The Information Highway Patrol: Here Come the Cyercops

Claire Ann Koegler

*
The Information Highway Patrol: Here Come the Cybercops*

Claire Ann Koegler**

As communications on the Internet become more and more a part of American culture, the law is evolving to regulate activities on the Internet ("Net"). Various government agencies and private entities are patrolling the Net to crack down on tortious and criminal activities.

In substance, these cyberspace activities are no different than activities in person, by mail, by telephone, by broadcast, or by print publication. Thus, government agencies patrolling the Net are seeing garden variety fraud, gambling, and securities violations, while private entities are seeing the usual copyright and trademark infringement, libel, and the like.

The message is the same only the medium is different. Thus, the courts have been applying preexisting substantive law to tortious and criminal conduct in this new medium. In some cases, Congress has amended statutes to include expressly Net activities.

A. An Introduction to the Net

The Net evolved from a computer system built a quarter of a century ago by the Department of Defense to enable academic and military researchers to continue to do government work even if part of the network were taken out by a nuclear blast. From its inception, it steadily grew to link universities, government facilities, and corporations around the world. The people given access to it soon learned that it was useful for more than official business, and thus e-mail and bulletin boards were born.1

From four host computers in 1969, the Net had grown to over one million computers by 1993 and was approaching ten million in 1996.2 There

---


** Attorney-at-Law, West Orange, New Jersey. The author is in private practice, concentrating in intellectual property and related matters.


were an estimated forty million users worldwide as of 1996; that number is expected to reach 200 million by 1999.3

"The Internet is a vast international network of networks that enables computers of all kinds to share services and communicate directly, as if they were part of one giant, seamless, global computing machine."4 The Net might be analogized to the system of interstate highways—many different routes to many different places. In this analogy, access providers are the companies that operate entrance ramps to the Net, some with tollgates.5

Content providers come in a variety of forms.6 Some provide archives of documents and operate much as newsstands, bookstores, or libraries. Some provide bulletin board systems ("BBS") which permit subscribers to post documents thereon; some provide chat rooms where subscribers can "talk;" some sell goods over the Net. Content providers exercise varying degrees of control over the material made available at their sites.

Since no one owns or controls the Net, activity thereon is determined by the access providers, the content providers, and the subscribers and/or users. While subscribers and users are typically liable for their own actions (although possibly judgment proof), liability of access providers and content providers depends upon the existing substantive law and the facts of each case.

B. Common Carriers, Vendors, and Publishers

The rights and obligations of providers and of users under the law is determined not only by the substantive law, but also by the characterization of the parties, which can determine the duty owed by a certain defendant to a certain plaintiff. For example, local telephone companies are considered

3. Id.
5. Congress defines an "access software provider" as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." Id. § 230(e)(4). Access software providers are also "interactive computer services," such a service being defined as: "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." Id. § 230(e)(2).
6. Congress has defined an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Id. § 230(e)(3).
common carriers; they must provide access to those who want it. They have neither the right nor the obligation to oversee how users use their phone lines. Since they cannot control the content of telephone conversations or facsimile transmissions, they cannot be held liable for customers' libelous, infringing, fraudulent, or otherwise tortious or criminal conduct. 7

Publishers stand on a different footing. A newspaper is not required to print every story, commentary, or letter submitted. Thus, it has an obligation not to publish material that it knows or should know is tortious, such as libelous, infringing a copyright or a trademark, or the like. 8

Vendors, such as libraries, bookstores, and newsstands, cannot be held to the same standards as publishers. They cannot be expected to review material in their possession, nor is it in the public interest to have them act as censors. Such would have a chilling effect on free speech. 9

7. The copyright act has a common carrier exemption:

The secondary transmission of a primary transmission embodying a performance or display of a work is not an infringement of copyright if—

the secondary transmission is made by any carrier who has no direct or indirect control over the content or selection of the primary transmission or over the particular recipients of the secondary transmission, and whose activities with respect to the secondary transmission consist solely of providing wires, cables, or other communications channels for the use of others . . . .


8. The trademark act does contain an exemption for innocent infringement by publishers carrying paid advertisements:

Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication . . . , the remedies . . . shall be limited to an injunction against the presentation [of such advertising matter in future issues of] such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.


9. In reversing a bookseller's conviction under an obscenity statute which had no requirement of scienter, the United States Supreme Court explained:

By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public's access to constitutionally protected matter. For if the bookseller is criminally liable without knowledge of the contents, . . . he will tend to restrict the books he sells to those he has inspected . . . . If the contents of
C. Protected Speech and Unprotected Speech

While freedom of speech or expression is recognized as a fundamental right, some types of expression—seditious, obscene, and tortious—are subject to regulation or even prohibition. In regulating speech, the courts look to both the content and the context: "The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."10

D. Obscenity

Federal law prohibits the importation, interstate transportation, mailing, and broadcasting of obscene material.11 This prohibition includes dissemination via the Net.12

In 1978, the United States Supreme Court upheld the Federal Communications Commission's ("FCC") regulation of indecent but not obscene material in radio broadcasting.13 The case involved the midafternoon broadcast of George Carlin's "Filthy Words" monologue, preceded by a notice that the program would include language which might be offensive to some.14 In a variation on the content/context analysis, the FCC had likened offensive language to nuisance and determined that it should be channeled, not prohibited.15 Specifically, words depicting sexual and excretory activity should be aired at "times of day when children most likely would not be exposed to it."16 In upholding the regulation, the Court stated:

We have long recognized that each medium of expression presents special First Amendment problems. And of all forms of communication, it is broadcasting that has received the most

---

bookshops and periodical stands were restricted to material of which their proprietors had made an inspection, they might be depleted indeed.

14. Id. at 729.
15. Id. at 726.
16. Id. at 733 (quoting In re Matter of a 'Petition for Clarification or Reconsideration,' 59 F.C.C. 2d 892 (1976)).
limited First Amendment protection . . . First, the broadcast media have established a uniquely pervasive presence in the lives of all Americans. Patently offensive, indecent material presented over the airwaves confronts the citizen, not only in public, but also in the privacy of the home, where the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder. Because the broadcast audience is constantly tuning in and out, prior warnings cannot completely protect the listener or viewer from unexpected program content.

Second, broadcasting is uniquely accessible to children, even those too young to read. Although Cohen's [sic] written message might have been incomprehensible to a first grader, Pacifica's broadcast could have enlarged a child's vocabulary in an instant. Other forms of offensive expression may be withheld from the young without restricting the expression at its source. Bookstores and motion picture theaters, for example, may be prohibited from making indecent material available to children . . . . The ease with which children may obtain access to broadcast material . . . amply justifies special treatment of indecent broadcasting. 17

In Sable Communications of California, Inc. v. FCC, 18 the Court chronicled the attempts of the FCC and Congress to regulate dial-a-porn in the wake of the Pacifica decision. In 1982, Congress amended the Communications Act to criminalize providing, to those under eighteen years of age, indecent as well as obscene commercial telephone messages. 19 The FCC promulgated regulations providing defenses based on time channeling and credit card screening; the time channeling defense was set aside in Carlin Communications, Inc. v. FCC ("Carlin I") as "both overinclusive and underinclusive." 20 The FCC promulgated new regulations keeping the credit card screening defense and adding a user identification code defense; these regulations were set aside in Carlin II for failure to consider exchange blocking. 21 The FCC promulgated a new set of regulations keeping the two prior defenses and adding as a defense message scrambling; these regulations were upheld in Carlin III. 22 The court, however, struck down as

17. Id. at 748–50.
19. Id. at 120.
20. Id. at 121 (quoting Carlin Communications, Inc. v. FCC, 749 F.2d 113 (2d Cir. 1984) [hereinafter Carlin I]).
21. Id. at 121–22 (citing Carlin Communications, Inc. v. FCC, 787 F.2d 846 (2d Cir. 1986) [hereinafter Carlin II]).
22. Id. at 122 (citing Carlin Communications, Inc. v. FCC, 837 F.2d 546 (2d Cir. 1998), cert. denied, 488 U.S. 924 (1988) [hereinafter Carlin III]).
unconstitutional the attempt to regulate "indecent" as opposed to "obscene" speech.\textsuperscript{23} Thereafter, Congress amended the act to ban indecent as well as obscene commercial telephone messages, without regard to the age of the recipient,\textsuperscript{24} thus leading to the \textit{Sable} case. The United States Supreme Court upheld the constitutionality of the statute as applied to obscene speech but struck down as unconstitutional its application to indecent speech, distinguishing the case before it from \textit{Pacifica}:

The private commercial telephone communications at issue here are substantially different from the public radio broadcast at issue in \textit{Pacifica}. In contrast to public displays, unsolicited mailings and other means of expression which the recipient has no meaningful opportunity to avoid, the dial-it medium requires the listener to take affirmative steps to receive the communication . . . . Unlike an unexpected outburst on a radio broadcast, the message received by one who places a call to a dial-a-porn service is not so invasive or surprising that it prevents an unwilling listener from avoiding exposure to it.\textsuperscript{25}

One might have thought that Congress would have learned something from the \textit{Carlin} and \textit{Sable} cases. Apparently not. Since the terms "indecent" and "patently offensive" were undefined in the statute, Congress amended the act to restrict the dissemination of both obscene and "indecent" material by telecommunications devices and of "patently offensive" material by interactive computer services, to persons under eighteen years of age.\textsuperscript{26} These provisions were found facially unconstitutional by a three-judge district court, and their enforcement was preliminarily enjoined.\textsuperscript{27} The court distinguished accessing the Net from broadcasting: "Communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'\textsuperscript{28}

The court rejected the act's defenses of credit card verification, adult access codes, and adult personal identification numbers as not available for "noncommercial, not-for-profit entities."\textsuperscript{29} The court also rejected the government's proposal for "tagging" of indecent material to facilitate blocking, as it was extremely burdensome to content providers such as

\begin{itemize}
\item[23.] \textit{Sable}, 492 U.S. at 122.
\item[24.] \textit{Id.}
\item[25.] \textit{Id.} at 127–28.
\item[26.] 47 U.S.C.A. § 223(a)(1)(B), (d)(1) (West Supp 1998). Liability was extended to facilities providers who knowingly permitted such activities to occur. \textit{Id.} § 223(a)(2), (d)(2).
\item[28.] \textit{Id.} at 844.
\item[29.] \textit{Id.} at 849.
\end{itemize}
libraries, that might simply tag an entire site, thereby not reaching foreign
content providers.\textsuperscript{30}

The principles enunciated in the obscenity cases have been adapted and
applied in libel and infringement cases.

E. Defamation and Other Intentional Torts

\textit{Cubby, Inc. v. CompuServe Inc.}\textsuperscript{31} was an action for libel, business
disparagement, and unfair competition.\textsuperscript{32} CompuServe included an online
forum called the Journalism Forum managed by an independent contractor
who agreed to "'manage, review, create, delete, edit and otherwise control
the contents' of the Journalism Forum 'in accordance with editorial and
technical standards and conventions of style as established by
CompuServe.'"\textsuperscript{33} The allegedly false and defamatory statements appeared in
a daily newsletter available on the \textit{Journalism Forum}.\textsuperscript{34} Under the
applicable New York State law, "'one who repeats or otherwise republishes
defamatory matter is subject to liability as if he had originally published it,'"
however, "'vendors and distributors of defamatory publications are not liable
if they neither know nor have reason to know of the defamation.'"\textsuperscript{35}

The rationale for the distinction is the same as in the obscenity cases:
vendors and distributors cannot be expected to review all material in their
possession; imposing such a requirement would severely limit the material
available to the public, in contravention of the First Amendment.\textsuperscript{36} The
court found that CompuServe acted as a for-profit library, not a publisher:
"CompuServe has no more editorial control over such a publication than
does a public library, book store, or newsstand, and it would be no more
feasible for CompuServe to examine every publication it carries for
potentially defamatory statements than it would be for any other distributor
to do so."\textsuperscript{37} In addition, "'given the relevant First Amendment
considerations, the appropriate standard of liability to be applied to
CompuServe is whether it knew or had reason to know of the allegedly
defamatory Rumorville statements.'"\textsuperscript{38}

\textsuperscript{30. \textit{Id.} at 847–48.}
\textsuperscript{32. \textit{Id.} at 135.}
\textsuperscript{33. \textit{Id.} at 137.}
\textsuperscript{34. \textit{Id.} at 138.}
\textsuperscript{35. \textit{Id.} at 139 (citations omitted).}
\textsuperscript{36. \textit{Cubby,} \textit{776 F. Supp.} at 139–40.}
\textsuperscript{37. \textit{Id.} at 140.}
\textsuperscript{38. \textit{Id.} at 140–41. Since the plaintiffs failed to show an issue of fact regarding
CompuServe's knowledge, summary judgment was granted for CompuServe. \textit{Id.} at 142.
Stratton Oakmont, Inc. v PRODIGY Services Co.,\textsuperscript{39} was an action for libel based on statements on a PRODIGY bulletin board "Money Talk," alleging fraud by the plaintiffs in the sale of an initial public offering.\textsuperscript{40} In finding that PRODIGY acted as a publisher, the court noted: "PRODIGY held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and expressly likening itself to a newspaper."\textsuperscript{41} PRODIGY stated:

We make no apology for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly no responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate.\textsuperscript{42}

PRODIGY also promulgated content guidelines, electronically prescreened bulletin board postings for offensive language, used board leaders to enforce the guidelines, and provided board leaders with an emergency delete function to remove inappropriate postings.\textsuperscript{43} In entering summary judgment for the plaintiffs, the court distinguished Cubby:

Let it be clear that this Court is in full agreement with Cubby . . . . Computer bulletin boards should generally be regarded in the same context as bookstores, libraries and network affiliates. . . .

PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.\textsuperscript{44}

F. Intellectual Property Rights

Numerous companies are patrolling the Net to enforce their intellectual property rights. Paramount Pictures for years has been trying to stop the proliferation of Star Trek photographs, Elvis Presley Enterprises has ordered

\textsuperscript{39} No. 31063/94, 1995 WL 323710 (N.Y. Sup. May 24, 1995).
\textsuperscript{40} Id. at *1.
\textsuperscript{41} Id. at *2.
\textsuperscript{42} Id. (quoting Ex. J).
\textsuperscript{43} Id. at *2-3.
the removal of sound clips of Presley's recordings and photographs of Graceland from home pages, and Sony Music Entertainment has sent notices to Web page owners using Pearl Jam images. Many publishers are pushing for the passage of changes to the Copyright Act to define digital transmission as a form of publication, to include electronic coding of copyrighted material that would notify publishers when their material was copied, and to impose criminal penalties.

Playboy Enterprises has complained to a number of universities about students posting Playboy photographs. Playboy Enterprises, Inc. v. Frena was an action for copyright infringement, trademark infringement, and unfair competition, in which the court granted the plaintiff's motion for summary judgment. The defendant provided a bulletin board for subscribers to upload and download pictures from Playboy magazine. In holding that the defendant infringed the plaintiff's copyrights, including distributing copies of and publicly displaying the works, the court rejected Frena's defense that he was unaware of the copyright infringement, since "[i]ntent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement." The court also found trademark infringement of the marks Playboy and Playmate used to identify files, again rejecting Frena's defense that he did not intend to use the plaintiff's mark, since "a showing of intent or bad faith is unnecessary to establish a violation of § 1141(a)."

The Church of Scientology has been particularly vigilant in patrolling the use of its material on the Internet, with varying results. In Religious Technology Center ("RTC") v. Lerma, a former church member posted allegedly stolen church documents through Digital Gateway Systems and provided them to the Washington Post. After the court ordered return of the documents and seizure of Defendant Lerma's computer equipment, the Washington Post copied the documents from the court file, which was

46. Id.
47. Id.
49. Id. at 1563.
50. Id. at 1554.
51. Id. at 1556–57, 1559.
52. Id. at 1560–61. To the extent that Frena removed the Playboy trademarks and substituted his own identification, the court found the intent necessary for the claim of unfair competition based "on reverse passing off." Playboy, 839 F. Supp. at 1562.
54. Id. at 261–62.
subsequently sealed.\textsuperscript{55} The court rejected the Religious Technology Center's request to restrain publication by the Washington Post of an article based on the documents, stating that if "a threat to national security was insufficient to warrant a prior restraint" in the "Pentagon Papers" case,\textsuperscript{56} "the threat to plaintiff's copyrights and trade secrets is woefully inadequate."\textsuperscript{57} Moreover, RTC was unlikely to succeed on the copyright claim, due to the fair use exception,\textsuperscript{58} or on the trade secret claim, since the documents were in the public domain, having found their way onto the Net from sources in addition to the defendant.\textsuperscript{59} In a later opinion,\textsuperscript{60} the court rejected RTC's claim that the failure to restrain the publication violated the Free Exercise Clause. The court further declined to issue an injunction against Lerma or Digital Gateway Systems, based in part on RTC's unclean hands in executing the TRO against Lerma and, in part, on the decision of the Colorado District Court in a related case.\textsuperscript{61}

The Colorado case was factually the same, with a different set of defendants—FACTNET and two former church members who were members of FACTNET's board.\textsuperscript{62} The defendant in the Virginia case, Lerma, was also a member of FACTNET's board and had posted the information from the court files in the Virginia case on the FACTNET BBS.\textsuperscript{63} Like the Virginia court, the Colorado court found that the plaintiff was unlikely to succeed on the copyright claim, due to the fair use exception,\textsuperscript{64} or on the trade secret claim, since the documents were in

\footnotesize{
\begin{itemize}
\item \textsuperscript{55} Id. at 262.
\item \textsuperscript{56} See New York Times Co. v. United States, 403 U.S. 713 (1971).
\item \textsuperscript{57} Religious Tech. Ctr., 897 F. Supp. at 263. In a rare case, the court restrained publication of an article containing technical information regarding the construction of a hydrogen bomb, accepting the government's claim that it posed a threat to the national security: "A mistake in ruling against The Progressive will seriously infringe cherished First Amendment rights . . . . A mistake in ruling against the United States could pave the way for thermonuclear annihilation for us all. In that event, our right to life is extinguished and the right to publish becomes moot." United States v. Progressive, Inc., 467 F. Supp. 990, 996 (W.D. Wis. 1979). The issue apparently became moot when similar articles were published elsewhere.
\item \textsuperscript{58} Religious Tech. Ctr., 897 F. Supp. at 263 (citing 17 U.S.C.A. § 107 (West Supp. 1995)).
\item \textsuperscript{59} Id. at 266.
\item \textsuperscript{61} Id. at 1358, 1361 (citing Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519 (D. Colo. 1995)).
\item \textsuperscript{63} Id. at 1522.
\item \textsuperscript{64} Id. at 1525–26.
\end{itemize}
}
public domain, having found their way onto the Net from sources other than the defendant Lerma.\textsuperscript{65} The Scientologists found a friendlier environment in California, where a similar action for copyright infringement and trade secret misappropriation was brought against Netcom and Erlich, a former minister of the church, who had posted allegedly proprietary church documents on a Netcom bulletin board.\textsuperscript{66} In issuing a preliminary injunction against Erlich, the court found a likelihood of success on the copyright claim, since the fair use exception was not justified on the facts,\textsuperscript{67} but that RTC was unlikely to succeed on the trade secret claim, since the information had been posted on the Net by others:

\begin{quote}
The court is troubled by the notion that any Internet user, including those using "anonymous remailers" to protect their identity, can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made.\textellipsis While the court is persuaded by the Church's evidence that those who made the original postings likely gained the information through improper means ... this does not negate the finding that, once posted, the works lost their secrecy.\textsuperscript{68}
\end{quote}

In a later opinion,\textsuperscript{69} the court considered motions for summary judgment by the access provider, Netcom, and the BBS operator Klemesrud.\textsuperscript{70} The court rejected Netcom's attempts to use the common carrier exception to the Copyright Act:\textsuperscript{71}

\begin{quote}
Netcom compares itself to a common carrier that merely acts as a passive conduit for information. In a sense, a Usenet server that forwards all messages acts like a common carrier, passively retransmitting every message that gets sent through it. Netcom would seem no more liable than the phone company for carrying an infringing facsimile transmission or storing an infringing audio recording on its voice mail. As Netcom's counsel argued, holding such a server liable would be like holding the owner of the
\end{quote}

\begin{footnotes}
\item[65] Id. at 1526.
\item[67] Id. at 1249–50.
\item[68] Id. at 1256 (footnote omitted).
\item[70] Id. at 1361.
\end{footnotes}
highway, or at least the operator of a toll booth, liable for the
criminal activities that occur on its roads.\textsuperscript{72}

Nevertheless, the court found that Netcom could not be held liable as a direct
infringer:

The court does not find workable a theory of infringement that
would hold the entire Internet liable for activities that cannot
reasonably be deterred. Billions of bits of data flow through the
Internet and are necessarily stored on servers throughout the
network and it is thus practically impossible to screen out
infringing bits from noninfringing bits. Because the court cannot
see any meaningful distinction (without regard to knowledge)
between what Netcom did and what every other Usenet server
does, the court finds that Netcom cannot be held liable for direct
infringement.\textsuperscript{73}

However, the court found that Netcom might still be liable for contributory
infringement or vicarious infringement, since RTC notified Nettcom and
Klemesrud of the alleged infringement and Netcom took no action.\textsuperscript{74}

In Sega Enterprises Ltd. v. Maphia,\textsuperscript{75} the court entered a preliminary
injunction against copyright infringement, trademark infringement, and
unfair competition.\textsuperscript{76} The defendant provided a bulletin board for
subscribers to upload and download SuperNintendo and Genesis games.\textsuperscript{77} In
some cases, subscribers were charged a fee for downloading games.\textsuperscript{78} The
court found a prima facie case that the defendant directly and contributorily
infringed the plaintiff’s copyrights including making copies of the works,
noting that the defendant had knowledge of the copying.\textsuperscript{79} The court further
found a prima facie case of trademark infringement and of false designation

\textsuperscript{72. Religious Tech. Ctr., 907 F. Supp. at 1369 n.12.}
\textsuperscript{73. Id. at 1372–73.}
\textsuperscript{74. Id. at 1375. “Where a defendant has knowledge of the primary infringer’s infringing
activities, it will be liable if it ‘induces, causes, or materially contributes to the infringing
conduct of’ the primary infringer.” Id. “A defendant is liable for vicarious liability for the
actions of a primary infringer where the defendant (1) has the right and ability to control the
infringer’s acts and (2) receives a direct financial benefit from the infringement.” Id. As
against Klemesrud, the court found no direct infringement for the same reasons as Netcom, a
possibility of contributory infringement for the same reasons as Netcom, and insufficient
evidence on the issue of vicarious liability, due to a failure to allege a financial benefit.
\textsuperscript{75. 857 F. Supp. 679 (N.D. Cal. 1994).}
\textsuperscript{76. Id.}
\textsuperscript{77. Id. at 683.}
\textsuperscript{78. Id. at 683–684.}
\textsuperscript{79. Id. at 686–87.}
of origin based on the use of Sega's trademark on files and in the programs copied.

United States v. LaMacchia\(^8\) was a criminal action against a student at the Massachusetts Institute of Technology ("MIT") who had created a bulletin board in which correspondents were encouraged to upload popular applications software and computer games, which LaMacchia transferred to a second bulletin board from which subscribers could download the software.\(^9\) Because there was no showing of any financial benefit to LaMacchia, he could not be prosecuted under the criminal provisions of the Copyright Act.\(^10\) Accordingly, he was indicted under the federal wire fraud statute.\(^11\) The court determined that in enacting the Copyright Felony Act in 1992, Congress made a conscious decision to limit the extension of the felony provisions to criminal copyright infringement as defined in the Copyright Act,\(^12\) so as not to accidentally bring "a large percentage of the American people... into the gray area of criminal law."\(^13\) Accordingly, the court declined to extend the reach of the wire fraud statute to reach LaMacchia for fear of reaching "the myriad of home computer users who succumb to the temptation to copy even a single software program for private use."\(^14\)

G. **Fraud on the Net**

Much of the attention to the Net in the popular press has been directed to fraud on the Net. What makes fraud on the Net different from other schemes is the large volume of potential dupes that can be reached at low cost. Moreover, if the pitch is made on a bulletin board, rather than by e-mail, the dupes come to the con artist, not the other way around. However, unlike telephone solicitations, the Net leaves the equivalent of a paper trail, so it is easier to police these fraud schemes.

At the federal level, the Department of Justice has a computer crimes unit which investigates online crimes,\(^15\) the Federal Trade Commission

---

82. Id. at 536.
84. LaMacchia, 871 F. Supp. at 536, 540 (citing 18 U.S.C. § 1343 (1994)).
85. Id. at 540.
86. Id. at 544–45 n.18.
87. Id. at 544.
("FTC") monitors online advertising and commercial services, the Securities and Exchange Commission ("SEC") does not monitor advertising but does watch financial chatter in cyberspace. What they are finding are the same old scams.

The FTC shut down an Internet-based pyramid scam that allegedly took in six million based on a purported 2000 percent return on investment. Fortuna Alliance of Bellingham, Washington, ran the operations for seven months before the FTC obtained an injunction shutting down the scheme. Some three-and-a-half million went into an Antiguan account, which the injunction ordered Fortuna to return to the United States.

The SEC brought charges of fraud and sale of unregistered securities against Telephone Information Systems, touted on CompuServe as a telephone lottery, which the SEC considered to be a pyramid scheme. The SEC was also investigating Biosonics, who claimed to have medical devices that could cure everything from dry mouth to a dull sex life and was touted on an investment news group.

The Minnesota Attorney General’s Office, first by accident and later by design, has become a leader in bringing lawsuits based on illegal business activities on the Net and in organizing states attorney generals to do the same. In one case, a Las Vegas company had been charged with illegal bookmaking, by allowing bettors to place wagers on sporting events using the Net. The company sought to avoid United States laws by setting up its WagerNet bookmaking service in Belize. In another, a company was charged with false advertising relating to health claims related to the sale of germanium for acquired immune deficiency syndrome ("AIDS"), cancer, and other diseases. In yet another case, they are trying to find a defendant who offered bogus "credit repair" services over America Online and collected the payments at a private post office box in Georgia.

The New Jersey Attorney General’s Office was one of the first to create a team of "cyber cops" who regularly log onto the Net and the various

---

92. Id.
93. See Antilla, supra note 90, at 5.
94. Id.
95. See Ojeda-Zapata, supra note 88, at 52.
96. Id.
97. Id.
98. See Drag-Net 1995, supra note 89.
commercial online services to crack down on electronic pyramid schemes, e-mail chain letters, false advertising, and illegal business offerings. The New Jersey Bureau of Securities went after questionable investment opportunities on newsgroup bulletin boards and forums on PRODIGY, CompuServe, and American OnLine, which led to cease and desist orders against twenty individuals on PRODIGY for e-mail chain letters found to be in violation of New Jersey’s security laws.

Programs to create fraudulent credit card numbers, such as Credit Master, are circulating on America Online and numerous electronic bulletin boards on the Net. While less than five percent of the numbers they generate correspond to valid card numbers, the increasing ability to charge services by entering credit card numbers through phone or computer lines without verification permits potential use of such numbers. However, it is relatively easy for the police to find the users, since the merchandise ordered by phone or computer must be shipped to an address, which is how Nassau County New York police arrested four college students who went on a $100,000 buying spree.

H. Expanding Notions of Jurisdiction on the Net

While an in-depth analysis of jurisdiction is beyond the scope of this paper, some consideration is necessary. General jurisdiction exists when the defendant’s activities in the state are such as to amount to doing business in the state; specific jurisdiction exists when the cause of action sued upon arises in the state. A cause of action can be based on acts in the state or acts outside the state causing injury within the state, the latter being evaluated by the “effects test.” In any case, the defendant’s contacts with the state must be such that exercise of personal jurisdiction does not offend due process. These contacts can be evaluated by whether the defendant purposefully availed to the forum.

Previous cases have found jurisdiction based on direct mail solicitation and telemarketing. There are only a handful of cases considering jurisdiction based on Net transactions and the authority is split.

100. See Drag-Net 1995, supra note 89.
101. Id.
103. Id.
104. Id.
In *EDIAS Software International, L.L.C. v. BASIS International Ltd.*\(^{109}\), the plaintiff was an Arizona company who had contracted with the defendant New Mexico company for distribution of software products.\(^{110}\) In addition to the breach of contract claims, the plaintiffs alleged that the Internet messages gave "rise to claims for libel, defamation, tortious interference with contract" and unfair competition under the Lanham Act.\(^{111}\) After considering the extent of the defendant’s sales in Arizona for the "purposeful availment" test, the court considered the "effects test" in upholding jurisdiction: “BASIS directed the e-mail, Web page, and forum message at Arizona because Arizona is EDIAS' principle place of business. EDIAS allegedly felt the economic effects of the defamatory statements in Arizona.”\(^{112}\)

*CompuServe, Inc. v. Patterson*\(^{113}\) was a declaratory judgment action for non-infringement of common law trademarks.\(^{114}\) The defendant was a subscriber who provided shareware; he entered into an agreement with the plaintiff by computer transmission from his home in Texas to their computer in Ohio and thereafter transmitted software in a similar manner.\(^{115}\) The court found that the "purposeful availment" prong of the jurisdiction test was satisfied by the "stream-of-commerce" approach: "Patterson frequently contacted Ohio to sell his computer software over CompuServe’s Ohio-based system. Patterson repeatedly sent his 'goods' to CompuServe in Ohio for their ultimate sale. CompuServe, in effect, acted as Patterson's distributor, albeit electronically and not physically.”\(^{116}\)

*Panavision International, L.P. v. Toeppen*\(^{117}\) was a trademark infringement and antidilution action based solely on registration of a domain name for an Internet site.\(^{118}\) The court analyzed the case under the "effects test," found infringement at the plaintiff's principal place of business in California, and concluded that such was sufficient to satisfy the "purposeful

---

110. Id. at 414–15.
111. Id. at 415.
112. Id. at 420.
113. 89 F.3d 1257 (6th Cir. 1996).
114. Id. at 1259.
115. Id. at 1260–61.
116. Id. at 1265.
118. Id. at 619.
availment” prong of the jurisdiction test. The court denied that it was finding jurisdiction based on doing business via the Net.

In *Hearst Corp. v. Goldberger*, the magistrate recommended against jurisdiction in a trademark infringement action based solely on a web site:

Where, as here, defendant has not contracted to sell or actually sold any goods or services to New Yorkers, a finding of personal jurisdiction in New York based on an Internet web site would mean that there would be nationwide (indeed, worldwide) personal jurisdiction over anyone and everyone who establishes an Internet web site. Such nationwide jurisdiction is not consistent with traditional personal jurisdiction case law nor acceptable to the Court as a matter of policy.

Jurisdiction is the most problematic issue regarding regulation of activities on the Net. As recognized by the court in *ACLU v. Reno*:

Once a provider posts content on the Internet, it is available to all other Internet users worldwide. For example, when the UCR/California Museum of Photography posts to its Web site nudes to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing—wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site are available not just in Philadelphia, but also in Provo and Prague. A chat room organized by the ACLU to discuss the United States Supreme Court's decision in *FCC v. Pacifica Foundation* would transmit George Carlin's seven dirty words to anyone who enters.

This concern is not theoretical. CompuServe ran afoul of German laws against minors viewing sexually explicit material. CompuServe reacted by banning world wide access to such material, including access in the

---

119. *Id.* at 621-22.
120. *Id.* at 622.
124. *Id.* at 844.
United States, thereafter, it reactivated the access and made blocking software available to users in Germany.

I. Conclusion

Because the intention of the Net was decentralization, there is no hub, no control point, and no on/off switch. As such, it has been described as "the closest thing to true anarchy that ever existed." The thinking of the old guard is "access to computers should be unlimited and total," "all information should be free," and "mistrust authority and promote decentralization."

The recent rumblings inside the Beltway about the possible creation of an Internet Commerce Commission to regulate the Net is troubling to newbies as well as the old guard. People tend to do the jobs they are given to do. Thus, regulators regulate and legislators legislate.

Activities in cyberspace should receive neither less nor more protection under the law. So far, the courts have been doing a fine job of applying existing law to activities on the Net. Likewise, Congress has exercised admirable self-restraint in not over-legislating in this area. A continued wait-and-see approach as the law develops in the courts appears to be a wise one.

126. Id.
128. See e.g., Elmer-Dewitt, supra note 1, at 53.
129. Id.