who controls the system software. The two primary ways that system software controls computer access are (1) requiring passwords, and (2) setting different "rights" for different accounts. By changing a user's password a computer owner can suspend a user's account. For example, one Internet access provider has suspended users' accounts on more than one thousand occasions for inappropriate commercial advertising, posting obscene materials, and off-topic postings. Thus, by controlling access in specific ways, the system administrator can control or police what a user does on the owner's computer.

26 Any legal standard that courts establish for computer owners on one type of computer network can also be applied to computer owners on other types of networks. Therefore, the courts will not have to create different legal standards for BBSs, online service companies, and the Internet.

27 However, computer owners can control only the information contained on the computers they own. See ACLU v Reno, 929 F Supp 824, 824 (E D Pa 1996), cert granted, 117 S Ct 554 (1996) (holding that speakers could not be held liable for indecent communications on the Internet because there were no effective ways for speakers to ensure that minors did not have access to indecent speech). The ACLU holding reflects the fact that on the Internet, it is often possible to access information through different computer systems.


29 For instance, a typical system administrator sets up bulletin board software to allow users to post and read any messages they want, but the software does not allow users to delete messages. Alternatively, the system administrator may allow users to post one-page text files, while requiring that longer messages be pre-approved. As this example demonstrates, system administrators will be responsible for "policing" computer networks, whether they want to or not. They enforce the rules created by Congress, the courts, and the computer owners because they control the software that in turn controls the computers.
2. Computer bulletin board software.

Computer bulletin board software allows users to post a message on a computer server where that message can then be retrieved by other users. Among the most widely used computer bulletin boards are “USENET newsgroups” on the Internet, to which almost one hundred thousand messages are posted each day. These messages are organized into topical newsgroups. There are over fifteen thousand newsgroups, covering every imaginable topic. Although readership of newsgroups has not been precisely determined, in 1994 a reasonably popular newsgroup had between one hundred thousand and two hundred thousand regular readers, and some exceeded four hundred thousand.

While some newsgroups have a moderator, most are free-for-alls and rely on social pressure to curb user abuse, such as off-topic postings, defamation, pornography and pirated copyrighted materials. Regardless of the specific software used to create a computer bulletin board, all bulletin board software allows individuals to communicate inexpensively to large numbers of potential readers. Essentially, anyone with a computer can now communicate as effectively as if they owned a printing press or a television station.

3. Software that allows pseudonymity and anonymity.

One of the many unique traits of computer networks is the ease with which users can communicate without revealing their identities. There are two ways to achieve this result: pseudonymity and anonymity. Pseudonymity occurs when a user sends a message and uses a pseudonym or nickname, rather than

---

30 On a BBS, the owner runs computer bulletin board software that allows some users to copy files to the owner’s hard drive and enables others to retrieve those files. See Rheingold, The Virtual Community at 131-32 (cited in note 18). Usually, online service companies use similar software for access to the material available within each online service, but also provide access to general resources on the Internet. For the Internet, there are two major groups of software: automatic mailing lists, called “listservs” and “USENET newsgroups,” which open discussions on a particular topic. Listservs work by automatically forwarding a message to each subscriber’s e-mail address. In contrast, USENET newsgroups do not require subscription but are distributed by peer-to-peer connections between approximately two hundred thousand computers known as “USENET servers.” See ACLU, 929 F Supp at 833-35.
31 ACLU, 929 F Supp at 835.
32 Id.
34 David Hoye, Online Sex Sells but Local Officials Warn There Are Limits, Phoenix Gazette C1 (Feb 27, 1995).
her true name, to identify herself. When a user employs a pseudonym, the only way to discover that user’s true identity is if she, or an access provider that knows her true identity, reveals it.

Users of the Internet can also communicate anonymously. If a user is concerned that his access provider will reveal his identity, he may use “anonymous remailers” to hide his identity. An anonymous remailer is software that removes the identification information of the user (included in all information sent across the Internet), and replaces it with identification information that points to the remailer itself. Thus, the owner of the anonymous remailer is the only individual who knows the sender’s e-mail address.

Although these methods generally safeguard a user’s true identity, theoretically a third party can trace an anonymous or pseudonymous message. Further, even if tracing proves impossible, the third party can identify the sender of such a message by obtaining a court order requiring an anonymous remailer owner to turn over the list of names of the people who use the remailer and add their pseudonyms. However, many anonymous remailers are located in other countries where such orders may be difficult to enforce.

Pseudonymity and anonymity are troublesome because they make it difficult, and sometimes impossible, to determine who is responsible for copyright infringements. This, in turn, makes it much easier for users to violate copyright laws without being held liable. Indeed, both have contributed (especially anonymity) to the explosion of copyright infringement on the Internet. However, this Comment argues that courts, by holding computer owners liable for vicarious and contributory infringement, can overcome this problem and minimize copyright infringement on computer networks.

35 In practice, most communications on computer networks are pseudonymous because many e-mail addresses, such as “iroo2263@access.com,” are cryptic at best. Unless an individual reveals his e-mail address, it is often difficult to ascertain his true identity.

36 Computer owners operating anonymous remailers attract users by promising not to turn over their list of users to anyone else. However, when served with a court order, at least one anonymous remailer operator has provided the sought-after identity, rather than have his entire computer, containing the identities of all who have sent messages through the remailer, seized. Daniel Akst, Postcard from Cyberspace, LA Times D1 (Feb 22, 1995).

37 See The property of the mind, The Economist 57, 59 (July 27, 1996) (“For enforcers, the Internet creates at least two problems. First, . . . it may be hard to track down the source of illicit material. People put it on to the Net anonymously[,]”).
II. THREE TYPES OF COPYRIGHT INFRINGEMENT

There are three types of copyright infringement. The Copyright Act makes anyone who violates one of its five exclusive rights liable for direct infringement. Although the Copyright Act does not expressly render anyone liable for infringement committed by a third party, the courts have long recognized claims of vicarious and contributory infringement, which developed out of the common law of torts.

A. Direct Infringement

The Copyright Act grants five exclusive economic rights to authors and other creators of a copyrighted work: reproduction, creation of derivative works, distribution, public display, and public performance. It further provides that anyone who violates any of these exclusive rights is liable for direct infringement, regardless of his lack of intent or knowledge of infringement. By granting exclusive rights of use, copyright law attempts to provide incentives for people to create and distribute information, and allows them to charge others for use of the information.

Several courts have held that, to establish a prima facie case of direct copyright infringement, the plaintiff must prove (1) ownership of a valid copyright in the infringed work, and (2) copying by the defendant. Courts have also held that, with regard to copyrighted computer software, a plaintiff may establish copying by demonstrating that the software was reproduced in a computer's memory without permission. Because it is rarely possible for a copyright owner to prove copying with direct...
evidence, courts have developed a two-part test to prove copying indirectly. Under this test, the plaintiff must show that the defendant had access to the plaintiff's copyrighted work, and that the defendant's work is substantially similar to the plaintiff's.47

B. Vicarious Infringement

The Second Circuit first applied the notion of vicarious infringement in the landmark case of Shapiro, Bernstein & Co v H.L. Green Co.48 The Shapiro court found a chain store owner liable for copyright infringement where the owner had the right to supervise a concessionaire of “bootleg” phonograph records and received a share of the profits from the concessionaire’s illegal sales. The court looked at two lines of cases: the landlord-tenant cases, and the dance hall cases.49

In the landlord-tenant cases, the landlords were not held liable for copyright infringement by their tenants if the lease gave the tenant control over the property and the landlord had no knowledge of the impending infringement at the time the lease was signed, because that is the point at which the landlord surrendered legal control over the property.50

By contrast, dance hall owners were held liable because they retained control over their property. They retained control even though they invited customers onto the property and hired the entertainers who actually played the music. The dance hall owners controlled their property because they could supervise the actions of the invitees on an ongoing basis and had the power to stop infringing activity. The courts reasoned that dance hall owners profited from invitees’ infringement because the owners used the entertainment to attract customers.51

After considering the landlord-tenant cases and the dance hall cases, the Shapiro court declared that a defendant is liable for vicarious infringement when that defendant (1) has the right

47 Kouf v Walt Disney Pictures & Television, 16 F3d 1042, 1043-44 & n 2 (9th Cir 1994).
48 316 F2d 304 (2d Cir 1963).
49 Id at 307-08.
50 See Fromont v Aeolian Co, 254 F 592 (S D NY 1918), in which a landlord was held not liable after a pianist publicly performed copyrighted work without permission in a concert hall the landlord leased to the pianist's agent, even though the landlord was given notice of the intended infringement before the night of the performance. The Fromont court reasoned that by the time the plaintiff informed the landlord of the impending infringement, the landlord was bound by the lease. The court felt that a landlord entering into an ordinary, everyday business contract should not be liable for what he did not know about until it was too late. Id at 594.
51 See Herbert v The Shanley Co, 242 US 591, 595 (1917) (finding that defendant hotel and restaurant owners caused the infringing performances to attract customers).
and the ability to control the infringer's acts, and (2) receives a direct financial benefit from the infringement.\textsuperscript{52}

There are two principal rationales for vicarious infringement. As the Shapiro court explained, one rationale for holding dance hall owners liable for vicarious infringement is that it gives owners an incentive to monitor their invitees' activities, "thus placing responsibility where it can and should be effectively exercised."\textsuperscript{53} Furthermore, the Shapiro court was concerned that, if it held otherwise, individuals and corporations would "establish[ ] 'dummy operations' and shield[ ] their own eyes from the possibility of copyright infringement, thus creating a buffer against liability while reaping the proceeds of infringement."\textsuperscript{54}

A second rationale is that the vicarious infringement test causes any enforcement or monitoring costs to be spread among the beneficiaries of a means of communication. Thus, if a new form of communication allows more infringement, it is reasonable for the owners of the new method to pay the costs of any precautions needed to minimize infringement. This is because the owners of the means of communication are better able than the copyright owners to spread the costs of precautions among users (customers), the primary beneficiaries of the new means of communication.\textsuperscript{55} By contrast, the copyright owners are only able to spread the costs among the legitimate purchasers of copyrighted materials, thus increasing the costs of legitimate copies and perversely encouraging more piracy.

Courts have relied upon a number of different factors (including contractual control, policing use of equipment, and supervising operations) to determine whether the first prong of the vicarious infringement test has been met.\textsuperscript{56} Thus, to determine

\textsuperscript{52} Shapiro, 316 F2d at 307-08.
\textsuperscript{53} Id at 308.
\textsuperscript{54} Id at 309.
\textsuperscript{55} In Polygram Intl Publishing, Inc v Nevada/TIG, Inc, 855 F Supp 1314 (D Mass 1994) the court offered a third rationale for vicarious infringement. According to the court,

When an individual seeks to profit from an enterprise in which identifiable types of losses are expected to occur, it is ordinarily fair and reasonable to place responsibility for those losses on the person who profits. . . . The enterprise and the person profiting from it are better able than either the innocent injured plaintiff or the person whose act caused the loss to distribute the costs and to shift them to others who have profited from the enterprise.

Id at 1325.
\textsuperscript{56} See Shapiro, 316 F2d at 308 (holding that the defendant had contractual control over the direct infringer's actions because it "retained the ultimate right of supervision" in its contract with the direct infringer); *RCA Ariola Intl*, Inc v Thomas & Grayston Co, 845 F2d 773, 781 (8th Cir 1988) (finding that the defendant company had supervisory
whether a party had the power to control the infringer's acts, courts have required that the owner have the ability to stop the infringement once it starts,\(^\text{77}\) giving owners an incentive to monitor activity on their property and to stop infringing activity once they become aware of it.

Courts have also articulated an additional standard for determining receipt of "direct financial benefit" under the second prong of the vicarious infringement test for cases where owners receive their financial benefit indirectly from entrance fees. Courts have developed this standard in several cases involving owners of swap meets and trade shows.\(^\text{58}\) By holding that such owners receive a financial benefit from entrance fees and food and drink sales, these decisions reflect the reasoning of many of the earlier dance hall cases, in which courts found that dance halls and other entertainment venues received financial benefits from such fees and sales.\(^\text{59}\)

In the swap meet cases, courts also appear to consider what proportion of the customers coming to the venue are attracted by the infringing activity. For example, in Fonovisa, Inc v Cherry Auction, Inc, the Ninth Circuit held that, if the infringing activity "enhance[d] the attractiveness of the venue" and acted as a "draw" for potential customers, then the owners of the swap meet are liable for vicarious infringement.\(^\text{60}\) This standard was clearly satisfied in Fonovisa, as the sheriff had raided the swap meet on one occasion and found thirty-eight thousand counterfeit record-
ings. Under the same analysis, however, a trade show operator was not held liable in Artists Music, Inc v Reed Publishing (USA), Inc because the court did not believe that minor infringements by 4 of the 134 exhibitors in any way affected the trade show's gate receipts.

C. Contributory Infringement

Contributory infringement is based on the "common law doctrine that one who knowingly participates in or furthers a tortious act is jointly and severally liable with the prime tortfeasor." In the leading case on contributory infringement, Gershwin Publishing Corp v Columbia Artists Mgmt, Inc, the Second Circuit held that contributory infringement occurs when the defendant (1) induces, causes, or materially contributes to the infringing conduct of another, and (2) knows or should have known of the infringing activity.

Several courts have interpreted the contribution prong of this test to require that the plaintiff prove the defendant was substantially involved in (contributed to) the infringement before the defendant is held liable for contributory infringement. This requirement effectively balances the interests of the copyright owners with the rights of others to conduct business in substantially unrelated areas of commerce. For example, in Gershwin, the court held that the concert promoter was liable for the infringement by the artists it promoted because of the promoter's "pervasive participation" in creating an audience for the artists.

Other courts have held that the knowledge prong of the contributory infringement test is met by either actual or constructive knowledge of infringing activity. Some of these courts have

---

61 Id at 261.
62 31 USPQ2d 1623, 1627 (S D NY 1994).
64 443 F2d 1159, 1162 (2d Cir 1971).
65 See, for example, Sony Corp of America v Universal City Studios, Inc, 464 US 417, 442 (1984) (holding that a manufacturer's sale of copying equipment "capable of substantial noninfringing uses" to a purchaser who uses the equipment for copyright infringement does not justify manufacturer liability for copyright infringement); Gershwin, 443 F2d at 1163 (holding the concert promoter liable for its artists' infringement because of the promoter's "pervasive participation" in creating an audience for the artists); Demetriades v Kaufmann, 690 F Supp 289, 294 (S D NY 1988) (holding that for contributory infringement, the defendant must be substantially involved in, or substantially aid or encourage, the direct infringement).
66 See Sony, 464 US at 442.
67 Gershwin, 443 F2d at 1163.
68 See, for example, Ez-Tixz, Inc v Hit-Tix, Inc, 919 F Supp 728, 732 (S D NY 1996) (holding that actual knowledge of infringement is not necessary to establish liability).
held that an individual has constructive knowledge if there is a particular trait about a product that indicates it is probably pirated. Specifically, courts have held that owner-operators of machines have constructive knowledge of their users' activities because the owners have continuous control over their machines and are thus in a position to monitor users easily. In *RCA Records v All Fast Systems, Inc*, the court held the defendant liable for contributory infringement because it had the opportunity to observe how each customer intended to use the cassette copying machine owned and operated by the defendant. Furthermore, the court pointed out that the defendant makes hundreds of commercial decisions in exploiting the machine—a choice every time it sells a cassette for use in the machine. It need have no impact on sales of cassettes for legitimate copying for defendant to cease selling to infringing customers. To do so may raise defendant's costs slightly, but this is a proper burden for it to bear if it wishes to profit from a machine which can so easily be used for improper purposes. Therefore, to encourage the defendant to monitor and supervise the actions of its customers, the court held that the defendant had constructive knowledge of infringing acts it would have been aware of had it been monitoring the customers' uses of the machine.

### III. COMPUTER COPYRIGHT CASES

As more and more computers have been connected to networks, people have used this new resource to transfer copied ma-

---

69 See, for example, *Screen Gems*, 256 F Supp at 404 (holding that defendant advertising agency could be liable for record company's infringement upon a finding that the suspiciously low price of records should have indicated to the agency that the company pirated the records); *R & R Recreation Prods Inc v Joan Cook Inc*, 25 USPQ2d 1781, 1784-85 (S D NY 1992) (finding that defendant's failure to put agreement in writing and acceptance of checks for profits without a cover letter may be sufficient to demonstrate actual or constructive knowledge of infringing activities); *Universal City Studios, Inc v American Inusco Mgmt, Inc*, 217 USPQ 1076, 1077 (N D Ill 1981) (finding that purchase of movie video released in the theaters only a few days before may be sufficient to show defendant knew or should have known the video was pirated).

70 Although control is not a formal element of contributory infringement, the courts in both *Sony* and *RCA Records v All-Fast Systems, Inc* focused on the knowledge of the defendants at the time they had control over the copying equipment. *Sony*, 464 US at 442 (control given up at the moment of sale); *RCA Records*, 594 F Supp 335, 339 (S D NY 1984) (owner-operator retained control).

71 594 F Supp 335, 339 (S D NY 1984).

72 Id.

73 Id.
Computer Network Copyright Infringement

From one computer to another. Predictably, bulletin board software has been one of the main tools for making these transfers. Equally predictably, some of these copies have infringed on copyrights. There are four reported cases involving copyright infringement by users of computer bulletin boards. In these cases, courts have disagreed about which theory of liability to use in determining when computer owners are liable for their users' copyright infringement. Two courts found the computer owner liable for direct infringement. The court in the third case held that the computer owners were not liable for direct or vicarious infringement but found that, as to contributory infringement, the sufficiency of the defendants' knowledge had to be determined at trial. The fourth court granted summary judgment to the copyright owner. After finding the computer owner liable for contributory infringement, the court explicitly denied liability based on direct infringement and did not consider vicarious infringement.

The facts in the first two cases and the fourth case are nearly identical. In each case, several copies of copyrighted material (pictures from Playboy, software utility programs, and game software, respectively) were posted on a particular BBS. Each BBS had a computer owner who operated the system and controlled the BBS. Each BBS also had numerous users capable of uploading and downloading posted messages. In none of these cases was there any evidence that the computer owner had personally uploaded or downloaded any of the copyrighted material. In each case, however, the courts found the computer owner liable.

In *Playboy Enterprises, Inc v Frena* and *Central Point Software, Inc v Nugent*, two district courts each held the defendant liable for directly infringing on the copyright owner's exclusive right to distribute copies of its materials to the public. The *Playboy* court relied on the two-part test for copying, discussed above, that requires the plaintiff to prove that the defendant had access to the allegedly infringed work, and that the allegedly infringing work is substantially similar to the copyrighted

---

Footnotes:

74 See note 5.
77 839 F Supp 1552, 1559 (M D Fla 1993).
78 903 F Supp 1057, 1060 (E D Tex 1995).
79 See notes 45-47 and accompanying text.
work. Finding the test satisfied, the court explained that "[t]here is no dispute that Defendant Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies itself [sic]." Similarly, the Nugent court held that the discovery of a copy of a software program on a BBS was sufficient evidence of a copyright infringement to hold the BBS owner liable for direct infringement. Unlike the defendant in Playboy, however, the Nugent defendant did not challenge the plaintiff's allegation that the defendant himself reproduced the infringing copies of the copyrighted material.

In the third case, Religious Technology Center v Netcom Online Communication Services, Inc, a district court reached the opposite conclusion from the first two courts to consider the issue. In Netcom, Dennis Erlich, a critic of the Church of Scientology, posted copies of copyrighted Church documents to the USENET newsgroup alt.religion.scientology. Erlich did this by posting the pirated copies to a BBS, where they were automatically copied onto Netcom's computer, which then automatically copied them within hours to thousands of other Usenet servers around the world. The court held that neither the BBS nor Netcom were liable for direct infringement of any copyrights because neither took any affirmative action that directly resulted in the copying of the copyrighted material. Indeed, the defendants' only activity—installing and maintaining software that automatically reproduced all user postings—was the minimum necessary to operate a working computer bulletin board. Thus, the court distinguished the instant case from Playboy, explaining that "some element of volition or causation" by the computer owner was a prerequisite for liability for direct infringement.

The Netcom court then examined the question of contributory infringement. Applying the two-part test established in Gershwin, the court held that both Netcom and the BBS substantially participated in the infringement because both provided

---

80 Playboy, 839 F Supp at 1556.
81 Id.
82 Nugent, 903 F Supp at 1060.
84 Id at 1368-69.
85 Id at 1368. One defendant owned and operated a BBS; the other was an Internet access provider.
86 Id at 1370-71. The Netcom court did not specifically address the Nugent decision. This might reflect the fact that Nugent was announced only two months before Netcom and was decided in a district court in a different circuit.
87 Netcom, 907 F Supp at 1370.
88 See text accompanying notes 64-65.
a service allowing for the automatic distribution of all bulletin board postings, infringing and noninfringing. However, the court also found that there was a genuine issue as to whether Netcom or the BBS had actual or constructive knowledge of the infringement. Although neither had knowledge of Erlich’s infringement prior to receiving written notice from the copyright owner, the court found a question of fact as to whether the defendants “knew or should have known” of the continuing infringement after they received the plaintiff’s letter. The court further found that Netcom and the BBS should be permitted a reasonable amount of time after receiving the letter to investigate whether Erlich had a fair use defense, and that a jury would need to determine what constituted a reasonable amount of time. With this ruling, the court effectively created a new test for what constitutes “knowledge” sufficient for contributory infringement.

Finally, the court examined the question of vicarious infringement. The court found that a question of fact existed as to whether the computer owners had control over Erlich’s actions, thereby satisfying the “control” prong of the vicarious infringement test. The evidence showed that Netcom had suspended subscribers’ accounts on over one thousand occasions, for commercial advertising, obscene postings, and off-topic postings. Furthermore, the evidence showed that Netcom could delete specific postings. The court explained that “[w]hether such sanctions occurred before or after the abusive conduct is not material to whether Netcom can exercise control.” Despite the evidence of control, however, the court declined to find vicarious infringement because the plaintiff failed to show a “direct financial benefit” under the second prong of the test. In determining that the access fees paid by customers to Netcom and the BBS were not a direct financial benefit, the court relied on the district court’s

---

90 Netcom, 907 F Supp at 1375.
91 Id at 1374-75.
92 Id. See also note 14.
93 The implications of this ruling are potentially profound. If courts allow computer owners a reasonable amount of time to investigate the fair use defense, they are actually requiring the computer owner both to investigate the copyright and to decide whether or not the standard for fair use is met. Essentially, the computer owner will have to develop a quasi-judicial system, as described by John Perry Barlow in his “Declaration of Independence of Cyberspace,” in which he calls for self-rule for the Internet. Catherine Yang, Law Creeps onto the Lawless Net, Business Week 58 (May 6, 1996).
94 Netcom, 907 F Supp at 1376. See also text accompanying note 52.
95 Id.
96 Id at 1376-77. See also text accompanying note 52.
opinion in *Fonovisa, Inc v Cherry Auction, Inc*, the swap meet case which held that entrance fees were not a financial benefit.96

The district court's holding in *Fonovisa* was reversed by the Ninth Circuit after the *Netcom* decision was reached.97 The reversal was based on the financial benefit prong of the test, which the appellate court concluded had been met.98 Although at first glance it might look like this would require the reversal of *Netcom* as well, it is not at all clear that a few postings of Church of Scientology materials among tens or hundreds of thousands of other newsgroup postings coming in at about the same time would satisfy the *Fonovisa* requirement that the infringing activity enhance the attractiveness of the venue or act as a "draw" for potential customers.99

In the fourth case, *Sega Enterprises Ltd v Maphia*, a district court granted a summary judgment against a BBS owner for contributory infringement. The court adopted the reasoning of *Netcom*.100 The court found that the defendant knew or had reason to know of the infringing activity by users. The court noted that "evidence of a screen printout of user uploading and downloading statistics from the Maphia BBS show[ed] that [the computer owner] tracked, or at least had the ability to track, user uploads and downloads."101 The court also found that the computer owner provided the facilities for copying the copyrighted material. Evidence showed that the BBS was "a central depository site for the unauthorized copies of games, and allowed subsequent distribution of the games by user downloads."102 The court explicitly denied liability based on direct infringement and stated that the plaintiff had "not shown that Sherman himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur."103 The court did not consider vicarious infringement, stating that "[b]ecause the Court finds that Sega has

97 See *Fonovisa, Inc v Cherry Auction, Inc*, 76 F3d 259 (9th Cir 1996). For a discussion of *Fonovisa*, see text accompanying notes 60-61.
98 Id at 263.
99 Id.
100 In a previous decision on a preliminary injunction, the *Sega* court found that the plaintiff had established a prima facie case of direct infringement. The court did not address the lack of evidence showing that the defendant actually caused the copying to occur. Subsequently, the *Netcom* court concluded that plaintiffs also have to prove "some element of volition or causation" in order to establish direct infringement. *Netcom*, 907 F Supp at 1370. The *Sega* court cited *Netcom* and found its reasoning persuasive. *Sega*, 1996 US Dist LEXIS 20385 at *21.
102 Id at *25.
103 Id at *21.
established a prima facie case of contributory copyright infringement liability, it need not address whether Sherman is also liable under the theory of vicarious liability." Therefore the court did not consider how the reversal of Fonovisa would affect the application of vicarious infringement.

IV. APPLYING INFRINGEMENT THEORIES TO COMPUTER OWNERS

As the reader will recall, there are three policy arguments the courts have considered when applying the vicarious and contributory theories of infringement: (1) balancing the competing interests of copyright owners with the rights of others to freely engage in unrelated areas of commerce, (2) spreading monitoring and enforcement costs among computer users, and (3) putting responsibility where the control is. Based on these concerns, this Comment argues that computer owners should be subject to vicarious and contributory infringement, rather than direct infringement, when their users post pirated material.

A. Direct Infringement

Although two of the BBS cases found the owner of the BBS liable for direct infringement, these holdings do not withstand close scrutiny. While the courts ostensibly applied the direct infringement standard, which requires the plaintiff to prove ownership of a valid copyright and copying by the defendant, neither of the plaintiffs presented any evidence that the BBS owner had in fact copied the protected works.

The Playboy court applied the two-part test for copying, which merely requires the plaintiff to prove that the defendant had access to the copyrighted material, and that there is a substantial similarity between the copyrighted material and the allegedly infringing work. In the BBS context, this test is overbroad. Evidence that a copy exists in or near a copying machine does not indicate that the owner was any more or less likely to have created the copy than were his customers. For example, many universities, libraries, and copy shops make photocopying equipment available to the public. Often these machines are coin operated and unsupervised. If courts strictly applied the two-part

1997] Computer Network Copyright Infringement

---

104 Id at *26.
105 See text accompanying note 4.
106 See text accompanying note 55.
107 See text accompanying note 53.
108 See text accompanying note 45.
109 See text accompanying note 47.
test for copying, any plaintiff who found an infringing copy of its copyrighted material near a photocopying machine could meet the test for holding the university, library, or copy shop liable for direct infringement.

The Nugent decision is less problematic than Playboy. The Nugent court accepted the plaintiff's allegation that the defendant had copied the copyrighted material after the defendant failed to rebut it. However, Nugent is minimally persuasive given that the case was not fully litigated.

As both the Netcom and Sega courts observed, some element of volition or causation by the computer owner should be required before courts find that a computer owner directly infringed a copyright. As another court observed about dance halls (which are similar to computer bulletin boards), "[i]n cases involving live performances by musicians or disc jockeys ... the only bases for liability of the nightclub owner are vicarious and contributory liability, because the owner is not performing the work. Only the actual performer—the musician or the disc jockey—is a direct infringer."

Although there will certainly be cases in which computer owners directly infringe copyrights, courts should apply only the vicarious and contributory infringement standards to computer owners where the user causes the actual infringement. If the courts hold computer owners directly liable for their users' infringement, they may cause all computer networks, including the Internet, to shut down rather than bear the risk of the potentially vast liability. Alternatively, computer owners could review every message before allowing it onto their computers, dramatically increasing the cost of operating or participating in a network. Furthermore, as the Supreme Court observed, courts need to strike a balance between a copyright holder's legitimate demand for effective protection and the rights of others to freely engage in "substantially unrelated areas of commerce." Direct infringement would not balance these interests because it effectively would put the entire burden on computer owners. In contrast to the direct infringement theory, both the vicarious and contributory infringement tests strike a better balance between

---

10 Nugent, 903 F Supp at 1060.
11 Id.
12 Netcom, 907 F Supp at 1370.
13 See Part IV.B for a more complete discussion of this point.
15 Sony, 464 US at 442. See also Kaplan, Unhurried View at vii-viii (cited in note 2).
the rights of the copyright owner and the rights of society to use computer networks because these two tests only require computer owners to take precautions against the more obvious, and therefore more easily policed, infringements.

B. Vicarious Infringement

The Netcom court is the only court to have addressed the liability of computer owners in terms of vicarious infringement. Applying the two-part vicarious infringement test, the court found that computer owners have "control" over the actions of their users because they can suspend the accounts of the direct infringers, and can delete infringing messages.116 The Netcom court also found that the computer owners did not receive a "direct financial benefit" from the infringing activity.117

Three basic arguments counsel for application of a vicarious infringement standard to computer owners. The first is that it creates incentives for property owners to police the activities of invitees and to exercise the control they have to stop the infringing activity. Second, owners of the means of communication are better able to spread these costs among the users of the computer networks. Finally, in applying copyright law to new technologies, it is important for courts to balance the interests of copyright owners with society's interest in exploiting the potential of electronic communications.

Given these policy considerations, the most fitting analogy for computer owners comes from the dance hall cases. Both dance hall owners and computer owners have control over the actions of their users and receive a financial benefit from entrance or access fees. The best way to balance the interests of copyright owners with society's interests is to require that plaintiffs provide evidence indicating the frequency, quantity, and value of pirated copies on the defendant's computer. The factfinder could then use this information to determine whether the amount of infringement was sufficient to act as a "draw" for customers.

1. Control over the actions of others.

Although two commentators have concluded that landlords are a good analogy to computer owners,118 dance hall owners are

116 Netcom, 907 F Supp at 1376.
117 Id at 1377.
118 Kelly Tickle, Comment, The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards, 80 Iowa L Rev 391 (1995) (arguing that vicarious liability model should be used for bulletin boards and
a better analogy. Both writers argue that the computer owners lack sufficient control over the bulletin boards. However, both commentators acknowledge that it was possible for computer owners to monitor and stop infringing activity, but argue that the costs would be prohibitive. However, neither commentator was able to cite a single case in which the courts took into consideration the costs of controlling the activities of invitees. Furthermore, the monitoring cost might be far lower than either of the two commentators considered.

Computer owners have control because they can suspend subscribers' accounts, delete specific postings, change a user's password, or restrict a user's access to files and programs. Computer owners also have control because they can require that postings (such as postings which are particularly large, contain pictures, or have software programs attached) be reviewed by the computer owner before they are posted on bulletin boards.

that the best analogy is the landlord-tenant relationship); M. David Dobbins, Note, Computer Bulletin Board Operator Liability for Users' Infringing Acts, 94 Mich L Rev 217 (1995) (advocating BBS operator liability for contributory infringement when operators have actual or constructive knowledge of infringement, but arguing against applying the vicarious infringement standard because operators do not have control).

Tickle argues that “Like the BBS operator, the landlord has limited control over the activities occurring in the leased property.” Tickle, Comment, 80 Iowa L Rev at 417 (cited in note 118); Dobbins concludes that: “The control requirement essential to the application of vicarious liability does not exist in the case of a bulletin board operator because an operator lacks practical control over the user's activity.” Dobbins, Note, 94 Mich L Rev at 227 (cited in note 118).

See Tickle, Comment, 80 Iowa L Rev at 417 (cited in note 118) (“The BBS operator, however, does not technically fit the facts of this model because the operator retains the ability to monitor the activities occurring on the bulletin board.”); Dobbins, Note, 94 Mich L Rev at 227 (cited in note 118) (“Although it might be possible for a bulletin board operator to prevent infringement by contemporaneously monitoring every upload and download to the bulletin board, requiring such control would be unrealistic and burdensome.”).

Computer networks are unique because digital information can be searched very quickly and inexpensively by computers. For example, Alta Vista is a search engine on the Internet that anyone can easily access. It takes only a few seconds to search its database, which contains fifteen billion words indexed from over thirty million web pages.

Because search engines can use samples of copyrighted materials to identify all messages that match the sample, search engines can be used to inexpensively track down pirated material.

Spiders add the latest antipiracy weapon to the cybersleuth's armory. . . . [A spider] roams the Internet in search of words or phrases that its masters have reason to believe may have been illicitly borrowed. . . . 'So far we can only do text,' [the developer of one of the best-known spiders] says, 'but I'm changing it to do picture files as well. You could also look for digital watermarks.'

See Ross, Forbes at 139 (cited in note 9).

112 Netcom, 907 F Supp at 1375-76.
2. A direct financial benefit.

Computer owners are also similar to dance hall owners insofar as both gain financial benefits from charging their customers access fees. Just as dance hall and swap meet owners—who are subject to liability for vicarious infringement—reap a profit by charging an entrance fee, so too do computer owners who gain by charging an access fee. Furthermore, dance hall owners attract customers by playing popular copyrighted songs. Similarly, computer owners attract customers and profits by providing access to useful copyrighted information.

Courts should apply the customer "draw" test described earlier to determine whether the computer owner has obtained a financial benefit. One could use the vicarious infringement standard to hold all computer owners liable for every instance of copyright infringement that appears on their computers. However, this would risk eliminating the direct financial benefit prong of the vicarious infringement standard. But it is important that the financial benefit prong be maintained. One of the principal rationales offered for the vicarious infringement test by the Shapiro court was that companies would create 'dummy' operations that would allow them to profit from infringement while escaping liability. If the computer owners are not profiting from the infringement, there is far less concern about the possibility of a dummy operation. However, if the computer owner is not making a profit from the infringement because he is running a free computer network, the monitoring costs might be prohibitive and might risk silencing free networks run by nonprofit organizations.

Under the customer "draw" test, the computer owner is not liable if the number of infringements is so minimal that customers are not "drawn." To implement this test, the courts could require the plaintiff to establish the number of infringements on

---

123 See text accompanying notes 58-62.
124 Shapiro, 316 F2d at 309.
125 Cash profits are the easy case. It is more problematic if the benefits a computer owner receives are reputations (that is, the owner becomes more popular because he allows copyright infringement, but does not charge for access). Alternatively, a university might enjoy an indirect financial benefit by providing access to students as an added benefit of enrollment (in which case the factfinder must decide if the infringement acted as a draw for prospective students).
126 This is similar to the concern over imposing monitoring costs on nonprofits for indecent speech. See ACLU v Reno, 929 F Supp 824, 846-49, 854 (E D Pa 1996), cert granted, 117 S Ct 554 (1996).
127 Artists Music, Inc v Reed Publishing (USA), Inc, 31 USPQ2d 1623, 1627 (S D NY 1994).
the defendant’s computer. The factfinder would then determine whether the infringing activity alleged in the case was a big enough “draw” to attract customers.

For example, it is possible that on the facts in Netcom, the factfinder would have decided that one or two postings of Church of Scientology documents did not constitute a “draw” for users, because there are over one hundred thousand postings a day on Netcom’s network, which is a part of the Internet. By contrast, consider the newsgroup alt.binaries.pictures.erotica, one of the ten most popular newsgroups on the Internet. At least one book has described it as having “gigabytes of copyright violations.” Although the computer owners do not profit directly from having users visit this newsgroup, they profit by having customers subscribe to their services, much like dance halls that play popular songs profit from entrance fees. If computer owners do not provide access to these popular newsgroups, they will likely lose customers.

The customer “draw” test distinguishes between cases where there are only one or two infringements and cases where there are thousands of infringements. The customer “draw” test would take into account not only the financial value of the pirated materials, but also the frequency and volume of the piracy. If computer owners are held vicariously liable for every copyright infringement on their computers, they might be forced to monitor every single message posted on their system. Given the tremendous daily volume of postings, the monitoring costs imposed on computer owners would be prohibitive. A monitoring requirement thus would undermine the greatest advantage of computer networks: inexpensive mass communication through automated copying and distribution of information. However, if computer owners only have to monitor for infringement sufficient to constitute a “draw,” monitoring costs will be reduced substantially.

C. Contributory Infringement

There are three reasons why computer owners should be held liable if they have constructive knowledge of infringement by their users. First, holding computer owners liable for con-

---

128 Hoye, Phoenix Gazette at C1 (cited in note 34).
129 See Braun, The Internet Directory at #306 (cited in note 10).
130 It may be possible that at least for some types of materials computer owners could buy licenses from such organizations as ASCAP and BMI.
131 Only a few courts have applied the constructive knowledge standard to contributory infringement. See, for example, Sony Corp of America v Universal City Studios, Inc, 464 US 417, 442 (1984) (considering what proportion of the uses of a copying machine must be
tributory infringement only when they have actual knowledge does not strike an appropriate balance between the competing interests. Although an actual knowledge requirement would lessen the monitoring burden on computer owners, it would substantially increase the burden on copyright owners, who might have to discover and give notice of infringement before computer owners could be held liable. Second, by applying a constructive knowledge standard, the courts would place the responsibility for infringement on computer owners, who can effectively exercise control over their computers. Third, as noted earlier, computer owners are in a better position to spread the costs among the users of computer networks than copyright owners.

Holding computer owners liable for contributory infringement based on the owners' constructive knowledge encourages computer owners to monitor their users efficiently, but it does not hold owners liable for every infringement on their computers. Courts might use any of four constructive knowledge standards, described below, to distinguish between cases where there are few incidents of piracy and cases where there are thousands. These tests will discourage widespread piracy on computer networks, while allowing de minimis "innocent" infringement.

Under the first standard, an individual has constructive knowledge when a product has a particular trait or characteristic indicating that it was probably pirated. The second standard provides that a defendant has constructive knowledge when a pattern of possibly illegal activity gives him notice that the pattern is likely to continue unless he takes precautions. The third

---

For example, when a computer owner finds a copy of a new software program that can be downloaded for free from a bulletin board (while it is still being sold in the stores), he or she is put on notice that the software is pirated. See Screen Gems-Columbia Music, Inc v Mark-Fi Records, Inc, 256 F Supp 399, 404-05 (S D NY 1966) (low price of records raised fact issue as to piracy); R & R Recreation Products Inc v Joan Cook Inc, 25 USPQ2d 1781, 1784 (S D NY 1992) (failure to put agreement in writing, and sending checks for profits without a cover letter raised fact issue as to infringement); Universal City Studios, Inc v American Invesco Mgmt, Inc, 217 USPQ 1076, 1077 (N D Ill 1981) (purchase of a video of a movie released in the theaters only a few days before raised fact issue as to piracy); Ez-Tixz, Inc v Hit-Tix, Inc, 919 F Supp 728, 732 (S D NY 1996) (although disputed issues of fact precluded summary judgment, constructive knowledge found sufficient to establish liability).

For example, the fact that some newsgroups like alt.binaries.pictures.erotica have a "reputation" for having gigabytes of copyright violations would put the computer owner on notice. See note 10 and accompanying text. See also Fletcher v Baltimore & Potomac R.R. Co, 168 US 135, 139 (1897) (finding railroad may be liable for actions of railroad employees who threw firewood from train and injured pedestrian); Francis T. v Village Green Owners Assn, 42 Cal 3d 490, 229 Cal Rptr 456, 462 (1986) (holding that defendant
standard finds constructive knowledge when an individual creates an opportunity for another person to commit a foreseeable tort.\textsuperscript{134} Finally, the courts should consider creating a fourth constructive knowledge standard applicable only to computer networks that would make them liable for any pirated material on their computer systems for which a sample is readily available.\textsuperscript{135}

CONCLUSION

Computer networks are undoubtedly one of the most influential innovations of the twentieth century. They make cheap mass communication available to anyone with access to a computer. In particular, the Internet may well be “the most participatory form of mass speech yet developed.”\textsuperscript{136} However, computer networks can also be used to undermine the entire system of copyright law because they make copyright piracy much easier, cheaper, and safer. This Comment argues that the existing legal standards for vicarious and contributory infringement can be used to put a reasonable burden on the owners of computer networks to stop widespread and systematic piracy on their systems.

This Comment concludes that computer owners should be held liable for vicarious and contributory infringement for three reasons. First, these theories of liability balance the interests of

\textsuperscript{134} For instance, this constructive knowledge standard could be applied to the owners of anonymous remailers. Anonymous remailers create an opportunity for pirating copyrighted materials by allowing individuals to escape responsibility for their actions. See Restatement (Second) of Torts §§ 448, 449 (1966); Johnston v Harris, 387 Mich 569, 198 NW2d 409, 410-11 (1972) (holding landlord could be liable for injuries to tenant because landlord failed to provide adequate lighting and locks in a high-crime district); Kush v City of Buffalo, 59 NY2d 26, 462 NYS2d 831, 833-34 (1983) (holding school liable because it did not adequately safeguard explosive chemicals which, after being stolen, injured the plaintiff); Francis T., 229 Cal Rptr at 462; Russo v Grace Inst, 546 NYS2d 509, 512, 145 Misc 2d 242 (1989) (finding that builder and property owner could be liable for criminal attack on tenant because builder erected scaffolding around adjacent building, neglected to post a guard, and burglars entered tenant’s apartment via scaffolding).

\textsuperscript{135} See note 121.

copyright owners with society's interest in using computer networks. These theories would hold the computer network owners liable for widespread or systematic copyright infringement, but they would not hold them liable for de minimis “innocent” infringement.

Second, computer owners are in the best position to distribute any monitoring and enforcement costs across the users of computer networks. These users should bear the cost because they benefit from the same network that makes piracy much easier. By contrast, copyright owners are only able to distribute costs among purchasers of legitimate copies.

Third, a burden should be placed on the computer network owners because they control the computers and are therefore in a position to stop the piracy. Furthermore, computer network owners profit from the piracy when it attracts customers.

Applying the vicarious and contributory infringement standards to computer owners will accomplish all three of these goals. Both tests are necessary—for instance, vicarious infringement is unlikely to apply to computer owners who allow others to use their computers without charging a fee. On the other hand, for computer networks that are run for profit, vicarious infringement probably creates a greater duty to monitor than does contributory infringement. Therefore, even though the two tests will often overlap, they will each affect computer owners' behavior in slightly different ways and should both be applied.

137 For example, universities, libraries, non-profit hobbyists, and employers who provide access to the Internet for their employees.