Cyberspace Law
Professor Eric Goldman (formerly Eric Schlachter)
Santa Clara University School of Law
Spring 1998

MECHANICS

1. **MEETINGS.** The course meets Thursdays from 7:25 to 9:05 in Bannan Hall Room 139. The first class meets January 15 and the last class meets April 23. There will be no class on March 5. The final exam is scheduled for May 6 at 6:00 p.m.

2. **PREREQUISITES.** There are no prerequisites other than first year courses. Prior background in copyright law and First Amendment law may be helpful. If you do not have prior online experience, you will need to spend significant time during the semester to obtain online experience.

3. **GRADING.** The course will be graded solely on the final exam. The final exam will probably be 2½ hours long and consist of 3 questions. The exam will emphasize real life situations and problems. The prior two years' exams are included in the reader.

4. **PAPERS.** I would be happy to work with you on papers and articles. I have included a list of possible topics in the reader.

5. **EMAIL.** Any student who has not already done so should obtain an email account. I will attempt to establish a course email list for class announcements. Your contributions to the list will be welcome.

6. **CERTIFICATE PROGRAM.** This class is tentatively approved for credit towards the High Technology Law Certificate.

7. **PROFESSOR CONTACT INFORMATION.**

Eric Goldman (formerly Eric Schlachter)
Cooley Godward LLP
5 Palo Alto Square
3600 El Camino Real
Palo Alto, CA 94306
(650) 843-5154 (direct)
(650) 857-0663 (fax)
eschlach@netcom.com
READING MATERIALS

The only required book is this course reader. You may opt to procure one of the many cyberspace law books that are available on the market. In previous years, I have recommended Lance Rose's book NetLaw, but this book is out of date. Last year I also recommended Thomas Smedinghoff, Ed., Online Law: The SPA's Legal Guide to Doing Business on the Internet, which is more current than Lance's book but still out of date.

1. **INTRODUCTION TO CYBERSPACE (2½ weeks).**
   - ACLU v. Reno (district court) facts (page 14)
   - ACLU v. Miller (page 33)

2. **FORMING CONTRACTS ONLINE (½ week).**
   - Memo on forming clickthrough agreements (page 40)
   - ProCD v. Zeidenberg (page 42)
   - Hill v. Gateway 2000 (page 49)

3. **TRESPASS (½ week).**
   - CompuServe v. Cyber Promotions (page 53)

4. **COMMERCE CLAUSE (½ week).**
   - American Library Association v. Pataki (page 65)

5. **JURISDICTION AND VENUE (1 week).**
   - Zippo Manufacturing v. Zippo Dot Com (page 90)
   - Weber v. Jolly Hotels (page 99)
   - CyberSell v. CyberSell (page 105)

6. **ONLINE INFORMATION TORTS (1 week) (including defamation, rights of publicity/privacy, dissemination of inaccurate information, harassment and gambling).**
   - Missouri v. Interactive Gaming & Communications (page 113)

7. **OBSCENITY, PORNOGRAPHY AND CHILD PORNOGRAPHY (1 week).**
   - ACLU v. Reno (page 120)
   - US v. Thomas (page 146)
8. **TRADEMARKS AND DOMAIN NAMES** (1 week).

Intematic v. Toeppen (page 158)
Panavision v. Toeppen (3rd case) (page 176)
Lockheed Martin v. NSI (page 181)

9. **COPYRIGHT, TRADE SECRETS, PATENTS AND HOT NEWS** (2 weeks).


10. **SYSSP LIABILITY AND ACCESS** (2 weeks).

RTC v. Netcom (page 223)
CDA Section 509 (page 243)
Zeran v. America Online (page 246)
Cyber Promotions v. America Online (page 255)

11. **ECPA AND COMPUTER CRIMES** (½ week).

12. **OTHER RESOURCES**.

Spring 1996 Exam with Sample Answer (page 265)
Spring 1997 Exam with Sample Answer and High Scoring Answer (page 275)
Cyberspace Legal Topics (page 299)
CYBERSPACE LAW
TABLE OF CASES

By Eric Goldman (formerly Eric Schlachter)
Cooley Godward LLP
schlachtere@cooley.com

This document provides a non-comprehensive list of cases and other relevant source materials applicable to topics in cyberspace law. The last major set of revisions were made December 7, 1997.

1) AGENCY LIABILITY.

Blumenthal v. Drudge (complaint only) (D.D.C. September 1997),
Haybeck v. Prodigy Services Corp., 944 F. Supp. 326 (S.D.N.Y. November 12, 1996) (finding Prodigy not liable for an employee’s failure to tell a woman that he met in a Prodigy chat room that the employee had AIDS even though they engaged in unprotected sex).

2) ANONYMITY

http://www.imls.edu/cyber/statutes/ga-fraud.txt.
American Civil Liberties Union of Georgia v. Miller (N.D. Ga. June 20, 1997),
Bowker v. America Online (III. Circuit Court September 26, 1995) (complaint seeking AOL’s help in identifying the anonymous poster of an allegedly defamatory email) (complaint only),

http://cpsr.org/cpsr/free_speech/mcintyre.txt.

3) ANTITRUST.

Image Online Design, Inc. v. Internet Assigned Number Authority (complaint only) (Cal. Superior Court filed February 27, 1997), http://www.iodesign.com/complaint.html. Case was dismissed.
PGP Media, Inc. v. Network Solutions, Inc. (complaint only) (S.D.N.Y. March 20, 1997),

4) COMMERCE CLAUSE.


[cross reference California consumer protection statute and Nevada anti-spam statute]
5) **COMPUTER FRAUD AND ABUSE ACT.**

18 U.S.C. §1030 (last amended October, 11 1996),

6) **CONSUMER PROTECTION**

California Business & Professions Code §17538 (amended September 1996),

7) **CONTRACT.**

Also relevant: ProCD v. Zeidenberg, 89 F.3d 1257 (7th Cir. 1996), http://www.bna.com/e-law/cases/procd.html.

8) **COPYRIGHT.**


A & M Records v. Internet Site Known as Fresh Kutz (S.D. Cal. June 10, 1997) (TRO),
Expert Pages v. Universal Networks, Inc. (N.D. Cal. May 2, 1997) (TRO),
http://www.jmls.edu/cyber/cases/expert2.html.
Religious Technology Center v. Netcom On-Line Communications Services (N.D. Cal. September 22, 1995),
http://www.eff.org/pub/Legal/Cases/CoS_v_the_Net/whyte_cos_v_erlich_092295.ruling.
Religious Technology Center v. Lerma (E.D. Va. August 30, 1995),
http://www.eff.org/pub/Legal/Cases/CoS_v_the_Net/brinkema_RTC_washpost_083095.ruling.
http://www.eff.org/pub/Legal/Cases/Scientology_cases/brinkema_RTC_washpost_112895.opinion.

Also Relevant:
Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984),


9) **DEFAMATION.**


10) **ELECTRONIC COMMUNICATIONS PRIVACY ACT.**

The statute: [http://www.law.vill.edu/vcclp/fed_leg/ecpa.htm](http://www.law.vill.edu/vcclp/fed_leg/ecpa.htm).


11) **EMAIL PRIVACY.**


12) **GAMBLING.**


13) **HARASSMENT.**


14) **“HOT NEWS.”**

Also relevant: National Basketball Association v. Motorola, 105 F. 3d. 841 (2d Cir. 1997), [http://www.tourolaw.edu/2ndcircuit/January97/96-7975.html](http://www.tourolaw.edu/2ndcircuit/January97/96-7975.html).
15) **INACCURATE/HARMFUL INFORMATION**

http://snysside.sunnysside.com/cpsr_free_speech/daniel_v_dowjones.txt.
Also relevant: Rice v. Paladin Enterprises, 1997 U.S. Dist. LEXIS 30889 (4th Cir. November 10, 1997),

16) **JURISDICTION, VENUE AND CHOICE OF LAW.**

a) **Cases Involving General Jurisdiction.**

Smith v. Hobby Lobby Stores, 968 F. Supp. 1356 (W.D. Ark. 1997) (Hong Kong company not subject to
general jurisdiction in Arkansas because it advertised its website on advertising collateral).
over a company based solely on a “passive” advertising website), http://www.bna.com/e-
law/cases/weber.html.

b) **Cases Involving Specific Jurisdiction.**

i) **Defamation.**

Edias Software International LLC v. Basis International Ltd., 947 F. Supp. 413 (D. Az. Nov. 19,
September 24, 1997) (releasing allegedly defamatory press releases to Business Wire, which
apparently were distributed on the Internet, sufficient to support jurisdiction where the plaintiff was

ii) **Gambling.**

law/cases/granite.html.
Minnesota v. Granite Gate Resorts, 568 N.W. 2d 715 (Minn. Ct. App. September 5, 1997),

iii) **Miscellaneous.**

law/cases/cody.html.
Hall v. LaRonde, 66 Cal. Rptr. 2d 399 (Cal. Ct. App. August 7, 1997)
http://www.jmls.edu/cyber/cases/pres-kap.txt.
iv) Trademark.


CyberSell, Inc. v. CyberSell, Inc. (9th Cir. Dec. 2, 1997) (Florida website allegedly committing trademark infringement not subject to jurisdiction in Arizona when it was effectively a passive website and there was no purposeful availing of Arizona laws), http://caselaw.findlaw.com/cgi-bin/setcase.pl?court=9th&navby=case&no=9617087.


Hearst Corp. v. Goldberger, 1997 U.S. Dist. LEXIS 2065 (S.D.N.Y. February 26, 1997),


Transcraft Corp. v. Doonan Trailer Corp., 1997 U.S. Dist. LEXIS 18687 (N.D. Ill. November 17, 1997) (no specific jurisdiction over a vendor for trademark infringement based on a passive website, even if the website contained contact information).


c) Choice of Law.

d) Venue.


http://www.lawemory.edu/6circuit/jan96/96a0032p.06.html.
17) OBSCENITY/INDECENCY/CHILD PORNOGRAPHY.


Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997), http://www.law.emory.edu/10circuit/apr97/95-6245.wpd.html.
U.S. v. Chapman, 60 F.3d 894 (1st Cir. 1995).

Also relevant:

18) PATENT.

19) PRIVACY OF INFORMATION.

Letter regarding SpectraCom/Kidscom (FTC Bureau of Consumer Protection, July 15, 1997) (denying an enforcement action against a website collecting personal information from minors after the site had made FTC-requested changes), http://www.ftc.gov/os/9707/cenmed-1.htm.

20) PUBLICITY/PRIVACY RIGHTS.

21) **REGISTRANT LIABILITY.**

DataBase Consultants, Inc. v. Network Solutions, Inc. (N.D. Tex. Apr. 23, 1997) (Stipulation),
http://www.patents.com/real/real.sht.
Lockheed Martin Corp. v. Network Solutions, Inc. (C.D. Cal. March 19, 1997),

22) **SPAM AND TRESPASS.**

Nevada Senate Bill No. 13 (July 8, 1997), http://www.leg.state.nv.us/97bills/sb/sb13_en.htm.
Concentric Network Corp., Inc. v. Wallace (N.D. Cal. November 4, 1996) (Declaration),
http://www.jmls.edu/cyber/cases/lipsitz.html.
Tierney and Email America, Virtual Magistrate Project Docket No. 96-0001 (May 20, 1996),
http://www.jmls.edu/cyber/cases/typhoon2.html.

23) **STATE ACTION.**

24) SYSOP LIABILITY.

a) General.


b) Copyright.

Central Point Software, Inc. v. Nugent, 903 F. Supp. 1057 (E.D. Tex. 1995) (a quirky, underreported case which found the sysop liable for "reproducing" software solely because the files were on the sysop's system—without any allegation that the sysop loaded the files or knew they were there).

c) Defamation.


d) Other Torts.

Doe v. America Online, (Ct. Court Fla., June 26, 1997),

25) TRADEMARK/UNFAIR COMPETITION

a) Domain Names.

NSI Domain Name Dispute Policy (September 9, 1996), http://rs.internic.net/domain-info/internic-domain-6.html.
Establishment of a Memorandum of Understanding on the Generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU) (February 28, 1997), http://www.gtld-mou.org/gTLD-MoU.html.

http://www.Loudvy/CASES/ActMedia_v_Active_Media.html.
http://www.jmls.edu/cyber/cases/amerstan.html.
http://www.jmls.edu/cyber/cases/cardsvc1.txt.
http://www.jmls.edu/cyber/cases/juris1.html.
http://www.jmls.edu/cyber/cases/gw2000-1.txt.
Marks & Spencer plc v. One in a Million (High Court of Justice, Chancery Division, November 28, 1997),
http://www.nic.uk/judgment2.html.
http://www.jmls.edu/cyber/cases/toysrus1.txt.
b) Linking and Framing.

Insituform Technologies Inc. v. National Envirotech Group LLC (E.D. La. August 27, 1997),
http://www.cll.com/case1.htm
http://www.patents.com/ac/complain.sht
Playboy Enterprises, Inc. v. Calvin Designer Label (N.D. Cal. Sept. 8, 1997),

c) Other Trademark Uses.

CompuServe Inc. v. Cyber Promotions, Inc. (S.D. Ohio, October 24, 1996) (TRO),
http://www.jmls.edu/cyber/cases/cs-cp1.html.
Concentric Network Corp., Inc. v. Wallace (N.D. Cal. November 4, 1996) (Declaration),

26) TRADE SECRET.

http://www.eff.org/pub/Legal/Cases/Scientology_cases/brinkema_rtc_washpost_112895.opinion.
(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person --

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

(6) The [Federal Communications] Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d) of this section. Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures....

II. FINDINGS OF FACT

All parties agree that in order to apprehend the legal questions at issue in these cases, it is necessary to have a clear understanding of the exponentially growing, worldwide medium that is the Internet, which presents unique issues relating to the application of First Amendment jurisprudence and due process requirements to this new and evolving method of communication. For this reason all parties insisted on having extensive evidentiary hearings before the three-judge court. The court's Findings of fact are made pursuant to Fed. R. Civ. P. 52(a). The history and basic technology of this medium are not in dispute, and the first forty-eight paragraphs of the following Findings of fact are derived from the like-numbered paragraphs of a stipulation(8) the parties filed with the court.(9)

The Nature of Cyberspace

The Creation of the Internet and the Development of Cyberspace

1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. This is best understood if one considers what a linked group of computers -- referred to here as a "network" -- is, and what it does. Small networks are now ubiquitous (and are often called "local area networks"). For example, in many United States Courthouses, computers are linked to each other for the purpose of exchanging files and messages (and to share equipment such as printers). These are networks.

2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.

3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.
4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole.

5. The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET. This network linked computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. The network later allowed researchers across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. As it evolved far beyond its research origins in the United States to encompass universities, corporations, and people around the world, the ARPANET came to be called the "DARPA Internet," and finally just the "Internet."

6. From its inception, the network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links were damaged or otherwise unavailable. Among other goals, this redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war.

7. To achieve this resilient nationwide (and ultimately global) communications medium, the ARPANET encouraged the creation of multiple links to and from each computer (or computer network) on the network. Thus, a computer located in Washington, D.C., might be linked (usually using dedicated telephone lines) to other computers in neighboring states or on the Eastern seaboard. Each of those computers could in turn be linked to other computers, which themselves would be linked to other computers.

8. A communication sent over this redundant series of linked computers could travel any of a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a computer in Philadelphia, and then be forwarded to a computer in Pittsburgh, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.

9. Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses "packet switching" communication protocols that allow individual messages to be subdivided into smaller "packets" that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become overloaded, then packets can be re-routed to less loaded computers.

10. At the same time that ARPANET was maturing (it subsequently ceased to exist), similar networks developed to link universities, research facilities, businesses, and individuals around the world. These other formal or loose networks included BITNET, CSNET, FIDONET, and USENET. Eventually, each of these networks (many of which overlapped) were themselves linked together, allowing users of any computers linked to any one of the networks to transmit communications to users of computers on other networks. It is this series of linked networks (themselves linking computers and computer networks) that is today commonly known as the Internet.

11. No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage
location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.

How Individuals Access the Internet

12. Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular. In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a "personal computer" with a "modem" to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. As detailed below, both direct and modem connections are made available to people by a wide variety of academic, governmental, or commercial entities.

13. Students, faculty, researchers, and others affiliated with the vast majority of colleges and universities in the United States can access the Internet through their educational institutions. Such access is often via direct connection using computers located in campus libraries, offices, or computer centers, or may be through telephone access using a modem from a student's or professor's campus or off-campus location. Some colleges and universities install "ports" or outlets for direct network connections in each dormitory room or provide access via computers located in common areas in dormitories. Such access enables students and professors to use information and content provided by the college or university itself, and to use the vast amount of research resources and other information available on the Internet worldwide.

14. Similarly, Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet). Such access might be used by, for example, a corporation involved in scientific or medical research or manufacturing to enable corporate employees to exchange information and ideas with academic researchers in their fields.

15. Those who lack access to the Internet through their schools or employers still have a variety of ways they can access the Internet. Many communities across the country have established "free-nets" or community networks to provide their citizens with a local link to the Internet (and to provide local-oriented content and discussion groups). The first such community network, the Cleveland Free-Net Community Computer System, was established in 1986, and free-nets now exist in scores of communities as diverse as Richmond, Virginia, Tallahassee, Florida, Seattle, Washington, and San Diego, California. Individuals typically can access free-nets at little or no cost via modem connection or by using computers available in community buildings. Free-nets are often operated by a local library, educational institution, or non-profit community group.

16. Individuals can also access the Internet through many local libraries. Libraries often offer patrons use of computers that are linked to the Internet. In addition, some libraries offer telephone modem access to the libraries' computers, which are themselves connected to the Internet. Increasingly, patrons now use library services and resources without ever physically entering the library itself. Libraries typically provide such direct or modem access at no cost to the individual user.

17. Individuals can also access the Internet by patronizing an increasing number of storefront "computer coffee shops," where customers -- while they drink their coffee -- can use computers provided by the shop to access the Internet. Such Internet access is typically provided by the shop for a small hourly fee.

18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including the members of plaintiff Commercial Internet Exchange Association -- are commercial entities offering Internet access for a monthly or hourly fee. Some Internet service providers, however, are non-profit organizations that offer free or very low cost access to the Internet. For example, the International Internet Association offers free modem access to the
Internet upon request. Also, a number of trade or other non-profit associations offer Internet access as a service to members.

19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States.

20. In addition to using the national commercial online services, individuals can also access the Internet using some (but not all) of the thousands of local dial-in computer services, often called "bulletin board systems" or "BBSs." With an investment of as little as $2,000.00 and the cost of a telephone line, individuals, non-profit organizations, advocacy groups, and businesses can offer their own dial-in computer "bulletin board" service where friends, members, subscribers, or customers can exchange ideas and information. BBSs range from single computers with only one telephone line into the computer (allowing only one user at a time), to single computers with many telephone lines into the computer (allowing multiple simultaneous users), to multiple linked computers each servicing multiple dial-in telephone lines (allowing multiple simultaneous users). Some (but not all) of these BBS systems offer direct or indirect links to the Internet. Some BBS systems charge users a nominal fee for access, while many others are free to the individual users.

21. Although commercial access to the Internet is growing rapidly, many users of the Internet -- such as college students and staff -- do not individually pay for access (except to the extent, for example, that the cost of computer services is a component of college tuition). These and other Internet users can access the Internet without paying for such access with a credit card or other form of payment.

Methods to Communicate Over the Internet

22. Once one has access to the Internet, there are a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:

(1) one-to-one messaging (such as "e-mail"),
(2) one-to-many messaging (such as "listserv"),
(3) distributed message databases (such as "USENET newsgroups"),
(4) real time communication (such as "Internet Relay Chat"),
(5) real time remote computer utilization (such as "telnet"), and
(6) remote information retrieval (such as "ftp", "gopher," and the "World Wide Web").

Most of these methods of communication can be used to transmit text, data, computer programs, sound, visual images (i.e., pictures), and moving video images.

23. One-to-one messaging. One method of communication on the Internet is via electronic mail, or "e-mail," comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. E-mail on the Internet is not routed through a central control point, and can
take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).

24. One-to-many messaging. The Internet also contains automatic mailing list services (such as "listservs"), [also referred to by witnesses as "mail exploders"] that allow communications about particular subjects of interest to a group of people. For example, people can subscribe to a "listserv" mailing list on a particular topic of interest to them. The subscriber can submit messages on the topic to the listserv that are forwarded (via e-mail), either automatically or through a human moderator overseeing the listserv, to anyone who has subscribed to the mailing list. A recipient of such a message can reply to the message and have the reply also distributed to everyone on the mailing list. This service provides the capability to keep abreast of developments or events in a particular subject area. Most listserv-type mailing lists automatically forward all incoming messages to all mailing list subscribers. There are thousands of such mailing list services on the Internet, collectively with hundreds of thousands of subscribers. Users of "open" listservs typically can add or remove their names from the mailing list automatically, with no direct human involvement. Listservs may also be "closed," i.e., only allowing for one's acceptance into the listserv by a human moderator.

25. Distributed message databases. Similar in function to listservs -- but quite different in how communications are transmitted -- are distributed message databases such as "USENET newsgroups." User-sponsored newsgroups are among the most popular and widespread applications of Internet services, and cover all imaginable topics of interest to users. Like listservs, newsgroups are open discussions and exchanges on particular topics. Users, however, need not subscribe to the discussion mailing list in advance, but can instead access the database at any time. Some USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups,(10) all messages to the newsgroup are forwarded to one person who can screen them for relevance to the topics under discussion. USENET newsgroups are disseminated using ad hoc, peer to peer connections between approximately 200,000 computers (called USENET "servers") around the world. For unmoderated newsgroups, when an individual user with access to a USENET server posts a message to a newsgroup, the message is automatically forwarded to all adjacent USENET servers that furnish access to the newsgroup, and it is then propagated to the servers adjacent to those servers, etc. The messages are temporarily stored on each receiving server, where they are available for review and response by individual users. The messages are automatically and periodically purged from each system after a time to make room for new messages. Responses to messages, like the original messages, are automatically distributed to all other computers receiving the newsgroup or forwarded to a moderator in the case of a moderated newsgroup. The dissemination of messages to USENET servers around the world is an automated process that does not require direct human intervention or review.

26. There are newsgroups on more than fifteen thousand different subjects. In 1994, approximately 70,000 messages were posted to newsgroups each day, and those messages were distributed to the approximately 190,000 computers or computer networks that participate in the USENET newsgroup system. Once the messages reach the approximately 190,000 receiving computers or computer networks, they are available to individual users of those computers or computer networks. Collectively, almost 100,000 new messages (or "articles") are posted to newsgroups each day.

27. Real time communication. In addition to transmitting messages that can be later read or accessed, individuals on the Internet can engage in an immediate dialog, in "real time", with other people on the Internet. In its simplest forms, "talk" allows one-to-one communications and "Internet Relay Chat" (or IRC) allows two or more to type messages to each other that almost immediately appear on the others' computer screens. IRC is analogous to a telephone party line, using a computer and keyboard rather than a telephone. With IRC, however, at any one time there are thousands of different party lines available, in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects. Moreover, one can create a new party line to discuss a different topic at any time. Some IRC conversations are "moderated" or include "channel operators."

28. In addition, commercial online services such as America Online, CompuServe, the Microsoft Network, and Prodigy have their own "chat" systems allowing their members to converse.
29. Real time remote computer utilization. Another method to use information on the Internet is to access and control remote computers in "real time" using "telnet." For example, using telnet, a researcher at a university would be able to use the computing power of a supercomputer located at a different university. A student can use telnet to connect to a remote library to access the library's online card catalog program.

30. Remote information retrieval. The final major category of communication may be the most well known use of the Internet -- the search for and retrieval of information located on remote computers. There are three primary methods to locate and retrieve information on the Internet.

31. A simple method uses "ftp" (or file transfer protocol) to list the names of computer files available on a remote computer, and to transfer one or more of those files to an individual's local computer.

32. Another approach uses a program and format named "gopher" to guide an individual's search through the resources available on a remote computer.

The World Wide Web

33. A third approach, and fast becoming the most well-known on the Internet, is the "World Wide Web." The Web utilizes a "hypertext" formatting language called hypertext markup language (HTML), and programs that "browse" the Web can display HTML documents containing text, images, sound, animation and moving video. Any HTML document can include links to other types of information or resources, so that while viewing an HTML document that, for example, describes resources available on the Internet, one can "click" using a computer mouse on the description of the resource and be immediately connected to the resource itself. Such "hyperlinks" allow information to be accessed and organized in very flexible ways, and allow people to locate and efficiently view related information even if the information is stored on numerous computers all around the world.

34. Purpose. The World Wide Web (W3C) was created to serve as the platform for a global, online store of knowledge, containing information from a diversity of sources and accessible to Internet users around the world. Though information on the Web is contained in individual computers, the fact that each of these computers is connected to the Internet through W3C protocols allows all of the information to become part of a single body of knowledge. It is currently the most advanced information system developed on the Internet, and embraces within its data model most information in previous networked information systems such as ftp, gopher, wais, and Usenet.

35. History. W3C was originally developed at CERN, the European Particle Physics Laboratory, and was initially used to allow information sharing within internationally dispersed teams of researchers and engineers. Originally aimed at the High Energy Physics community, it has spread to other areas and attracted much interest in user support, resource recovery, and many other areas which depend on collaborative and information sharing. The Web has extended beyond the scientific and academic community to include communications by individuals, non-profit organizations, and businesses.

36. Basic Operation. The World Wide Web is a series of documents stored in different computers all over the Internet. Documents contain information stored in a variety of formats, including text, still images, sounds, and video. An essential element of the Web is that any document has an address (rather like a telephone number). Most Web documents contain "links." These are short sections of text or image which refer to another document. Typically the linked text is blue or underlined when displayed, and when selected by the user, the referenced document is automatically displayed, wherever in the world it actually is stored. Links for example are used to lead from overview documents to more detailed documents, from tables of contents to particular pages, but also as cross-references, footnotes, and new forms of information structure.

37. Many organizations now have "home pages" on the Web. These are documents which provide a set of links designed to represent the organization, and through links from the home page, guide the user directly or indirectly to information about or relevant to that organization.
38. As an example of the use of links, if these Findings were to be put on a World Wide Web site, its home page might contain links such as those:

- THE NATURE OF CYBERSPACE
- CREATION OF THE INTERNET AND THE DEVELOPMENT OF CYBERSPACE
- HOW PEOPLE ACCESS THE INTERNET
- METHODS TO COMMUNICATE OVER THE INTERNET

39. Each of these links takes the user of the site from the beginning of the Findings to the appropriate section within this Adjudication. Links may also take the user from the original Web site to another Web site on another computer connected to the Internet. These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique. The Web was designed with a maximum target time to follow a link of one tenth of a second.

40. Publishing. The World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information. When information is made available, it is said to be "published" on the Web. Publishing on the Web simply requires that the "publisher" has a computer connected to the Internet and that the computer is running W3C server software. The computer can be as simple as a small personal computer costing less than $1500 dollars or as complex as a multi-million dollar mainframe computer. Many Web publishers choose instead to lease disk storage space from someone else who has the necessary computer facilities, eliminating the need for actually owning any equipment oneself.

41. The Web, as a universe of network accessible information, contains a variety of documents prepared with quite varying degrees of care, from the hastily typed idea, to the professionally executed corporate profile. The power of the Web stems from the ability of a link to point to any document, regardless of its status or physical location.

42. Information to be published on the Web must also be formatted according to the rules of the Web standards. These standardized formats assure that all Web users who want to read the material will be able to view it. Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.

43. Web publishers have a choice to make their Web sites open to the general pool of all Internet users, or close them, thus making the information accessible only to those with advance authorization. Many publishers choose to keep their sites open to all in order to give their information the widest potential audience. In the event that the publishers choose to maintain restrictions on access, this may be accomplished by assigning specific user names and passwords as a prerequisite to access to the site. Or, in the case of Web sites maintained for internal use of one organization, access will only be allowed from other computers within that organization's local network.

44. Searching the Web. A variety of systems have developed that allow users of the Web to search particular information among all of the public sites that are part of the Web. Services such as Yahoo, Magellan, Altavista, Webcrawler, and Lycos are all services known as "search engines" which allow users to search for Web sites that contain certain categories of information, or to search for key words. For example, a Web user looking for the text of Supreme Court opinions would type the words "Supreme Court" into a search engine, and then be presented with a list of World Wide Web sites that contain Supreme Court information. This list would actually be a series of links to those sites. Having searched out a number of sites that might contain the desired information, the user would then follow individual links, browsing through the information on each site, until the desired material is found. For
many content providers on the Web, the ability to be found by these search engines is very important.

45. Common standards. The Web links together disparate information on an ever-growing number of Internet-linked computers by setting common information storage formats (HTML) and a common language for the exchange of Web documents (HTTP). Although the information itself may be in many different formats, and stored on computers which are not otherwise compatible, the basic Web standards provide a basic set of standards which allow communication and exchange of information. Despite the fact that many types of computers are used on the Web, and the fact that many of these machines are otherwise incompatible, those who "publish" information on the Web are able to communicate with those who seek to access information with little difficulty because of these basic technical standards.

46. A distributed system with no centralized control. Running on tens of thousands of individual computers on the Internet, the Web is what is known as a distributed system. The Web was designed so that organizations with computers containing information can become part of the Web simply by attaching their computers to the Internet and running appropriate World Wide Web software. No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web. From a user's perspective, it may appear to be a single, integrated system, but in reality it has no centralized control point.

47. Contrast to closed databases. The Web's open, distributed, decentralized nature stands in sharp contrast to most information systems that have come before it. Private information services such as Westlaw, Lexis/Nexis, and Dialog, have contained large storehouses of knowledge, and can be accessed from the Internet with the appropriate passwords and access software. However, these databases are not linked together into a single whole, as is the World Wide Web.

48. Success of the Web in research, education, and political activities. The World Wide Web has become so popular because of its open, distributed, and easy-to-use nature. Rather than requiring those who seek information to purchase new software or hardware, and to learn a new kind of system for each new database of information they seek to access, the Web environment makes it easy for users to jump from one set of information to another. By the same token, the open nature of the Web makes it easy for publishers to reach their intended audiences without having to know in advance what kind of computer each potential reader has, and what kind of software they will be using.

Restricting Access to Unwanted On-Line Material(12)

PICS

49. With the rapid growth of the Internet, the increasing popularity of the Web, and the existence of material online that some parents may consider inappropriate for their children, various entities have begun to build systems intended to enable parents to control the material which comes into their homes and may be accessible to their children. The World Wide Web Consortium launched the PICS ("Platform for Internet Content Selection") program in order to develop technical standards that would support parents' ability to filter and screen material that their children see on the Web.

50. The Consortium intends that PICS will provide the ability for third parties, as well as individual content providers, to rate content on the Internet in a variety of ways. When fully implemented, PICS-compatible World Wide Web browsers, Usenet News Group readers, and other Internet applications, will provide parents the ability to choose from a variety of rating services, or a combination of services.

51. PICS working group [PICS-WG] participants include many of the major online services providers, commercial internet access providers, hardware and software companies, major internet content providers, and consumer organizations. Among active participants in the PICS effort are:

Adobe Systems, Inc.

Apple Computer
America Online
AT&T
Center for Democracy and Technology
CompuServe
Delphi Internet Services
Digital Equipment Corporation
IBM
First floor
First Virtual Holdings Incorporated
France Telecom
FTP Software
Industrial Technology Research Institute of Taiwan
Information Technology Association of America
Institut National de Recherche en Informatique et en Automatique (INRIA)
Interactive Services Association
MCI
Microsoft
MIT/LCS/World Wide Web Consortium
NCD
NEC
Netscape Communications Corporation
NewView
O'Reilly and Associates
Open Market
Prodigy Services Company
Progressive Networks
Providence Systems/Parental Guidance
Recreational Software Advisory Council
SafeSurf
SoftQuad, Inc.
Songline Studios
Spyglass
SurfWatch Software
Telequip Corp.
Time Warner Pathfinder
Viacom Nickelodeon(13)

52. Membership in the PICS-WG includes a broad cross-section of companies from the computer, communications, and content industries, as well as trade associations and public interest groups. PICS technical specifications have been agreed to, allowing the Internet community to begin to deploy products and services based on the PICS-standards.

53. Until a majority of sites on the Internet have been rated by a PICS rating service, PICS will initially function as a "positive" ratings system in which only those sites that have been rated will be displayed using PICS compatible software. In other words, PICS will initially function as a site inclusion list rather than a site exclusion list. The default configuration for a PICS compatible Internet application will be to block access to all sites which have not been rated by a PICS rating service, while allowing access to sites which have a PICS rating for appropriate content.(14)

Software

54. For over a year, various companies have marketed stand alone software that is intended to enable parents and other adults to limit the Internet access of children. Examples of such software include: Cyber Patrol, CYBERsitter, The Internet Filter, Net Nanny, Parental Guidance, SurfWatch, Netscape Proxy Server, and WebTrack. The market for this type of software is growing, and there is increasing competition among software providers to provide products.

Cyber Patrol

55. As more people, particularly children, began to use the Internet, Microsystems Software, Inc. decided to develop and market Internet software intended to empower parents to exercise individual choice over what material their children could access. Microsystems' stated intent is to develop a product which would give parents comfort that their children can reap the benefits of the Internet while shielding them from objectionable or otherwise inappropriate materials based on the parents' own particular tastes and values. Microsystems' product, Cyber Patrol, was developed to address this need.

56. Cyber Patrol was first introduced in August 1995, and is currently available in Windows and Macintosh versions. Cyber Patrol works with both direct Internet Access providers (ISPs, e.g., Netcom, PSI, UUnet), and Commercial Online Service Providers (e.g., America Online, Compuserve, Prodigy, Microsoft). Cyber Patrol is also compatible with all major World Wide Web browsers on the market (e.g., Netscape, Navigator, Mosaic, Prodigy's Legacy and Skimmer browsers, America Online, Netcom's NetCruiser, etc.). Cyber Patrol was the first parental empowerment application to be compatible with the PICS standard. In February of 1996, Microsystems put the first PICS ratings server on the Internet.

57. The CyberNOT list contains approximately 7000 sites in twelve categories. The software is designed to enable parents to selectively block access to any or all of the twelve CyberNOT categories simply by checking boxes in the Cyber Patrol Headquarters (the Cyber Patrol program manager). These categories
are:

Violence/Profanity: Extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity defined as text that uses George Carlin's seven censored words more often than once every fifty messages or pages.

Partial Nudity: Full or partial exposure of the human anatomy except when exposing genitalia.

Nudity: Any exposure of the human genitalia.

Sexual Acts (graphic or text): Pictures or text exposing anyone or anything involved in explicit sexual acts and lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy and involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personals, CD-ROM and videos.

Gross Depictions (graphic or text): Pictures or descriptive text of anyone or anything which are crudely vulgar, deficient in civility or behavior, or showing scatological impropriety. Includes such depictions as maiming, bloody figures, indecent depiction of bodily functions.

Racism/Ethnic Impropriety: Prejudice or discrimination against any race or ethnic culture. Ethnic or racist jokes and slurs. Any text that elevates one race over another.

Satanic/Cult: Worship of the devil; affinity for evil, wickedness. Sects or groups that potentially coerce individuals to grow, and keep, membership.

Drugs/Drug Culture: Topics dealing with the use of illegal drugs for entertainment. This would exclude current illegal drugs used for medicinal purposes (e.g., drugs used to treat victims of AIDS). Includes substances used for other than their primary purpose to alter the individual's state of mind such as glue sniffing.

Militant/Extremist: Extremely aggressive and combative behaviors, radicalism, advocacy of extreme political measures. Topics include extreme political groups that advocate violence as a means to achieve their goal.

Gambling: Of or relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting including non-monetary dares.

Questionable/Illegal: Material or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, software piracy, and copyright infringement.

Alcohol, Beer & Wine: Material pertaining to the sale or consumption of alcoholic beverages. Also includes sites and information relating to tobacco products.

58. Microsystems employs people to search the Internet for sites containing material in these categories. Since new sites are constantly coming online, Microsystems updates the CyberNOT list on a weekly basis. Once installed on the home PC, the copy of Cyber Patrol receives automatic updates to the CyberNOT list over the Internet every seven days.

59. In February of 1996, Microsystems signed a licensing arrangement with CompuServe, one of the leading commercial online services with over 4.3 million subscribers. CompuServe provides Cyber Patrol free of charge to its subscribers. Microsystems the same month signed a licensing arrangement with Prodigy, another leading commercial online service with over 1.4 million subscribers. Prodigy will provide Cyber Patrol free of charge of its subscribers.
60. Cyber Patrol is also available directly from Microsystems for $49.95, which includes a six month subscription to the CyberNOT blocked sites list (updated automatically once every seven days). After six months, parents can receive six months of additional updates for $19.95, or twelve months for $29.95. Cyber Patrol Home Edition, a limited version of Cyber Patrol, is available free of charge on the Internet. To obtain either version, parents download a seven day demonstration version of the full Cyber Patrol product from the Microsystems Internet World Wide Web Server. At the end of the seven day trial period, users are offered the opportunity to purchase the complete version of Cyber Patrol or provide Microsystems some basic demographic information in exchange for unlimited use of the Home Edition. The demographic information is used for marketing and research purposes. Since January of 1996, over 10,000 demonstration copies of Cyber Patrol have been downloaded from Microsystems' Web site.

61. Cyber Patrol is also available from Retail outlets as NetBlocker Plus. NetBlocker Plus sells for $19.95, which includes five weeks of updates to the CyberNOT list.

62. Microsystems also sells Cyber Patrol into a growing market in schools. As more classrooms become connected to the Internet, many teachers want to ensure that their students can receive the benefit of the Internet without encountering material they deem educationally inappropriate.

63. Microsystems is working with the Recreational Software Advisory Council (RSAC), a non-profit corporation which developed rating systems for video games, to implement the RSAC rating system for the Internet.

64. The next release of Cyber Patrol, expected in second quarter of this year, will give parents the ability to use any PICS rating service, including the RSAC rating service, in addition to the Microsystems CyberNOT list.

65. In order to speed the implementation of PICS and encourage the development of PICS-compatible Internet applications, Microsystems maintains a server on the Internet which contains its CyberNOT list. The server provides software developers with access to a PICS rating service, and allows software developers to test their products' ability to interpret standard PICS labels. Microsystems is also offering its PICS client test program for Windows free of charge. The client program can be used by developers of PICS rating services to test their services and products.

**SurfWatch**

66. Another software product, SurfWatch, is also designed to allow parents and other concerned users to filter unwanted material on the Internet. SurfWatch is available for both Apple Macintosh, Microsoft Windows, and Microsoft Windows 95 Operating Systems, and works with direct Internet Access Providers (e.g., Netcom, PSI, UUnet, AT&T, and more than 1000 other Internet Service Providers).

67. The suggested retail price of SurfWatch Software is $49.95, with a street price of between $20.00 and $25.00. The product is also available as part of CompuServe/Spry Inc.'s Internet in a Box for Kids, which includes access to Spry's Kids only Internet service and a copy of SurfWatch. Internet in a Box for Kids retails for approximately $30.00. The subscription service, which updates the SurfWatch blocked site list automatically with new sites each month, is available for $5.95 per month or $60.00 per year. The subscription is included as part of the Internet in a Box for Kids program, and is also provided as a low-cost option from Internet Service Providers.

68. SurfWatch is available at over 12,000 retail locations, including National stores such as Comp USA, Egghead Software, Computer City, and several national mail order outlets. SurfWatch can also be ordered directly from its own site on the World Wide Web, and through the Internet Shopping Network.

69. Plaintiffs America Online (AOL), Microsoft Network, and Prodigy all offer parental control options free of charge to their members. AOL has established an online area designed specifically for children. The "Kids Only" parental control feature allows parents to establish an AOL account for their children.
that accesses only the Kids Only channel on America Online.(15)

70. AOL plans to incorporate PICS-compatible capability into its standard Web browser software, and to make available to subscribers other PICS-compatible Web browsers, such as the Netscape software.

71. Plaintiffs CompuServe and Prodigy give their subscribers the option of blocking all access to the Internet, or to particular media within their proprietary online content, such as bulletin boards and chat rooms.

72. Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images unaccompanied by suggestive text unless those who configure the software are aware of the particular site.

73. Despite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available.

Content on the Internet

74. The types of content now on the Internet defy easy classification. The entire card catalogue of the Carnegie Library is on-line, together with journals, journal abstracts, popular magazines, and titles of compact discs. The director of the Carnegie Library, Robert Croneberger, testified that on-line services are the emerging trend in libraries generally. Plaintiff Hotwired Ventures LLC organizes its Web site into information regarding travel, news and commentary, arts and entertainment, politics, and types of drinks. Plaintiff America Online, Inc., not only creates chat rooms for a broad variety of topics, but also allows members to create their own chat rooms to suit their own tastes. The ACLU uses an America Online chat room as an unordered forum for people to debate civil liberties issues. Plaintiffs' expert, Scott Bradner,(16) estimated that 15,000 newsgroups exist today, and he described his own interest in a newsgroup devoted solely to Formula 1 racing cars. America Online makes 15,000 bulletin boards available to its subscribers, who post between 200,000 and 250,000 messages each day. Another plaintiffs' expert, Harold Rheingold, participates in "virtual communities" that simulate social interaction. It is no exaggeration to conclude that the content on the Internet is as diverse as human thought.

75. The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication -- e-mail, bulletin boards, newsgroups, and chat rooms -- frequently have non-commercial goals. For the economic and technical reasons set forth in the following paragraphs, the Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences. There are examples in the parties' stipulation of some of the non-commercial uses that the Internet serves. Plaintiff Human Rights Watch, Inc., offers information on its Internet site regarding reported human rights abuses around the world. Plaintiff National Writers Union provides a forum for writers on issues of concern to them. Plaintiff Stop Prisoner Rape, Inc., posts text, graphics, and statistics regarding the incidence and prevention of rape in prisons. Plaintiff Critical Path AIDS Project, Inc., offers information on safer sex, the transmission of HIV, and the treatment of AIDS.

76. Such diversity of content on the Internet is possible because the Internet provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions. The start-up and operating costs entailed by communication on the Internet are significantly lower than those associated with use of other forms of mass communication, such as television, radio, newspapers, and magazines. This enables operation of their own Web sites not only by large companies, such as Microsoft and Time Warner, but also by small, not-for-profit groups, such as Stop Prisoner Rape and Critical Path AIDS Project. The Government's expert, Dr. Dan R. Olsen,(17) agreed that creation of a Web site would cost between $1,000 and $15,000, with monthly operating costs depending on one's goals and the Web site's traffic. Commercial online services such as America Online allow subscribers to create Web pages free
of charge. Any Internet user can communicate by posting a message to one of the thousands of newsgroups and bulletin boards or by engaging in an on-line "chat", and thereby reach an audience worldwide that shares an interest in a particular topic.

77. The ease of communication through the Internet is facilitated by the use of hypertext markup language (HTML), which allows for the creation of "hyperlinks" or "links". HTML enables a user to jump from one source to other related sources by clicking on the link. A link might take the user from Web site to Web site, or to other files within a particular Web site. Similarly, by typing a request into a search engine, a user can retrieve many different sources of content related to the search that the creators of the engine have collected.

78. Because of the technology underlying the Internet, the statutory term "content provider,"(18) which is equivalent to the traditional "speaker," may actually be a hybrid of speakers. Through the use of HTML, for example, Critical Path and Stop Prisoner Rape link their Web sites to several related databases, and a user can immediately jump from the home pages of these organizations to the related databases simply by clicking on a link. America Online creates chat rooms for particular discussions but also allows subscribers to create their own chat rooms. Similarly, a newsgroup gathers postings on a particular topic and distributes them to the newsgroup's subscribers. Users of the Carnegie Library can read on-line versions of Vanity Fair and Playboy, and America Online's subscribers can peruse the New York Times, Boating, and other periodicals. Critical Path, Stop Prisoner Rape, America Online and the Carnegie Library all make available content of other speakers over whom they have little or no editorial control.

79. Because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between "speakers" and "listeners" on the Internet. Chat rooms, e-mail, and newsgroups are interactive forms of communication, providing the user with the opportunity both to speak and to listen.

80. It follows that unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in the dialogue that occurs there. In the argot of the medium, the receiver can and does become the content provider, and vice-versa.

81. The Internet is therefore a unique and wholly new medium of worldwide human communication.

Sexually Explicit Material On the Internet

82. The parties agree that sexually explicit material exists on the Internet. Such material includes text, pictures, and chat, and includes bulletin boards, newsgroups, and the other forms of Internet communication, and extends from the modestly titillating to the hardest-core.

83. There is no evidence that sexually-oriented material is the primary type of content on this new medium. Purveyors of such material take advantage of the same ease of access available to all users of the Internet, including establishment of a Web site.

84. Sexually explicit material is created, named, and posted in the same manner as material that is not sexually explicit. It is possible that a search engine can accidentally retrieve material of a sexual nature through an imprecise search, as demonstrated at the hearing. Imprecise searches may also retrieve irrelevant material that is not of a sexual nature. The accidental retrieval of sexually explicit material is one manifestation of the larger phenomenon of irrelevant search results.

85. Once a provider posts content on the Internet, it is available to all other Internet users worldwide. Similarly, once a user posts a message to a newsgroup or bulletin board, that message becomes available to all subscribers to that newsgroup or bulletin board. For example, when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe 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, written in street language so that the teenage receiver can understand them, 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. Messages posted to a newsgroup dedicated to the Oklahoma City bombing travel to all subscribers to that newsgroup.

86. Once a provider posts its content on the Internet, it cannot prevent that content from entering any community. Unlike the newspaper, broadcast station, or cable system, Internet technology necessarily gives a speaker a potential worldwide audience. Because the Internet is a network of networks (as described above in Findings 1 through 4), any network connected to the Internet has the capacity to send and receive information to any other network. Hotwired Ventures, for example, cannot prevent its materials on mixology from entering communities that have no interest in that topic.

87. Demonstrations at the preliminary injunction hearings showed that it takes several steps to enter cyberspace. At the most fundamental level, a user must have access to a computer with the ability to reach the Internet (typically by way of a modem). A user must then direct the computer to connect with the access provider, enter a password, and enter the appropriate commands to find particular data. On the World Wide Web, a user must normally use a search engine or enter an appropriate address. Similarly, accessing newsgroups, bulletin boards, and chat rooms requires several steps.

88. 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." A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content. Even the Government's witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a sexually explicit site by accident.

89. Evidence adduced at the hearing showed significant differences between Internet communications and communications received by radio or television. Although content on the Internet is just a few clicks of a mouse away from the user, the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended.

Obstacles to Age Verification on the Internet

90. There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee, who may use an e-mail "alias" or an anonymous remailer. There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list.

91. Because of similar technological difficulties, individuals posting a message to a newsgroup or engaging in chat room discussions cannot ensure that all readers are adults, and Dr. Olsen agreed. Although some newsgroups are moderated, the moderator's control is limited to what is posted and the moderator cannot control who receives the messages.

92. The Government offered no evidence that there is a reliable way to ensure that recipients and participants in such fora can be screened for age. The Government presented no evidence demonstrating the feasibility of its suggestion that chat rooms, newsgroups and other fora that contain material deemed
indecent could be effectively segregated to "adult" or "moderated" areas of cyberspace.

93. Even if it were technologically feasible to block minors' access to newsgroups and similar fora, there is no method by which the creators of newsgroups which contain discussions of art, politics or any other subject that could potentially elicit "indecent" contributions could limit the blocking of access by minors to such "indecent" material and still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent.

94. Likewise, participants in MUDs (Multi-User Dungeons) and MUSEs (Multi-User Simulation Environments) do not know whether the other participants are adults or minors. Although MUDs and MUSEs require a password for permanent participants, they need not give their real name nor verify their age, and there is no current technology to enable the administrator of these fantasy worlds to know if the participant is an adult or a minor.

95. Unlike other forms of communication on the Internet, there is technology by which an operator of a World Wide Web server may interrogate a user of a Web site. An HTML document can include a fill-in-the-blank "form" to request information from a visitor to a Web site, and this information can be transmitted back to the Web server and be processed by a computer program, usually a Common Gateway Interface (cgi) script. The Web server could then grant or deny access to the information sought. The cgi script is the means by which a Web site can process a fill-in form and thereby screen visitors by requesting a credit card number or adult password.

96. Content providers who publish on the World Wide Web via one of the large commercial online services, such as America Online or CompuServe, could not use an online age verification system that requires cgi script because the server software of these online services available to subscribers cannot process cgi scripts. There is no method currently available for Web page publishers who lack access to cgi scripts to screen recipients online for age.

The Practicalities of the Proffered Defenses

Note: The Government contends the CDA makes available three potential defenses to all content providers on the Internet: credit card verification, adult verification by password or adult identification number, and "tagging".

Credit Card Verification

97. Verification(19) of a credit card number over the Internet is not now technically possible. Witnesses testified that neither Visa nor Mastercard considers the Internet to be sufficiently secure under the current technology to process transactions in that manner. Although users can and do purchase products over the Internet by transmitting their credit card number, the seller must then process the transaction with Visa or Mastercard off-line using phone lines in the traditional way. There was testimony by several witnesses that Visa and Mastercard are in the process of developing means of credit card verification over the Internet.

98. Verification by credit card, if and when operational, will remain economically and practically unavailable for many of the non-commercial plaintiffs in these actions. The Government's expert "suspect[ed]" that verification agencies would decline to process a card unless it accompanied a commercial transaction. There was no evidence to the contrary.

99. There was evidence that the fee charged by verification agencies to process a card, whether for a purchase or not, will preclude use of the credit-card verification defense by many non-profit, non-commercial Web sites, and there was no evidence to the contrary. Plaintiffs' witness Patricia Nell Warren, an author whose free Web site allows users to purchase gay and lesbian literature, testified that she must pay $1 per verification to a verification agency. Her Web site can absorb this cost because it arises in connection with the sale of books available there.

100. Using credit card possession as a surrogate for age, and requiring use of a credit card to enter a site,
would impose a significant economic cost on non-commercial entities. Critical Path, for example, received 3,300 hits daily from February 4 through March 4, 1996. If Critical Path must pay a fee every time a user initially enters its site, then, to provide free access to its non-commercial site, it would incur a monthly cost far beyond its modest resources. The ACLU's Barry Steinhardt testified that maintenance of a credit card verification system for all visitors to the ACLU's Web site would require it to shut down its Web site because the projected cost would exceed its budget.

101. Credit card verification would significantly delay the retrieval of information on the Internet. Dr. Olsen, the expert testifying for the Government, agreed that even "a minute is [an] absolutely unreasonable [delay]. . . . [P]eople will not put up with a minute." Plaintiffs' expert Donna Hoffman similarly testified that excessive delay disrupts the "flow" on the Internet and stifles both "hedonistic" and "goal-directed" browsing.

102. Imposition of a credit card requirement would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material. At this time, credit card verification is effectively unavailable to a substantial number of Internet content providers as a potential defense to the CDA.

Adult Verification by Password

103. The Government offered very limited evidence regarding the operation of existing age verification systems, and the evidence offered was not based on personal knowledge. AdultCheck and Verify, existing systems which appear to be used for accessing commercial pornographic sites, charge users for their services. Dr. Olsen admitted that his knowledge of these services was derived primarily from reading the advertisements on their Web pages. He had not interviewed any employees of these entities, had not personally used these systems, had no idea how many people are registered with them, and could not testify to the reliability of their attempt at age verification.

104. At least some, if not almost all, non-commercial organizations, such as the ACLU, Stop Prisoner Rape or Critical Path AIDS Project, regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge.

105. It would not be feasible for many non-commercial organizations to design their own adult access code screening systems because the administrative burden of creating and maintaining a screening system and the ongoing costs involved is beyond their reach. There was testimony that the costs would be prohibitive even for a commercial entity such as HotWired, the online version of Wired magazine.

106. There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password. Andrew Anker testified that HotWired has received many complaints from its members about HotWired's registration system, which requires only that a member supply a name, e-mail address and self-created password. There is concern by commercial content providers that age verification requirements would decrease advertising and revenue because advertisers depend on a demonstration that the sites are widely available and frequently visited.

107. Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a substantial number of Internet content providers.

The Government's "Tagging" Proposal

108. The feasibility and effectiveness of "tagging" to restrict children from accessing "indecent" speech, as proposed by the Government has not been established. "Tagging" would require content providers to label all of their "indecent" or "patently offensive" material by imbedding a string of characters, such as "XXX," in either the URL or HTML. If a user could install software on his or her computer to recognize the "XXX" tag, the user could screen out any content with that tag. Dr. Olsen proposed a "-L18" tag, an
idea he developed for this hearing in response to Mr. Bradner's earlier testimony that certain tagging would not be feasible.

109. The parties appear to agree that it is technologically feasible -- "trivial", in the words of plaintiffs' expert -- to imbed tags in URLs and HTML, and the technology of tagging underlies both plaintiffs' PICS proposal and the Government's "-L18" proposal.

110. The Government's tagging proposal would require all content providers that post arguably "indecent" material to review all of their online content, a task that would be extremely burdensome for organizations that provide large amounts of material online which cannot afford to pay a large staff to review all of that material. The Carnegie Library would be required to hire numerous additional employees to review its on-line files at an extremely high cost to its limited budget. The cost and effort would be substantial for the Library and frequently prohibitive for others. Witness Kiroshi Kuromiya testified that it would be impossible for his organization, Critical Path, to review all of its material because it has only one full and one part-time employee.

111. The task of screening and tagging cannot be done simply by using software which screens for certain words, as Dr. Olsen acknowledged, and we find that determinations as to what is indecent require human judgment.

112. In lieu of reviewing each file individually, a content provider could tag its entire site but this would prevent minors from accessing much material that is not "indecent" under the CDA.

113. To be effective, a scheme such as the -L18 proposal would require a worldwide consensus among speakers to use the same tag to label "indecent" material. There is currently no such consensus, and no Internet speaker currently labels its speech with the -L18 code or with any other widely-recognized label.

114. Tagging also assumes the existence of software that recognizes the tags and takes appropriate action when it notes tagged speech. Neither commercial Web browsers nor user-based screening software is currently configured to block a -L18 code. Until such software exists, all speech on the Internet will continue to travel to whomever requests it, without hindrance. Labelling speech has no effect in itself on the transmission (or not) of that speech. Neither plaintiffs nor the Government suggest that tagging alone would shield minors from speech or insulate a speaker from criminal liability under the CDA. It follows that all speech on any topic that is available to adults will also be available to children using the Internet (unless it is blocked by screening software running on the computer the child is using).

115. There is no way that a speaker can use current technology to know if a listener is using screening software.

116. Tags can not currently activate or deactivate themselves depending on the age or location of the receiver. Critical Path, which posts on-line safer sex instructions, would be unable to imbed tags that block its speech only in communities where it may be regarded as indecent. Critical Path, for example, must choose either to tag its site (blocking its speech in all communities) or not to tag, blocking its speech in none.

The Problems of Offshore Content and Caching

117. A large percentage, perhaps 40% or more, of content on the Internet originates outside the United States. At the hearing, a witness demonstrated how an Internet user could access a Web site of London (which presumably is on a server in England), and then link to other sites of interest in England. A user can sometimes discern from a URL that content is coming from overseas, since InterNIC allows a content provider to imbed a country code in a domain name. (20) Foreign content is otherwise indistinguishable from domestic content (as long as it is in English), since foreign speech is created, named, and posted in the same manner as domestic speech. There is no requirement that foreign speech contain a country code in its URL. It is undisputed that some foreign speech that travels over the Internet
is sexually explicit.

118. The use of "caching" makes it difficult to determine whether the material originated from foreign or domestic sources. Because of the high cost of using the trans-Atlantic and trans-Pacific cables, and because the high demand on those cables leads to bottleneck delays, content is often "cached", or temporarily stored, on servers in the United States. Material from a foreign source in Europe can travel over the trans-Atlantic cable to the receiver in the United States, and pass through a domestic caching server which then stores a copy for subsequent retrieval. This domestic caching server, rather than the original foreign server, will send the material from the cache to the subsequent receivers, without placing a demand on the trans-oceanic cables. This shortcut effectively eliminates most of the distance for both the request and the information and, hence, most of the delay. The caching server discards the stored information according to its configuration (e.g., after a certain time or as the demand for the information diminishes). Caching therefore advances core Internet values: the cheap and speedy retrieval of information.

119. Caching is not merely an international phenomenon. Domestic content providers store popular domestic material on their caching servers to avoid the delay of successive searches for the same material and to decrease the demand on their Internet connection. America Online can cache the home page of the New York Times on its servers when a subscriber first requests it, so that subsequent subscribers who make the same request will receive the same home page, but from America Online's caching service rather than from the New York Times's server.(21)

120. Put simply, to follow the example in the prior paragraph, America Online has no control over the content that the New York Times posts to its Web site, and the New York Times has no control over America Online's distribution of that content from a caching server.

Anonymity

121. Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

Plaintiffs' Choices Under the CDA

122. Many speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution. The CDA's defenses -- credit card verification, adult access codes, and adult personal identification numbers -- are effectively unavailable for non-commercial, not-for-profit entities.

123. The plaintiffs in this action are businesses, libraries, non-commercial and not-for-profit organizations, and educational societies and consortia. Although some of the material that plaintiffs post online -- such as information regarding protection from AIDS, birth control or prison rape -- is sexually explicit and may be considered "indecent" or "patently offensive" in some communities, none of the plaintiffs is a commercial purveyor of what is commonly termed "pornography."

III. CONCLUSIONS OF LAW

Plaintiffs have established a reasonable probability of eventual success in the litigation by demonstrating that §§ 223(a)(1)(B) and 223(a)(2) of the CDA are unconstitutional on their face to the extent that they reach indecency. Sections 223(d)(1) and 223(d)(2) of the CDA are unconstitutional on their face. Accordingly, plaintiffs have shown irreparable injury, no party has any interest in the enforcement of an unconstitutional law, and therefore the public interest will be served by granting the preliminary injunction. Elrod v. Burns, 427 U.S. 347, 373-74 (1976); Hohe v. Casey, 868 F.2d 69, 72 (3d Cir.), cert. denied, 493 U.S. 848 (1989); Acierno v. New Castle County, 40 F.3d 645, 653 (3d Cir. 1994). The motions for preliminary injunction will therefore be granted.
ORDER

This action is before the Court on plaintiffs' motion for preliminary injunction and defendants' motion to dismiss. For the reasons stated below, the Court grants plaintiffs' motion and denies defendants' motion.

Factual Background

Plaintiffs bring this action for declaratory and injunctive relief challenging the constitutionality of Act No. 1029, Ga. Laws 1996, p. 1505, codified at O.C.G.A. § 16-9-93.1 ("act" or "statute"). The act makes it a crime for

any person . . . knowingly to transmit any data through a computer network . . . for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name . . . to falsely identify the person . . .

and for

any person . . . knowingly to transmit any data through a computer network . . . if such data uses any . . . trade name, registered trademark, logo, legal or official seal, or copyrighted symbol . . . which would falsely state or imply that such person . . . has permission or is legally authorized to use [it] for such purpose when such permission or authorization has not been obtained.

The parties vigorously dispute the scope of the act. Plaintiffs, a group of individuals and organization members who communicate over the internet, interpret it as imposing unconstitutional content-based restrictions on their right to communicate anonymously and pseudonymously over the internet, as well as on their right to use trade names, logos, and other graphics in a manner held to be constitutional in other contexts.

Plaintiffs argue that the act has tremendous implications for internet users, many of whom "falsely identify" themselves on a regular basis for the purpose of communicating about sensitive topics without subjecting themselves to ostracism or embarrassment. Plaintiffs further contend that the trade name and logo restriction frustrates one of the internet's unique features--the "links"(1) that connect web pages on the World Wide Web and enable
users to browse easily from topic to topic through the computer network system. Plaintiffs claim that the act's broad language is further damaging in that it allows for selective prosecution of persons communicating about controversial topics.

Defendants contend that the act prohibits a much narrower class of communications. They interpret it as forbidding only fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose. Defendants ask the Court to abstain from exercising jurisdiction in this case in order to give the Georgia Supreme Court an opportunity to definitively interpret the act.

Motion for Preliminary Injunction

In order to prevail on a preliminary injunction motion, plaintiffs must establish 1) a substantial likelihood of success on the merits; 2) a substantial threat of irreparable injury if the injunction is not granted; 3) that the threatened injury to the plaintiffs outweighs the harm an injunction may cause defendants; and 4) that granting the injunction would not disserve the public interest. Teper v. Miller, 82 F.3d 989, 992-93 n.3 (11th Cir. 1996). The Court concludes that plaintiffs have satisfied each of these requirements and are thus entitled to injunctive relief.

1. Likelihood of Success on the Merits

In their motion to dismiss, defendants assert two affirmative defenses which, if persuasive, would make plaintiffs' success on the merits unlikely. First, defendants argue that because plaintiffs have not been prosecuted or threatened with prosecution under the act, no live controversy exists and plaintiffs therefore lack standing to bring this action. The Court concludes, however, that plaintiffs do have standing because "a credible threat of prosecution" exists. Graham v. Butterworth, 5 F.3d 496, 499 (11th Cir. 1993). When plaintiffs filed this action "they intended to engage in arguably protected conduct, which the statute seemed to proscribe." Id. at 499. Furthermore, the rules of standing are relaxed in the first amendment context where "the statute's alleged danger is, in large measure, one of self-censorship; a harm that can be realized even without an actual prosecution." Virginia v. American Booksellers Ass'n, 484 U.S. 383, 384 (1988).

Defendants also ask the Court to abstain from exercising jurisdiction over this case on the grounds that the law is ambiguous and in need of state court interpretation.(3) However, abstention should rarely be invoked in cases involving facial challenges to statutes allegedly violative of the first amendment. Dombrowski v. Pfister, 380 U.S. 479, 489-90 (1965) (holding abstention "inappropriate for cases [where] . . . statutes are justifiably attacked on their face as abridging free expression"). The reluctance to abstain in first amendment cases recognizes that the delay abstention imposes has a further chilling effect on speech. Zwicker v. Koota, 389 U.S. 241, 252 (1967).

The correct inquiry, when asked to abstain in a case involving a facial statutory challenge, is whether the statute is "fairly subject to an interpretation which will render unnecessary or substantially modify the federal constitutional question." City of Houston v. Hill, 482 U.S. 451, 468 (1987). "If the statute is not obviously susceptible of a limiting construction, then even if the statute has never [been] interpreted by a state court tribunal . . . it is the duty of the federal court to exercise its properly invoked jurisdiction." Id. The Court finds, as set forth below, that O.C.G.A. § 16-9-93.1 is not fairly subject to a limiting construction which would obviate its constitutional problems. Moreover, abstention would impose great costs on plaintiffs by further chilling their expression while they wait for an interpretation of the act by the Georgia Supreme Court or by forcing them to risk prosecution if they choose not to wait. Therefore, the Court finds that abstention is inappropriate in this case.

Having addressed defendants' affirmative defenses, the Court concludes that plaintiffs are likely to prevail on the merits of their claim. It appears from the record that plaintiffs are
likely to prove that the statute imposes content-based restrictions which are not narrowly
tailored to achieve the state's purported compelling interest. Furthermore, plaintiffs are
likely to show that the statute is overbroad and void for vagueness.

First, because "the identity of the speaker is no different from other components of [a]
document's contents that the author is free to include or exclude," McIntyre v. Ohio
Elections Comm'n, 115 S. Ct. 1511, 1516 (1995), the statute's prohibition of internet
transmissions which "falsely identify" the sender constitutes a presumptively invalid
impose content-based restrictions only to promote a "compelling state interest" and only
through use of "the least restrictive means to further the articulated interest." Sable
Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989). Thus, in order to
overcome the presumption of invalidity, defendants must demonstrate that the statute
furthers a compelling state interest and is narrowly tailored to achieve it.

Defendants allege that the statute's purpose is fraud prevention, which the Court agrees is a
compelling state interest. However, the statute is not narrowly tailored to achieve that end
and instead sweeps innocent, protected speech within its scope. Specifically, by its plain
language the criminal prohibition applies regardless of whether a speaker has any intent to
deceive or whether deception actually occurs. Therefore, it could apply to a wide range of
transmissions which "falsely identify" the sender, but are not "fraudulent" within the
specific meaning of the criminal code.

Defendants respond that the act does not mean what it says and that, instead, a variety of
limiting concepts should be engrafted onto it. First, defendants propose to add an element of
fraud, or a specific intent requirement of "intent to defraud" or "intent to deceive" to the
act.(4) None of these terms or phrases appears in the statute, however, although they are
expressly included in other Georgia criminal statutes which require proof of specific intent.
See, e.g., O.C.G.A. §§ 10-1-453, 16-9-1(a), 16-9-2, and 16-8-3.

Second, defendants contend that the act applies only to persons who misappropriate the
identity of another specific entity or person. Again, there is nothing in the language of the
act from which a reasonable person would infer such a requirement, and the General
Assembly has specifically included analogous elements when it meant to do so. See
O.C.G.A. § 10-1-453.

Third, defendants seek to limit the restriction on use of trade names, marks, and seals by
collapsing the act's two clauses--suggesting that "use" of a mark is prohibited only when it
would "falsely identify" the user. Without explanation, this construction borrows the "false
identification" portion of the first clause and applies it to the second. In addition to not
making sense grammatically, the interpretation also imports into the second clause all of the
previously discussed interpretive problems with the phrase "falsely identify." (5)

In construing a statute, the Court must "follow the literal language of the statute 'unless it
produces contradiction, absurdity or such an inconvenience as to insure that the legislature
Department of Trans. v. City of Atlanta, 255 Ga. 124, 137 (1985)). Only if a statute is
"readily susceptible to a narrowing construction" may such an interpretation be applied to
save a questionable law. American Booksellers Ass'n, 484 U.S. at 397. The words and
phrases defendants seek to add to the act appear nowhere in it. Moreover, defendants'
attempt to interpret the act is so confusing and contradictory that it could not possibly
constitute grounds for rejecting the act's plain language. Even if the Court could impose a
limiting construction on the act, defendants' brief provides no real guidance on what that
construction should be, but instead offers a variety of very different possible interpretations
in hopes that the Court will select one. The Court concludes, therefore, that the act is not
readily susceptible to a limiting construction and that its plain language is not narrowly
tailored to promote a compelling state interest.
For similar reasons, plaintiffs are likely to succeed on their overbreadth claim because the statute "sweeps protected activity within its proscription." M.S. News Co. v. Casado, 721 F.2d 1281, 1287 (10th Cir. 1983) (citing Erznoznik v. City of Jacksonville, 422 U.S. 205, 212-13 (1975)). In the first amendment context, the overbreadth doctrine, which invalidates overbroad statutes even when some of their applications are valid, United States v. Salerno, 481 U.S. 739, 745 (1987), is based on the recognition that "the very existence of some broadly written laws has the potential to chill the expressive activity of others not before the Court." Forsyth County v. Nationalist Movement, 505 U.S. 123, 129 (1992).

The Court concludes that the statute was not drafted with the precision necessary for laws regulating speech. On its face, the act prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy, as well as the use of trade names or logos in non-commercial educational speech, news, and commentary -- a prohibition with well-recognized first amendment problems.(6) Therefore, even if the statute could constitutionally be used to prosecute persons who intentionally "falsely identify" themselves in order to deceive or defraud the public, or to persons whose commercial use of trade names and logos creates a substantial likelihood of confusion or the dilution of a famous mark, the statute is nevertheless overbroad because it operates unconstitutionally for a substantial category of the speakers it covers. Village of Schaumburg v. Citizens for a Better Environment, 444 U.S. 620, 634 (1980).

Finally, plaintiffs are likely to succeed on their claim that the statute is unconstitutionally vague. The void-for-vagueness doctrine requires a criminal statute to "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983). Like the overbreadth doctrine, the policies underlying the vagueness rule apply with special force where the statute at issue restricts speech. ACLU v. Reno, 929 F. Supp. 824, 860 (E.D. Pa. 1996). The Court concludes that plaintiffs are likely to prove that the statute is void for vagueness because it 1) does not give fair notice of the scope of conduct it proscribes; 2) is conducive to arbitrary enforcement; and 3) infringes upon plaintiffs' free expression. See Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972).

First, the act fails to give fair notice of proscribed conduct to computer network users by failing to define the following terms and phrases: "falsely identify," "use," "falsely imply," and "point of access to electronic information." These undefined terms provide inadequate notice of the scope of proscribed conduct to persons of ordinary intelligence and thus void the act for vagueness.

The statute criminalizes computer transmissions which "falsely identify" the sender, yet fails to state whether or not proof of specific intent to deceive, or proof of actual deception, is required. Plaintiffs' affidavits demonstrate that, although they have no intent to deceive when sending transmissions which may "falsely identify" them and, indeed, have many legitimate and important reasons for concealing their identity, they cannot determine whether or not their conduct violates the act.

Similarly, the portion of the act relating to trade names and logos fails to define or adequately limit the word "use." Other statutes protecting intellectual property expressly limit the definition of "use" to use in a commercial context. See, e.g., 15 U.S.C. § 1125 (federal trademark infringement law); O.C.G.A. § 10-1-440 (b) (1994) (defining "use" within the meaning of Georgia trademark infringement laws); O.C.G.A. § 10-1-450 (1994) (Georgia trademark infringement law). In contrast, the only limiting concept of "use" in the act is that such use must "falsely imply" that permission to use the mark has been obtained. This restriction, which is also undefined and suffers from the same vagueness problems as the term "falsely identify," fails to provide sufficiently specific notice of proscribed conduct.
Finally, the act fails to explain the phrase "any data . . . over the transmission facilities or through the network facilities of a local telephone network for the purpose of . . . exchanging data with . . . a point of access to electronic information." Plaintiffs contend that this phrase could mean that the act applies not only to computer transmissions per se, but also to transmissions by telephone, fax machine, answering machine, voice mail system, pager, or any other electronic device which might be connected to computer network facilities. The act provides no guidance about these potential applications.

Second, the act's vague provisions create a risk of arbitrary and discriminatory enforcement. As plaintiffs point out, not only does the act fail to notify potential defendants of proscribed conduct, but it also fails to notify law enforcement officials of what exactly is prohibited. The act's failure to specifically articulate proscribed conduct affords prosecutors and police officers substantial room for selective prosecution of persons who express minority viewpoints.

Third, the act's vagueness is particularly harmful because it chills protected expression. Plaintiffs' affidavits indicate that they have already altered what they believe to be innocent and legitimate behavior because of their inability to discern what exactly the act proscribes. Without court intervention, this self-censorship will continue until the act is amended, revoked, or definitively interpreted by the state supreme court.

For all of these reasons, the Court concludes that plaintiffs are likely to succeed on their claim that the act is void for vagueness, overbroad, and not narrowly tailored to promote a compelling state interest.

2. Substantial threat of irreparable injury

Plaintiffs have also demonstrated a substantial threat of irreparable injury in the absence of a preliminary injunction. The Supreme Court has held that "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." Elrod v. Burns, 427 U.S. 347, 373 (1976). As described above, the act has already induced self-censorship. The Court concludes, therefore, that failure to enjoin enforcement of the act will force plaintiffs either to continue self-censorship or to risk criminal prosecution. Thus, plaintiffs have demonstrated a substantial threat of irreparable injury unless a preliminary injunction is issued.

3. Balance of hardships

The balance of hardships weighs heavily in plaintiffs' favor. As stated above, plaintiffs will suffer irreparable injury if prosecution under the statute is not enjoined. In contrast, Georgia already has in place many less restrictive means to address fraud and misrepresentation—the interests defendants claim the act at issue promotes. See, e.g., O.C.G.A. § 16-8-3 (1996) (theft by deception); O.C.G.A. § 16-9-93(a)(2) (1996) (computer theft by deception); O.C.G.A. § 10-1-453 (1994) (unauthorized and deceptive use of name or seal of another); O.C.G.A. § 10-1-393 (Supp. 1996) (unfair and deceptive consumer trade practices). Defendants contend that these statutes do not fully reach problematic behavior over the internet, but they fail adequately to explain why. If the act prevents some ill-defined category of fraud or deception not covered by existing laws, defendants do not articulate why they have a compelling interest in preventing that conduct on the internet but have done nothing to prevent the same practices in the print media. Therefore, the Court concludes that plaintiffs face substantially greater harms if the act is allowed to stand than defendants face if its enforcement is enjoined.

4. Promotion of the Public Interest

Finally, for all the reasons set forth above, a preliminary injunction will advance the public
interest. "No long string of citations is necessary to find that the public interest weighs in favor of having access to a free flow of constitutionally protected speech." Reno, 929 F. Supp. at 851.

5. Conclusion

For the foregoing reasons, the Court DENIES defendants' motion to dismiss [#11-1], GRANTS plaintiffs' motion for preliminary injunction [#3-1], and enjoins defendants from enforcing O.C.G.A. § 16-9-93.1 pending a final determination on the merits of plaintiffs' complaint.

IT IS SO ORDERED, this 20th day of June, 1997.

_________________________________

Marvin H. Shoob, Senior Judge
United States District Court
Northern District of Georgia

_________________________________

NOTES

(1) Links are often graphics or logos which, if "clicked on" by the user with a computer mouse, will transport the user to a different web page covering a new topic of information.

(2) In this section of the order, the Court will also address arguments advanced in defendants' motion to dismiss.

(3) Significantly, this argument contradicts defendants' contention that the statute is sufficiently clear to avoid vagueness and overbreadth challenges.

(4) The terms "fraud," "intent to defraud," and "intent to deceive," although used interchangeably by defendants, are not synonymous in the criminal code. See, e.g., United States v. Godwin, 566 F.2d 975, 976 (5th Cir. 1978). Each term requires proof of different elements, and by using the terms interchangeably, defendants fail to explain which of the distinct elements should be applied to the statute.

Also, the word "falsely"--the only term which actually does appear in the statute--is synonymous with none of the above terms defendants seek to add. "Falsely" means merely "wrongly," "incorrectly," or "not truthfully." Webster's Third New Int'l Dictionary 819 (1976).

(5) To further confuse the matter, defendants suggest elsewhere in their brief that the second clause actually does mean what it says and prohibits all uses of marks which would imply permission for that use which has not been obtained. A fair reading of the clause, as written, is that it prohibits the current use of web page links. The linking function requires publishers of web pages to include symbols designating other web pages which may be of interest to a user. This means that an entity or person's seal may appear on hundreds or thousands of other web pages, just for the purpose of enabling the linking system. The appearance of the seal, although completely innocuous, would definitely "imply" to many users that permission for use had been obtained. Defendants have articulated no compelling state interest that would be furthered by restricting the linking function in this way.

(6) Congress acknowledged the first amendment problems with banning non-commercial use of trademarks by limiting the scope of the new Federal Trademark Dilution Act to apply
MEMORANDUM

This memo describes techniques for, and possible limitations to, forming an enforceable software license agreement (the “Agreement”) online with a party who downloads Licensor’s software.

To create binding contractual obligations, there must be an offer by the licensor (Licensor), acceptance by the licensee (an evaluating ISP), and “consideration” (some form of benefit to each party that supports their respective obligations). If the Agreement is intended to constitute licensor’s “offer,” the licensee must be given an opportunity to review and reject the Agreement prior to the time the licensee makes the final decision about whether or not to consummate the transaction. Otherwise, the licensee will not be deemed to have agreed to the terms of the Agreement.

Historically, the enforceability of “shrinkwrap” software license agreements contained inside software boxes has been in doubt because the licensee/buyer did not have an opportunity to review the terms before purchase. A recent case has suggested that these shrinkwrap agreements may be enforceable if the buyer has the opportunity to return the software after reviewing the terms of the license. On the Internet, however, returning software tends to make little sense. Therefore, it is important to make the Agreement terms available to licensees as early in the process as possible. Early exposure to the Agreement terms will support the argument that licensees had the opportunity to reject the transaction if they did not agree to the license terms.

To procure acceptance early in the process, Licensor should require potential licensees to review the Agreement terms prior to giving them the opportunity to download the software. To accomplish this, a page on the website should contain the Agreement. At the top of the page should be a statement, in all capital letters, stating that the software is being offered pursuant to the terms of the Agreement and that the licensee can demonstrate acceptance by pressing the “I AGREE” button. At the bottom of the Agreement, there should be two buttons: “I AGREE to the above terms” and “CANCEL.” If the “CANCEL” button is selected, the downloading process should terminate. Some licensors include a “PRINT” button so that potential licensees can review the Agreement in hard copy before making the decision, but this button is optional. Some licensors embellish the “I AGREE” button by actually requiring the licensee to type the words “I agree” and, in some cases, to type the licensee’s name. While such additional steps are theoretically beneficial under some legal principles, this extra step is not mandatory.

The most crucial point is that it should be impossible (within existing technological constraints) for the software to be downloaded unless and until the “I AGREE” button is selected. Otherwise, the purported licensee can claim that they were unaware of the Agreement terms before consummating the transaction.

In Licensor’ case, once the download is complete, the licensee will possess an executable file which may be used to collect the prospective membership information and email it back to
Licensor. Upon review of this information by Licensor, Licensor will deliver to the licensee an evaluation key and Licensor will have the opportunity to enter into other relationships then.

To avoid possible legal problems associated with offering terms on a “take-it-or-leave-it” basis, some licensors state that if the licensee has any concerns about the license, they should contact the licensor. However, the danger is that licensees will seek to negotiate the Agreement, which in turn could result in significant transaction costs. Some licensors have tried a compromise approach: they state in the introductory paragraph of the Agreement that licensees should approach the licensor with any concerns, but there is no obvious email addresses or hypertext links for such feedback.

If Licensor believes that the licensees may be legitimately giving a copy of the software to third parties, it would be a good idea to include the Agreement as a bootstrap that launches when the software is executed the first time after the copy is made and which must be agreed to before the software will operate. Of course, the bootstrap license has less likelihood of being enforced given it is raised relatively late in the licensee’s decision-making process.

It should be noted that there are some reasons why the Agreement may be unenforceable even if all the efforts described in this memo are undertaken. These situations may occur if the licensee does not understand the Agreement because it was not translated into their native language, if the licensee is a minor or has other incapacities (such as insanity or intoxication), if the Agreement terms are deemed unconscionable or if the Agreement terms are “trumped” by local laws that cannot be contractually overridden or waived. Even if some or all of the Agreement terms fail, however, Licensor will have copyright rights—which are enforceable without reference to the Agreement—in the software.
In the United States Court of Appeals For the Seventh Circuit

No. 96-1139

PROCD, INCORPORATED,

Plaintiff-Appellant,

v.

MATTHEW ZEIDENBERG and SILKEN MOUNTAIN WEB SERVICES, INC.,

Defendants-Appellees.

Appeal from the United States District Court for the Western District of Wisconsin. No. 95-C-0671-C—Barbara B. Crabb, Judge.

ARGUED MAY 23, 1996—DECIDED JUNE 20, 1996

Before COFFEY, FLAUM, and EASTERBROOK, Circuit Judges.

EASTERBROOK, Circuit Judge. Must buyers of computer software obey the terms of shrinkwrap licenses? The dis- trict court held not, for two reasons: first, they are not contracts because the licenses are inside the box rather than printed on the outside; second, federal law forbids enforcement even if the licenses are contracts. 908 F. Supp. 640 (W.D. Wis. 1996). The parties and numerous amici curiae have briefed many other issues, but these are the only two that matter—and we disagree with the district judge's conclusion on each. Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example, if they violate a rule of positive law, or if they are un- conscionable). Because no one argues that the terms of the license at issue here are troublesome, we remand with instructions to enter judgment for the plaintiff.

I

ProCD, the plaintiff, has compiled information from more than 3,000 telephone directories into a computer database. We may assume that this database cannot be copyrighted, although it is more complex, contains more information (nine-digit zip codes and census industrial codes), is organ- ized differently, and therefore is more original than the single alphabetical directory at issue in Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991). See Paul J. Heald, The Vices of
Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991). See Paul J. Heald, The Vices of Originality, 1991 Sup. Ct. Rev. 143, 160-68. ProCD sells a version of the database, called SelectPhone (trademark), on CD-ROM discs. (CD-ROM means "compact disc--read only memory." The "shrinkwrap license" gets its name from the fact that retail software packages are covered in plastic or cellophane "shrinkwrap," and some vendors, though not ProCD, have written licenses that become effective as soon as the customer tears the wrapping from the package. Vendors prefer "end user license," but we use the more common term.) A proprietary method of compressing the data serves as effective encryption too. Customers decrypt and use the data with the aid of an application program that ProCD has written. This program, which is copyrighted, searches the database in response to users' criteria (such as "find all people named Tatum in Tennessee, plus all firms with 'Door Systems' in the corporate name"). The resulting lists (or, as ProCD prefers, "listings") can be read and manipulated by other software, such as word processing programs.

The database in SelectPhone (trademark) cost more than $10 million to compile and is expensive to keep current. It is much more valuable to some users than to others. The combination of names, addresses, and sic codes enables manufacturers to compile lists of potential customers. Manufacturers and retailers pay high prices to specialized information intermediaries for such mailing lists; ProCD offers a potentially cheaper alternative. People with nothing to sell could use the database as a substitute for calling long distance information, or as a way to look up old friends who have moved to unknown towns, or just as an electronic substitute for the local phone book. ProCD decided to engage in price discrimination, selling its database to the general public for personal use at a low price (approximately $150 for the set of five discs) while selling information to the trade for a higher price. It has adopted some intermediate strategies too: access to the SelectPhone (trademark) database is available via the America On-line service for the price America Online charges to its clients (approximately $3 per hour), but this service has been tailored to be useful only to the general public.

If ProCD had to recover all of its costs and make a profit by charging a single price--that is, if it could not charge more to commercial users than to the general public--it would have to raise the price substantially over $150. The ensuing reduction in sales would harm consumers who value the information at, say, $200. They get consumer surplus of $50 under the current arrangement but would cease to buy if the price rose substantially. If because of high elasticity of demand in the consumer segment of the market the only way to make a profit turned out to be a price attractive to commercial users alone, then all consumers would lose out--and so would the commercial clients, who would have to pay more for the listings because ProCD could not obtain any contribution toward costs from the consumer market.

To make price discrimination work, however, the seller must be able to control arbitrage. An air carrier sells tickets for less to vacationers than to business travelers, using advance purchase and Saturday-night-stay requirements to distinguish the categories. A producer of movies segments the market by time, releasing first to theaters, then to pay-per-view services, next to the videotape and laserdisc market, and finally to cable and commercial TV. Vendors of computer software have a harder task. Anyone can walk into a retail store and buy a box. Customers do not wear tags saying "commercial user" or "consumer user." Anyway, even a commercial-user-detector at the door would not work, because a consumer could buy the software and resell to a commercial user. That arbitrage would break down the price discrimination and drive up the minimum price at which ProCD would sell to anyone.

Instead of tinkering with the product and letting users sort themselves--for example, furnishing current data at a high price that would be attractive only to commercial customers, and two-year-old data at a low price--ProCD turned to the institution of contract. Every box containing its consumer product declares that the software comes with restrictions stated in an enclosed license. This license, which is encoded on the CD-ROM disks as well as printed in the manual, and which appears on a user's screen every time the software runs, limits use of the application program and listings to non-commercial purposes.

Matthew Zeidenberg bought a consumer package of SelectPhone (trademark) in 1994 from a retail outlet in Madison, Wisconsin, but decided to ignore the license. He formed Silken Mountain Web Services, Inc., to resell the information in the SelectPhone (trademark) database. The corporation makes the database available on the Internet to anyone willing to pay its price--which, needless to say, is less than
ProCD charges its commercial customers. Zeidenberg has purchased two additional SelectPhone (trademark) packages, each with an updated version of the database, and made the latest information available over the World Wide Web, for a price, through his corporation. ProCD filed this suit seeking an injunction against further dissemination that exceeds the rights specified in the licenses (identical in each of the three packages Zeidenberg purchased). The district court held the licenses ineffectual because their terms do not appear on the outside of the packages. The court added that the second and third licenses stand no different from the first, even though they are identical, because they might have been different, and a purchaser does not agree to--and cannot be bound by--terms that were secret at the time of purchase. 908 F. Supp. at 654.

II

Following the district court, we treat the licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code. Whether there are legal differences between "contracts" and "licenses" (which may matter under the copyright doctrine of first sale) is a subject for another day. See Microsoft Corp. v. Harmony Computers & Electronics, Inc., 846 F. Supp. 208 (E.D. N.Y. 1994). Zeidenberg does not argue that Silken Mountain Web Services is free of any restrictions that apply to Zeidenberg himself, because any effort to treat the two parties as distinct would put Silken Moun-tain behind the eight ball on ProCD's argument that copy-ing the application program onto its hard disk violates the copyright laws. Zeidenberg does argue, and the dis-trict court held, that placing the package of software on the shelf is an "offer," which the customer "accepts" by paying the asking price and leaving the store with the goods. Peeters v. State, 154 Wis. 111, 142 N.W. 181 (1913). In Wisconsin, as elsewhere, a contract includes only the terms on which the parties have agreed. One cannot agree to hidden terms, the judge concluded. So far, so good--but one of the terms to which Zeidenberg agreed by pur-chasing the software is that the transaction was subject to a license. Zeidenberg's position therefore must be that the printed terms on the outside of a box are the parties' contract--except for printed terms that refer to or incor-porate other terms. But why would Wisconsin fetter the parties' choice in this way? Vendors can put the entire terms of a contract on the outside of a box only by using microscopic type, removing other information that buyers might find more useful (such as what the software does, and on which computers it works), or both. The "Read Me" file included with most software, describing system requirements and potential incompatibilities, may be equivalent to ten pages of type; warranties and license restrictions take still more space. Notice on the outside, terms on the inside, and a right to return the software for a refund if the terms are unacceptable (a right that the license expressly extends), may be a means of doing business valuable to buyers and sellers alike. See E. Allan Farnsworth, 1 Farnsworth on Contracts sec. 4.26 (1990); Restatement (2d) of Contracts sec. 211 comment a (1981) ("Standardization of agreements serves many of the same functions as standardization of goods and services; both are essential to a system of mass production and distribu-tion. Scarce and costly time and skill can be devoted to a class of transactions rather than the details of individual transactions."). Doubtless a state could forbid the use of standard contracts in the software business, but we do not think that Wisconsin has done so.

Transactions in which the exchange of money precedes the communication of detailed terms are common. Con-sider the purchase of insurance. The buyer goes to an agent, who explains the essentials (amount of coverage, number of years) and remits the premium to the home office, which sends back a policy. On the district judge's understanding, the terms of the policy are irrelevant because the insured paid before receiving them. Yet the device of payment, often with a "binder" (so that the in-surance takes effect immediately even though the home office reserves the right to withdraw coverage later), in advance of the policy, serves buyers' interests by ac-celerating effectiveness and reducing transactions costs. Or consider the purchase of an airline ticket. The traveler calls the carrier or an agent, is quoted a price, reserves a seat, pays, and gets a ticket, in that order. The ticket contains elaborate terms, which the traveler can reject by canceling the reservation. To use the ticket is to ac-cept the terms, even terms that in retrospect are dis-advantageous. See Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991); see also Vimar Seguros y Reaseguros, S.A. v. M/V Sky Reefer, 115 S. Ct. 2322 (1995) (bills of lading). Just so with a ticket to a concert. The back of the ticket states that the patron promises not to record the concert; to attend is to agree. A theater that detects a violation will confiscate the tape and escort the violator to the exit. One could arrange things so that every con-certgoer signs this promise before forking over the money, but that cumbersome way of doing things not only would lengthen queues and
raise prices but also would scotch the sale of tickets by phone or electronic data service.

Consumer goods work the same way. Someone who wants to buy a radio set visits a store, pays, and walks out with a box. Inside the box is a leaflet containing some terms, the most important of which usually is the warranty, read for the first time in the comfort of home. By Zeidenberg's lights, the warranty in the box is irrelevant; every consumer gets the standard warranty implied by the UCC in the event the contract is silent; yet so far as we are aware no state disregards warranties furnished with consumer products. Drugs come with a list of ingredients on the outside and an elaborate package insert on the inside. The package insert describes drug interactions, contraindications, and other vital information—but, if Zeidenberg is right, the purchaser need not read the package insert, because it is not part of the contract. Next consider the software industry itself. Only a minority of sales take place over the counter, where there are boxes to peruse. A customer pays an order by phone in response to a line item in a catalog or a review in a magazine. Much software is ordered over the Internet by purchasers who have never seen a box. Increasingly software arrives by wire. There is no box; there is only a stream of electrons, a collection of information that includes data, an application program, instructions, many limitations ("MegaPixel 3.14159 cannot be used with Byte- Pusher 2.718"), and the terms of sale. The user purchases a serial number, which activates the software's features. On Zeidenberg's arguments, these unboxed sales are un-fettered by terms—so the seller has made a broad warranty and must pay consequential damages for any short-falls in performance, two "promises" that if taken seriously would drive prices through the ceiling or return transactions to the horse-and-buggy age.

According to the district court, the UCC does not countenance the sequence of money now, terms later. (Wisconsin's version of the UCC does not differ from the Official Version in any material respect, so we use the regular numbering system. Wis. Stat. sec. 402.201 corresponds to UCC sec. 2-201, and other citations are easy to derive.) One of the court's reasons—that by proposing as part of the draft Article 2B a new UCC sec. 2-2203 that would explicitly validate standard-form user licenses, the American Law Institute and the National Conference of Commissioners on Uniform Laws have conceded the invalidity of shrink-wrap licenses under current law, see 908 F. Supp. at 655-66—depends on a faulty inference. To propose a change in a law's text is not necessarily to propose a change in the law's effect. New words may be designed to fortify the current rule with a more precise text that curtails uncertainty. To judge by the flux of law review articles discussing shrink-wrap licenses, uncertainty is much in need of reduction—although businesses seem to feel less uncertainty than do scholars, for only three cases (other than ours) touch on the subject, and none directly address it. See Step-Saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91 (3d Cir. 1991); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268-70 (5th Cir. 1988); Arizona Retail Systems, Inc. v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993). As their titles suggest, these are not consumer transactions. Step-Saver is a battle-of-the-forms case, in which the parties exchanged incompatible forms and a court must decide which prevails. See Northrop Corp. v. Litronic Industries, 29 F.3d 1173 (7th Cir. 1994) (Illinois law); Douglas G. Baird & Robert Weisberg, Rules, Standards, and the Battle of the Forms: A Reassessment of sec. 2-207, 68 Va. L. Rev. 1217, 1227-31 (1982). Our case has only one form; UCC sec. 2-207 is irrelevant. Vault holds that Louisiana's special shrink-wrap-license statute is preempted by federal law, a question to which we return. And Arizona Retail Systems did not reach the question, because the court found that the buyer knew the terms of the license before purchasing the software.

What then does the current version of the UCC have to say? We think that the place to start is sec. 2-204(1): "A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance. And that is what happened. ProCD proposed a contract that a buyer would accept by using the software after having an opportunity to read the license at leisure. This Zeidenberg did. He had no choice, because the software splashed the license on the screen and would not let him proceed without indicating acceptance. So although the district judge was right to say that the contract can be, and often is, formed simply by paying the price and walking out of the store, the UCC permits contracts to be formed in other ways. ProCD proposed such a different way, and without protest Zeidenberg agreed. Ours is not a case in which a consumer opens a package to find an insert saying "you owe us an extra $10,000" and the seller files suit to collect. Any buyer finding such a demand can prevent formation of
$10,000" and the seller files suit to collect. Any buyer finding such a demand can prevent formation of the contract by return- ing the package, as can any consumer who concludes that the terms of the license make the software worth less than the purchase price. Nothing in the UCC requires a seller to maximize the buyer's net gains.

Section 2-606, which defines "acceptance of goods", rein- forces this understanding. A buyer accepts goods under sec. 2-606(1)(b) when, after an opportunity to inspect, he fails to make an effective rejection under sec. 2-602(1). ProCD ex- tended an opportunity to reject if a buyer should find the license terms unsatisfactory; Zeidenberg inspected the package, tried out the software, learned of the license, and did not reject the goods. We refer to sec. 2-606 only to show that the opportunity to return goods can be impor- tant; acceptance of an offer differs from acceptance of goods after delivery, see Gillen v. Atalanta Systems, Inc., 997 F.2d 280, 284 n.1 (7th Cir. 1993); but the UCC con- sistently permits the parties to structure their relations so that the buyer has a chance to make a final decision after a detailed review.

Some portions of the UCC impose additional require- ments on the way parties agree on terms. A disclaimer of the implied warranty of merchantability must be "con- spicuous." UCC sec. 2-316(2), incorporating UCC sec. 1-201(10). Promises to make firm offers, or to negate oral modifications, must be "separately signed." UCC secs. 2-205, 2-209(2). These special provisos reinforce the impression that, so far as the UCC is concerned, other terms may be as in- conspicuous as the forum-selection clause on the back of the cruise ship ticket in Carnival Lines. Zeidenberg has not located any Wisconsin case--for that matter, any case in any state--holding that under the UCC the ordinary terms found in shrinkwrap licenses require any special prominence, or otherwise are to be undercut rather than enforced. In the end, the terms of the license are con- ceptually identical to the contents of the package. Just as no court would dream of saying that SelectPhone (trademark) must contain 3,100 phone books rather than 3,000, or must have data no more than 30 days old, or must sell for $100 rather than $150--although any of these changes would be welcomed by the customer, if all other things were held constant--so, we believe, Wisconsin would not let the buyer pick and choose among terms. Terms of use are no less a part of "the product" than are the size of the database and the speed with which the software compiles listings. Competition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy. Digital Equipment Corp. v. Uniq Digital Technologies, Inc., 73 F.3d 756 (7th Cir. 1996). ProCD has rivals, which may elect to compete by offer- ing superior software, monthly updates, improved terms of use, lower price, or a better compromise among these elements. As we stressed above, adjusting terms in buyers' favor might help Matthew Zeidenberg today (he already has the software) but would lead to a response, such as a higher price, that might make consumers as a whole worse off.

III

The district court held that, even if Wisconsin treats shrinkwrap licenses as contracts, sec. 301(a) of the Copyright Act, 17 U.S.C. sec. 301(a), prevents their enforcement. 908 F. Supp. at 656-59. The relevant part of sec. 301(a) preempts any "legal or equitable rights [under state law] that are equivalent to any of the exclusive rights within the gen- eral scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103". ProCD's soft- ware and data are "fixed in a tangible medium of expres- sion", and the district judge held that they are "within the subject matter of copyright". The latter conclusion is plainly right for the copyrighted application program, and the judge thought that the data likewise are "within the subject matter of copyright" even if, after Feist, they are not sufficiently original to be copyrighted. 908 F. Supp. at 656-57. Baltimore Orioles, Inc. v. Major League Baseball Players Ass'n, 805 F.2d 663, 676 (7th Cir. 1986), supports that conclusion, with which commentators agree. E.g., Paul Goldstein, III Copyright sec. 15.2.3 (2d ed. 1996); Melville B. Nimmer & David Nimmer, Nimmer on Copy- right sec. 101[B] (1995); William F. Patry, II Copyright Law and Practice 1108-09 (1994). One function of sec. 301(a) is to prevent states from giving special protection to works of authorship that Congress has decided should be in the public domain, which it can accomplish only if "subject matter of copyright" includes all works of a type covered by sections 102 and 103, even if federal law does not af- ford protection to them. Cf. Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989) (same principle under patent laws).
But are rights created by contract "equivalent to any of the exclusive rights within the general scope of copy-right"? Three courts of appeals have answered "no." Na-tional Car Rental Systems, Inc. v. Computer Associates International, Inc., 991 F.2d 426, 433 (8th Cir. 1993); Ta-quino v. Teledyne Monarch Rubber, 893 F.2d 1488, 1501 (5th Cir. 1990); Acorn Structures, Inc. v. Swantz, 846 F.2d 923, 926 (4th Cir. 1988). The district court disagreed with these decisions, 908 F. Supp. at 658, but we think them sound. Rights "equivalent to any of the exclusive rights within the general scope of copyright" are rights estab-lished by law—rights that restrict the options of persons who are strangers to the author. Copyright law forbids duplication, public performance, and so on, unless the per-son wishing to copy or perform the work gets permission; silence means a ban on copying. A copyright is a right against the world. Contracts, by contrast, generally af-fect only their parties; strangers may do as they please, so contracts do not create "exclusive rights." Someone who found a copy of SelectPhone (trademark) on the street would not be affected by the shrinkwrap license—though the fed-eral copyright laws of their own force would limit the finder's ability to copy or transmit the application pro-gram.

Think for a moment about trade secrets. One common trade secret is a customer list. After Feist, a simple alpha-betical list of a firm's customers, with address and tele-phone numbers, could not be protected by copyright. Yet Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974), holds that contracts about trade secrets may be enforced—precisely because they do not affect strangers' ability to discover and use the information independently. If the amendment of sec. 301(a) in 1976 overruled Kewanee and abolished consensual protection of those trade secrets that cannot be copyrighted, no one has noticed—though aboli-tion is a logical consequence of the district court's ap-proach. Think, too, about everyday transactions in intellec-tual property. A customer visits a video store and rents a copy of Night of the Lepus. The customer's contract with the store limits use of the tape to home viewing and requires its return in two days. May the customer keep the tape, on the ground that sec. 301(a) makes the promise unenforceable?

A law student uses the LEXIS database, containing public-domain documents, under a contract limiting the results to educational endeavors; may the student resell his access to this database to a law firm from which LEXIS seeks to collect a much higher hourly rate? Suppose ProCD hires a firm to scour the nation for telephone directories, promising to pay $100 for each that ProCD does not al-ready have. The firm locates 100 new directories, which it sends to ProCD with an invoice for $10,000. ProCD incorp-orates the directories into its database; does it have to pay the bill? Surely yes; Aronson v. Quick Point Pencil Co., 440 U.S. 257 (1979), holds that promises to pay for intellectual property may be enforced even though federal law (in Aronson, the patent law) offers no protection against third-party uses of that property. See also Kennedy v. Wright, 851 F.2d 963 (7th Cir. 1988). But these illustra-tions are what our case is about. ProCD offers software and data for two prices: one for personal use, a higher price for commercial use. Zeidenberg wants to use the data without paying the seller's price; if the law student and Quick Point Pencil Co. could not do that, neither can Zeidenberg.

Although Congress possesses power to preempt even the enforcement of contracts about intellectual property--or railroads, on which see Norfolk & Western Ry. v. Train Dispatchers, 499 U.S. 117 (1991)—courts usually read pre-emption clauses to leave private contracts unaffected. American Airlines, Inc. v. Wolens, 115 S. Ct. 817 (1995), provides a nice illustration. A federal statute preempts any state "law, rule, regulation, standard, or other pro- vision . . . relating to rates, routes, or services of any air carrier." 49 U.S.C. App. sec. 1305(a)(1). Does such a law preempt the law of contracts—so that, for example, an air carrier need not honor a quoted price (or a contract to reduce the price by the value of frequent flyer miles)? The Court allowed that it is possible to read the statute that broadly but thought such an interpretation would make little sense. Terms and conditions offered by con-tract reflect private ordering, essential to the efficient functioning of markets. 115 S. Ct. at 824-25. Although some principles that carry the name of contract law are designed to defeat rather than implement consensual trans-actions, id. at 826 n.8, the rules that respect private choice are not preempted by a clause such as sec. 1305(a)(1). Sec-tion 301(a) plays a role similar to sec. 1301(a)(1): it prevents states from substituting their own regulatory systems for those of the national government. Just as sec. 301(a) does not itself interfere with private transactions in intellectual property, so it does not prevent states from respecting those transactions. Like the Supreme Court in Wolens, we think it prudent to refrain from adopting a rule that anything with the label "contract" is necessarily outside the preemption clause: the variations and possibilities are too numerous to foresee. National Car Rental likewise recognizes the
possibility that some applications of the law of contract could interfere with the attainment of national objectives and therefore come within the domain of sec. 301(a). But general enforcement of shrinkwrap licenses of the kind before us does not create such interference.

Aronson emphasized that enforcement of the contract between Aronson and Quick Point Pencil Company would not withdraw any information from the public domain. That is equally true of the contract between ProCD and Zeidenberg. Everyone remains free to copy and disseminate all 3,000 telephone books that have been incorporated into ProCD's database. Anyone can add sic codes and zip codes. ProCD's rivals have done so. Enforcement of the shrinkwrap license may even make information more readily available, by reducing the price ProCD charges to consumer buyers. To the extent licenses facilitate dis- tribution of object code while concealing the source code (the point of a clause forbidding disassembly), they serve the same procompetitive functions as does the law of trade secrets. Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174, 180 (7th Cir. 1991). Licenses may have other benefits for consumers: many licenses permit users to make extra copies, to use the software on multiple computers, even to incorporate the software into the user's products. But whether a particular license is gen- erous or restrictive, a simple two-party contract is not "equivalent to any of the exclusive rights within the gen- eral scope of copyright" and therefore may be enforced.

REVERSED AND REMANDED

Copyright © 1994-1997 FindLaw Inc.
RICH HILL and ENZA HILL, on behalf of a class of persons similarly situated, Plaintiffs-Appellees, v. GATEWAY 2000, INC., and DAVID PRAIS, Defendants-Appellants.

No. 96-3294

UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

105 F.3d 1147; 1997 U.S. App. LEXIS 176

December 10, 1996, ARGUED
January 6, 1997, DECIDED


DISPOSITION: Vacated and remanded.


JUDGES: Before CUMMINGS, HARLINGTON WOOD, JR., and EASTERBROOK, Circuit Judges.

OPINIONBY: EASTERBROOK

OPINION: [*1148] EASTERBROOK, Circuit Judge. A customer picks up the phone, orders a computer, and gives a credit card number. Presently a box arrives, containing the computer and a list of terms, said to govern unless the customer returns the computer within 30 days. Are these terms effective as the parties' contract, or is the contract term-free because the order-taker did not read any terms over the phone and elicited the customer's assent?

One of the terms in the box containing a Gateway 2000 system was an arbitration clause. Rich and Enza Hill, the customers, kept the computer more than 30 days before complaining about its components and performance. They filed suit in federal court arguing, among other things, that the product's shortcomings make Gateway a racketeer (mail and wire fraud are said to be the predicate offenses), leading to treble damages under RICO for the Hills and a class of all other purchasers. Gateway asked the district court to enforce the arbitration clause; the judge refused, writing that "the present record is insufficient to support a finding of a valid arbitration agreement between the parties or that the plaintiffs were given adequate notice of the arbitration clause." Gateway took an immediate appeal, as is its right. 9 U.S.C. § 5(a)(1)(A).
The Hills say that the arbitration clause did not stand out: they concede noticing the statement of terms but deny reading it closely enough to discover the agreement to arbitrate, and they ask us to conclude that they therefore may go to court. Yet an agreement to arbitrate must be enforced "save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. @ 2. Doctor's Associates, Inc. v. Casarotto, 134 L. Ed. 2d 902, 116 S. Ct. 1652 (1996), holds that this provision [***3] of the Federal Arbitration Act is inconsistent with any requirement that an arbitration clause be prominent. A contract need not be read to be effective; people who accept take the risk that the unread terms may in retrospect prove unwelcome. Carr v. CIGNA Securities, Inc., 95 F.3d 544, 547 (7th Cir. 1996); Chicago Pacific Corp. v. Canada Life Assurance Co., 850 F.2d 334 (7th Cir. 1988). Terms inside Gateway's box stand or fall together. If they constitute the parties' contract because the Hills had an opportunity to return the computer after reading them, then all must be enforced.

ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), holds that terms inside a box of software bind consumers who use the software after an opportunity to read the terms and to reject them by returning the product. Likewise, Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585, 113 L. Ed. 2d 622, 111 S. Ct. 1522 (1991), enforces a forum-selection clause that was included among three pages of terms attached to a cruise ship ticket. ProCD and Carnival Cruise Lines exemplify the many commercial transactions in which people pay for products with terms to follow; ProCD discusses others. 86 F.3d at 1451-52. The district [***4] court concluded in ProCD that the contract is formed when the consumer pays for the software; as a result, the court held, only terms known to the consumer at that moment are part of the contract, and provisions inside the box do not count. Although this is one way a contract [*1149] could be formed, it is not the only way: "A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance." Id. at 1452. Gateway shipped computers with the same sort of accept-or-return offer ProCD made to users of its software. ProCD relied on the Uniform Commercial Code rather than any peculiarities of Wisconsin law; both Illinois and South Dakota, the two states whose law might govern relations between Gateway and the Hills, have adopted the UCC; neither side has pointed us to any atypical doctrines in those states that might be pertinent; ProCD therefore applies to this dispute.

Plaintiffs ask us to limit ProCD to software, but where's the sense in that? ProCD is about the law of contract, not the law of software. Payment [***5] preceding the revelation of full terms is common for air transportation, insurance, and many other endeavors. Practical considerations support allowing vendors to enclose the full legal terms with their products. Cashiers cannot be expected to read legal documents to customers before ringing up sales. If the staff at the other end of the phone for direct-sales operations such as Gateway's had to read the four-page statement of terms before taking the buyer's credit card number, the droning voice would anesthetize rather than enlighten many potential buyers. Others would hang up in a rage over the waste of their time. And oral recitation would not avoid customers' assertions (whether true or feigned) that the clerk did not read term X to them, or that they did not remember or understand it. Writing provides benefits for both sides of commercial transactions. Customers as a group are better off when vendors skip costly and ineffectual steps such as telephonic recitation, and use instead a simple approve-or-return device. Competent adults are bound by such documents,
read or unread. For what little it is worth, we add that the box from Gateway
screwed with software. The computer came [**6] with an operating system,
without which it was useful only as a boat anchor. See Digital Equipment Corp.
v. Unig Digital Technologies, Inc., 73 F.3d 756, 761 (7th Cir. 1996). Gateway
also included many application programs. So the Hills' effort to limit ProCD to
software would not avail them factually, even if it were sound legally—which it
is not.

For their second sally, the Hills contend that ProCD should be limited to
executory contracts (to licenses in particular), and therefore does not apply
because both parties' performance of this contract was complete when the box
arrived at their home. This is legally and factually wrong: legally because the
question at hand concerns the formation of the contract rather than its
performance, and factually because both contracts were incompletely performed.
ProCD did not depend on the fact that the seller characterized the transaction
as a license rather than as a contract; we treated it as a contract for the sale
of goods and reserved the question whether for other purposes a "license"
characterization might be preferable. 86 F.3d at 1450. All debates about
characterization to one side, the transaction in ProCD [**7] was no more
executory than the one here: Zeidenberg paid for the software and walked out of
the store with a box under his arm, so if arrival of the box with the product
ends the time for revelation of contractual terms, then the time ended in ProCD
before Zeidenberg opened the box. But of course ProCD had not completed
performance with delivery of the box, and neither had Gateway. One element of
the transaction was the warranty, which obliges sellers to fix defects in their
products. The Hills have invoked Gateway's warranty and are not satisfied with
its response, so they are not well positioned to say that Gateway's obligations
were fulfilled when the motor carrier unloaded the box. What is more, both ProCD

Gateway promised to help customers to use their products. Long-term service
and information obligations are common in the computer business, on both
hardware and software sides. Gateway offers "lifetime service" and has a
round-the-clock telephone hotline to fulfill this promise. Some vendors spend
more money helping customers use their products than on developing and
manufacturing them. The document in Gateway's box includes promises of
[**1150] future performance that some consumers value highly; these
promises bind Gateway just as the arbitration clause binds the Hills.

Next the Hills insist that ProCD is irrelevant because Zeidenberg was a
"merchant" and they are not. Section 2-207(2) of the UCC, the infamous
battle-of-the-forms section, states that "additional terms [following acceptance
of an offer] are to be construed as proposals for addition to a contract.
Between merchants such terms become part of the contract unless...".
Plaintiffs tell us that ProCD came out as it did only because Zeidenberg was a
"merchant" and the terms inside ProCD's box were not excluded by the "unless"
clause. This argument pays scant attention to the opinion in ProCD, which
concluded that, when there is only one form, "@ 2-207 is irrelevant." 86 F.3d
at 1452. The question in ProCD was not whether terms were added to a contract
after its formation, but how and when the contract was formed—in particular,
whether a vendor may propose that a contract of sale be formed, not in the store
(or over the phone) with the payment of money or a general "send me the
product," but after the customer has had a chance to inspect both the Item and
the terms. ProCD answers [**9] "yes," for merchants and consumers alike. Yet
again, for what little it is worth we observe that the Hills misunderstand the
setting of ProCD. A "merchant" under the UCC "means a person who deals in goods
c of the kind or otherwise by his occupation holds himself out as having
knowledge or skill peculiar to the practices or goods involved in the transaction", @ 2-104(1). Zeidenberg bought the product at a retail store, an uncommon place for merchants to acquire inventory. His corporation put ProCD's database on the Internet for anyone to browse, which led to the litigation but did not make Zeidenberg a software merchant.

At oral argument the Hills propounded still another distinction: the box containing ProCD's software displayed a notice that additional terms were within, while the box containing Gateway's computer did not. The difference is functional, not legal. Consumers browsing the aisles of a store can look at the box, and if they are unwilling to deal with the prospect of additional terms can leave the box alone, avoiding the transactions costs of returning the package after reviewing its contents. Gateway's box, by contrast, is just a shipping carton; it is not on display anywhere. Its function is to protect the product during transit, and the information on its sides is for the use of handlers ("Fragile!" "This Side Up!" ) rather than would-be purchasers.

Perhaps the Hills would have had a better argument if they were first alerted to the bundling of hardware and legal-ware after opening the box and wanted to return the computer in order to avoid disagreeable terms, but were dissuaded by the expense of shipping. What the remedy would be in such a case--could it exceed the shipping charges?--is an interesting question, but one that need not detain us because the Hills knew before they ordered the computer that the carton would include some important terms, and they did not seek to discover these in advance. Gateway's ads state that their products come with limited warranties and lifetime support. How limited was the warranty--30 days, with service contingent on shipping the computer back, or five years, with free onsite service? What sort of support was offered? Shoppers have three principal ways to discover these things. First, they can ask the vendor to send a copy before deciding whether to buy. The Magnuson-Moss Warranty Act requires firms [**11] to distribute their warranty terms on request, 15 U.S.C. @ 2302(b)(1)(A); the Hills do not contend that Gateway would have refused to enclose the remaining terms too. Concealment would be bad for business, scaring some customers away and leading to excess returns from others. Second, shoppers can consult public sources (computer magazines, the Web sites of vendors) that may contain this information. Third, they may inspect the documents after the product's delivery. Like Zeidenberg, the Hills took the third option. By keeping the computer beyond 30 days, the Hills accepted Gateway's offer, including the arbitration clause.

The Hills' remaining arguments, including a contention that the arbitration [**11] clause is unenforceable as part of a scheme to defraud, do not require more than a citation to Prima Paint Corp. v. Flood & Conklin Mfg. Co., 388 U.S. 395, 18 L. Ed. 2d 1270, 87 S. Ct. 1801 (1967). Whatever may be said pro and con about the cost and efficacy of arbitration (which the Hills disparage) is for Congress and the contracting parties to consider. Claims based on RICO are no less arbitrable than those founded on the contract or the law of torts. Shearson/ American Express, Inc. v. McMahon, 482 U.S. 220, [**12] 238-42, 96 L. Ed. 2d 185, 107 S. Ct. 2332 (1987). The decision of the district court is vacated, and this case is remanded with instructions to compel the Hills to submit their dispute to arbitration.
IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

CompuServe Incorporated, Plaintiff,
vs.
Cyber Promotions, Inc. and Sanford Wallace, Defendants.

Case No. C2-96-1070

Filed Feb. 3, 1997

MEMORANDUM OPINION AND ORDER

This case presents novel issues regarding the commercial use of the Internet, specifically the right of an online computer service to prevent a commercial enterprise from sending unsolicited electronic mail advertising to its subscribers.

Plaintiff CompuServe Incorporated ("CompuServe") is one of the major national commercial online computer services. It operates a computer communication service through a proprietary nationwide computer network. In addition to allowing access to the extensive content available within its own proprietary network, CompuServe also provides its subscribers with a link to the much larger resources of the Internet. This allows its subscribers to send and receive electronic messages, known as "e-mail," by the Internet. Defendants Cyber Promotions, Inc. and its president Sanford Wallace are in the business of sending unsolicited e-mail advertisements on behalf of themselves and their clients to hundreds of thousands of Internet users, many of whom are CompuServe subscribers. CompuServe has notified defendants that they are prohibited from using its computer equipment to process and store the unsolicited e-mail and has requested that they terminate the practice. Instead, defendants have sent an increasing volume of e-mail solicitations to CompuServe subscribers. CompuServe has attempted to employ technological means to block the flow of defendants' e-mail transmissions to its computer equipment, but to no avail.

This matter is before the Court on the application of CompuServe for a preliminary injunction which would extend the duration of the temporary restraining order issued by this Court on October 24, 1996 and which would extend the in addition prevent defendants from sending unsolicited advertisements to CompuServe subscribers.

For the reasons which follow, this Court holds that where defendants engaged in a course of conduct of transmitting a substantial volume of electronic data in the form of unsolicited e-mail to plaintiff's proprietary computer equipment, where defendants continued such practice after repeated demands to cease and desist, and where defendants deliberately evaded plaintiff's affirmative efforts to protect its computer equipment from such use, plaintiff has a viable claim for trespass to personal property and is entitled to injunctive relief to protect its property.
The Court will begin its analysis of the issues by acknowledging, for the purpose of providing background, certain findings of fact recently made by another district court in a case involving the Internet:

1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks . . . .

2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.

3. "The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years . . . . In all, reasonable estimates are that as any as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.

4. Some of the computers and computer networks that make up the network are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world . . . .

11. No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.


Internet users often pay a fee for Internet access. However, there is no per-message charge to send electronic messages over the Internet and such messages usually reach their destination within minutes. Thus electronic mail provides an opportunity to reach a wide audience quickly and at almost no cost to the sender. It is not surprising therefore that some companies, like defendant Cyber Promotions, Inc., have begun using the Internet to distribute advertisements by sending the same unsolicited commercial message to hundreds of thousands of Internet users at once. Defendants refer to this as "bulk e-mail," while plaintiff refers to it as "junk e-mail." In the vernacular of the Internet, unsolicited e-mail advertising is sometimes referred to pejoratively as "spam." [1]

CompuServe subscribers use CompuServe's domain name "CompuServe.com" together with their own unique alpha-numeric identifier to form a distinctive e-mail mailing address. That address may be used by the subscriber to exchange electronic mail with any one of tens of millions of other Internet users who have electronic mail capability. E-mail sent to CompuServe subscribers is processed and stored on CompuServe's proprietary computer equipment. Thereafter, it becomes accessible to CompuServe's subscribers, who can access CompuServe's equipment and electronically retrieve those messages.
Over the past several months, CompuServe has received many complaints from subscribers threatening to discontinue their subscription unless CompuServe prohibits its electronic mass mailers from using its equipment to send unsolicited advertisements. CompuServe asserts that the volume of messages generated by such mass mailings places a significant burden on its equipment which has finite processing and storage capacity. CompuServe receives no payment from the mass mailers for processing their unsolicited advertising. However, CompuServe's subscribers pay for their access to CompuServe's services in increments of time and thus the process of accessing, reviewing and discarding unsolicited e-mail costs them money, which is one of the reasons for their complaints. CompuServe has notified defendants that they are prohibited from using its proprietary computer equipment to process and store unsolicited e-mail and has requested them to cease and desist from sending unsolicited e-mail to its subscribers. Nonetheless, defendants have sent an increasing volume of e-mail solicitations to CompuServe subscribers.

In an effort to shield its equipment from defendants' bulk e-mail, CompuServe has implemented software programs designed to screen out the messages and block their receipt. In response, defendants have modified their equipment and the messages they send in such a fashion as to circumvent CompuServe's screening software. Allegedly, defendants have been able to conceal the true origin of their messages by falsifying the point-of-origin information contained in the header of the electronic messages. Defendants have removed the "sender" information in the header of their messages and replaced it with another address. Also, defendants have developed the capability of configuring their computer servers to conceal their true domain name and appear on the Internet as another computer, further concealing the true origin of the messages. By manipulating this data, defendants have been able to continue sending messages to CompuServe's equipment in spite of CompuServe's protests and protective efforts.

Defendants assert that they possess the right to continue to send these communications to CompuServe subscribers. CompuServ contends that, in doing so, the defendants are trespassing upon its personal property.

II.

The grant or denial of a motion for preliminary injunction rests within the discretion of the trial court. Deckert v. Independence Shares Corp., 311 U.S. 282 (1940). In determining whether a motion for preliminary injunction should be granted, a court must consider and balance four factors: (1) the likelihood that the party seeking the preliminary injunction will succeed on the merits of the claim; (2) whether the party seeking the injunction will suffer irreparable harm without the grant of the extraordinary relief; (3) the probability that granting the injunction will cause substantial harm to others; and (4) whether the public interest is advanced by the issuance of the injunction. Washington v. Reno, 35 F.3d 1093, 1099 (6th Cir. 1994); International Longshoremen's Assoc. v. Norfolk S. Corp., 927 F.2d 900, 903 (6th Cir. 1991). None of these individual factors constitute prerequisites that must be met for the issuance of preliminary injunction, they are instead factors that are to be balanced. In re DeLorean Motor Co., 755 F.2d 1223, 1229 (6th Cir. 1985). A preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a full trial on the merits. Indeed, "[a] party ... is not required to prove his case in full at a preliminary injunction hearing." University of Texas v. Camenisch, 451 U.S. 390, 395 (1981).

III.

This Court shall first address plaintiff's motion as it relates to perpetuating the temporary restraining order filed on October 24, 1996. That order enjoins defendants from:

(i) Using CompuServe accounts or CompuServe's equipment or support services to send or receive electronic mail or messages or in connection with the sending or receiving of electronic mail or messages;

(ii) Inserting any false reference to a CompuServe account or CompuServe equipment in any electronic message sent by Defendants; and
(iii) Falsely representing or causing their electronic mail or messages to bear the representation that any electronic mail or message sent by Defendants was sent by or originated from CompuServe or a CompuServe account.

(Temporary Restraining Order at 4).

As a general matter, the findings of this Court enunciated in its temporary restraining order are applicable to the request for preliminary injunction now at issue. The behavior described in subsections (ii) and (iii) of the temporary restraining order would be actionable as false representations or descriptions under §43 (a) of the Lanham Act, 15 U.S.C. §1125(a). Also, the same behavior is actionable under the Ohio Deceptive Trade Practices Act, Ohio Rev. Code §4165(B) and (D).

Defendants argue that the restrictions in the temporary restraining order are no longer necessary because defendants no longer have a CompuServe account. That being the case, a preliminary injunction perpetuating the proscribed activity articulated in subsection (i) of the temporary restraining order will present no hardship at all to defendants. Next, it does not appear that defendants would need to have a CompuServe account to perpetrate the proscribed acts articulated in subsections (ii) and (iii) of the temporary restraining order. Therefore, the fact that defendants no longer have an account with plaintiff does not vitiate the need which CompuServe has demonstrated for an injunction proscribing the acts set forth in those subsections.

For the foregoing reasons and the reasons articulated in the temporary restraining order issued by this Court, defendants Cyber Promotions, Inc. and its president Sanford Wallace are hereby enjoined from performing any of the acts therein described during the pendency of this litigation.

IV.

This Court will now address the second aspect of plaintiff's motion in which it seeks to enjoin defendants Cyber Promotions, Inc. and its president Sanford Wallace from sending any unsolicited advertisements to any electronic mail address maintained by CompuServe.

CompuServe predicates this aspect of its motion for a preliminary injunction on the common law theory of trespass to personal property or to chattels, asserting that defendants' continued transmission of electronic messages to its computer equipment constitutes an actionable tort.

Trespass to chattels has evolved from its original common law application, concerning primarily the asportation of another's tangible property, to include the unauthorized use of personal property:

Its chief importance now, is that there may be recovery ... for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.


The scope of an action for conversion recognized in Ohio may embrace the facts in the instant case. The Supreme Court of Ohio established the definition of conversion under Ohio law in Baltimore & O. R. Co. v. O'Donnell, 49 Ohio St. 489, 32 N.E. 476, 478 (1892) by stating that:

[I]n order to constitute a conversion, it was not necessary that there should have been an actual appropriation of the property by the defendant to its own use and benefit. It might arise from the exercise of a dominion over it in exclusion of the rights of the owner, or withholding it from his possession under a claim inconsistent with his rights. If one take the property of another, for a temporary purpose only, in disregard of the owner's right, it is a conversion. Either a wrongful taking, an assumption of ownership, an illegal use or misuse, or a wrongful detention of chattels will constitute a conversion.
Id. at 497-98; see also Miller v. Uhl, 37 Ohio App. 276, 174 N.E. 591 (1929); Great American Mut. Indemn. Co. v. Meyer, 18 Ohio App. 97 (1924); 18 O. Jur. 3d, Conversion §17. While authority under Ohio law respecting an action for trespass to chattels is extremely meager, it appears to be an actionable tort. See State of Ohio v. Herbert, 49 Ohio St.2d 88, 119, 358 N.E.2d 1090, 1106 (1976) (dissenting opinion) ("any workable cause of action would appear to be trespass to chattels"); see also Greenwald v. Kearns, 104 Ohio App. 473, 145 N.E.2d 462 (1957) (trespass on the rights of plaintiff in personal property is a precursor to an act in conversion); Simmons v. Dimitrouleas Wallcovering, Inc., No. 14804, 1995 WL 19136, at *2 (Ohio App. Jan. 18, 1995) (the court of appeals acknowledged that trespass to chattel claims were barred because those claims were dependent upon claimant's ownership of the subject personal property); Klenbriel v. Smith, No. 94CA1641, 1996 WL 57947, at *2 (Ohio App. Feb. 6, 1996) (where the court of appeals let stand a jury award on a "trespass against personal property" claim); Springfield Bank v. Casserta, 10 B.R. 57 (Bankr.S.D.Ohio 1981) (common law principles of trespass to chattels in Am. Jur. 2d applied as controlling under Ohio law).

Both plaintiff and defendants cite the Restatement (Second) of Torts to support their respective positions. In determining a question unanswered by state law, it is appropriate for this Court to consider such sources as the restatement of the law and decisions of other jurisdictions. Bailey v. V & O Press Co., Inc., 770 F.2d 601, 604-606 (6th Cir. 1985) (where court considered positions expressed in the Restatement (Second) of Torts in interpreting Ohio's principles of comparative negligence); Garrison v. Jervis B. Webb Co., 583 F.2d 258, 262 n. 6 (1978); see also Wright, Miller & Cooper, Federal Practice and Procedure, §4507 (West 1996).

The Restatement §217(b) states that a trespass to chattel may be committed by intentionally using or meddling with the chattel in possession of another. Restatement §217, Comment e defines physical "intermeddling" as follows:

... intentionally bringing about a physical contact with the chattel. The actor may commit a trespass by an act which brings him into an intended physical contact with a chattel in the possession of another.[1]

Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action. Thrifty-Tel, Inc. v. Bezenec, 46 Cal.App.4th 1559, 1567 (1996); State v. McGraw, 480 N.E.2d 552, 554 (Ind. 1985) (Indiana Supreme Court recognizing in dicta that a hacker's unauthorized access to a computer was more in the nature of trespass than criminal conversion); and State v. Riley, 121 Wash.2d 22, 846 P.2d 1365 (1993) (computer hacking as the criminal offense of "computer trespass" under Washington law). It is undisputed that plaintiff has a possessory interest in its computer systems. Further, defendants' contact with plaintiff's computers is clearly intentional. Although electronic messages may travel through the Internet over various routes, the messages are affirmatively directed to their destination.

Defendants, citing Restatement (Second) of Torts §221, which defines "dispossession", assert that not every interference with the personal property of another is actionable and that physical dispossession or substantial interference with the chattel is required. Defendants then argue that they did not, in this case, physically dispossess plaintiff of its equipment or substantially interfere with it. However, the Restatement (Second) of Torts §218 defines the circumstances under which a trespass to chattels may be actionable:

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

(c) the possessor is deprived of the use of the chattel for a substantial time, or

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.
Therefore, an interference resulting in physical dispossesssion is just one circumstance under which a defendant can be found liable. Defendants suggest that "unless an alleged trespasser actually takes physical custody of the property or physically damages it, courts will not find the "substantial interference'' required to maintain a trespass to chattel claim." (Defendant's Memorandum at 13). To support this rather broad proposition, defendants cite only two cases which make any reference to the Restatement. In Glidden v. Szymbek, 95 N.H. 318, 63 A.2d 233 (1949), the court simply indicated that an action for trespass to chattels could not be maintained in the absence of some form of damage. The court held that where plaintiff did not contend that defendant's pulling on her pet dog's ears caused any injury, an action in tort could not be maintained. Id. at 235. In contrast, plaintiff in the present action has alleged that it has suffered several types of injury as a result of defendants' conduct. In Koepnick v. Sears Roebuck & Co., 158 Ariz. 322, 762 P.2d 609 (1988) the court held that a two-minute search of an individual's truck did not amount to a "dispossession" of the truck as defined in Restatement §221 or a deprivation of the use of the truck for a substantial time. It is clear from a reading of Restatement §218 that an interference or intermeddling that does not fit the §221 definition of "dispossession" can nonetheless result in defendants' liability for trespass. The Koepnick court did not discuss any of the other grounds for liability under Restatement §218.

A plaintiff can sustain an action for trespass to chattels, as opposed to an action for conversion, without showing a substantial interference with its right to possession of that chattel. Thrifty-Tel, Inc., 46 Cal.App.4th at 1567 (quoting Zaslow v. Kroenert, 29 Cal.2d 541, 176 P.2d 1 (Cal. 1946)). Harm to the personal property or diminution of its quality, condition, or value as a result of defendants' use can also be the predicate for liability. Restatement §218(b).

An unprivileged use or other intermeddling with a chattel which results in actual impairment of its physical condition, quality or value to the possessor makes the actor liable for the loss thus caused. In the great majority of cases, the actor's intermeddling with the chattel impairs the value of it to the possessor, as distinguished from the mere affront to his dignity as possessor, only some impairment of the physical condition of the chattel. There may, however, be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition .... In such a case, the intermeddling is actionable even though the physical condition of the chattel is not impaired.

The Restatement (Second) of Torts §218, comment h. In the present case, any value CompuServe realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base. Michael Mangino, a software developer for CompuServe who monitors its mail processing computer equipment, states by affidavit that handling the enormous volume of mass mailings that CompuServe receives places a tremendous burden on its equipment. (Mangino Supp. Dec. at ¶12). Defendants' more recent practice of evading CompuServe's filters by disguising the origin of their messages commandeers even more computer resources because CompuServe's computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. (Magino Supp. Dec. at ¶7-8). To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiffs' computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

Next, plaintiff asserts that it has suffered injury aside from the physical impact of defendants' messages on its equipment. Restatement §218(d) also indicates that recovery may be had for a trespass that causes harm to something in which the possessor ha a legally protected interest. Plaintiff asserts that defendants' messages are largely unwanted by its subscribers, who pay incrementally to access their e-mail, read it, and discard it. Also, the receipt of a bundle of unsolicited messages at once can require the subscriber to sift through, at his expense, all of the messages in order to find the ones he wanted or expected to receive. These inconveniences decrease the utility of CompuServe's e-mail service and are the foremost subject in recent complaints from CompuServe subscribers. Patrick Hole, a customer service manager for plaintiff, states by affidavit that in November 1996 CompuServe received approximately 9,970 e-mail complaints from subscribers about junk e-mail, a figure up from approximately two hundred complaints the previous year. (Hole 2d Supp. Dec. at ¶4). Approximately fifty such complaints per day
specifically reference defendants. (Hole Supp. Dec. at ¶3). Defendants contend that CompuServe subscribers are provided with a simple procedure to remove themselves from the mailing list. However, the removal procedure must be performed by the e-mail recipient at his expense, and some CompuServe subscribers complain that the procedure is inadequate and ineffectual. (See, e.g., Hole Supp. Dec. at ¶8).

Many subscribers have terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages (Hole Supp. Dec. at ¶9, Hole 2d Supp. Dec. at ¶6). Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement §218(d).

The reason that the tort of trespass to chattels requires some actual damage as a prima facie element, whereas damage is assumed where there is a trespass to real property, can be explained as follows:

The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in clause (c). Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

Restatement (Second) of Torts §218, Comment e (emphasis added). Plaintiff CompuServe has attempted to exercise this privilege to protect its computer systems. However, defendants' persistent affirmative efforts to evade plaintiff's security measures have circumvented any protection those self-help measures might have provided. In this case CompuServe has alleged and supported by affidavit that it has suffered several types of injury as a result of defendants' conduct. The foregoing discussion simply underscores that the damage sustained by plaintiff is sufficient to sustain an action for trespass to chattels. However, this Court also notes that the implementation of technological means of self-help, to the extent that reasonable measures are effective, is particularly appropriate in this type of situation and should be exhausted before legal action is proper.

Under Restatement §252, the owner of personal property can create a privilege in the would-be trespasser by granting consent to use the property. A great portion of the utility of CompuServe's e-mail service is that it allows subscribers to receive messages from individuals and entities located anywhere on the Internet. Certainly, then, there is at least a tacit invitation for anyone on the Internet to utilize plaintiff's computer equipment to send e-mail to its subscribers.

Buchanan Marine, Inc. v. McCormack Sand Co., 743 F.Supp. 139 (E.D.N.Y. 1990) (whether there is consent to community use is a material issue of fact in an action for trespass to chattels). However, in or around October 1995, CompuServe employee Jon Schmidt specifically told Mr. Wallace that he was "prohibited from using CompuServe's equipment to send his junk e-mail messages." (Schmidt Dec. at ¶5). There is apparently some factual dispute as to this point, but it is clear from the record that Mr. Wallace became aware at about this time that plaintiff did not want to receive messages from Cyber Promotions and that plaintiff was taking steps to block receipt of those messages. (Transcript of December 15, 1996 Hearing at 81-86).

Defendants argue that plaintiff made the business decision to connect to the Internet and that therefore it cannot now successfully maintain an action for trespass to chattels. Their argument is analogous to the argument that because an establishment invites the public to enter its property for business purposes, it cannot later restrict or revoke access to that property, a proposition which is erroneous under Ohio law. See, e.g., State v. Carriker, 5 Ohio App.2d 255, 214 N.E.2d 809 (1964) (the law in Ohio is that a business invitee's privilege to remain on the premises of another may be revoked upon the reasonable notification to leave by the owner or his agents); Allstate Ins, Co v. U.S. Associates Realty, Inc., 11 Ohio App.3d 242, 464 N.E.2d 169 (1983) (notice express restriction or limitation on invitation turns
business invites into trespass). On or around October 1995, CompuServe notified defendants that it no longer consented to the use of its proprietary computer equipment. Defendants' continued use thereafter was a trespass. Restatement (Second) of Torts §§252 and 892A(5); see also Restatement (Second) of Torts §217, Comment f ('The actor may commit a new trespass by continuing an intermeddling which he has already begun, with or without the consent of the person in possession. Such intermeddling may persist after the other's consent, originally given, has been terminated.'); Restatement (Second) of Torts §217, Comment g.

Further, CompuServe expressly limits the consent it grants to Internet users to send e-mail to its proprietary computer system by denying unauthorized parties the use of CompuServe to equipment send unsolicited electronic mail messages. (Kolehmainen Dec. at ¶2). This policy statement, posted by CompuServe online, states as follows:

CompuServe is a private online and communications services company. CompuServe does not permit its facilities to be used by unauthorized parties to process and store unsolicited e-mail. If an unauthorized party attempts to send unsolicited messages to e-mail addresses on a CompuServe service, CompuServe will take appropriate action to attempt to prevent those messages from being processed by CompuServe. Violations of CompuServe's policy prohibiting unsolicited e-mail should be reported to ...

Id. at ¶2 and 3. Defendants Cyber Promotions, Inc. and its president Sanford Wallace have used plaintiff's equipment in a fashion that exceeds that consent. The use of personal property exceeding consent is a trespass: City of Amsterdam v. Daniel Goldreyer, Ltd., 882 F. Supp. 1273 (E.D.N.Y. 1995); Restatement (Second) of Torts §256. It is arguable that CompuServe's policy statement, insofar as it may serve as a limitation upon the scope of its consent to the use of its computer equipment, may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network. However, in the present case the record indicates that defendants were actually notified that they were using CompuServe's equipment in an unacceptable manner. To prove that a would-be trespasser acted with the intent required to support liability in tort it is crucial that defendant be placed on notice that he is trespassing.

As a general matter, the public possesses a privilege to reasonably use the facilities of a public utility, Restatement (Second) of Torts §259, but Internet service providers have been held not to be common carriers. Religious Technology Center v. Netcom on-Line Communications Services, Inc., 907 F. Supp. 1361 (N.D.Cal. 1995). The definition of public utility status under Ohio law was recently articulated in A & B Refuse Disposers, Inc. v. Bd. Of Ravenna Township Trustees, 64 Ohio St. 3d 385, 596 N.E. 2d 423 (1992). The Ohio Supreme Court held that the detrination of whether an entity is a "public utility" requires consideration of several factors relating to the "public service" and "public concern" characteristics of a public utility. Id. at 426. The public service characteristic contemplates an entity which the devotes an essential good or service to the general public which the public in turn has a legal right to demand or receive. Id at 425. CompuServe's network, Internet access and electronic mail services are simply not essential to society. There are many alternative forms of communication which are customarily used for purposes. Further, only a minority of society at large has the equipment to send and receive e-mail messages via the Internet, and even fewer actually do. The second characteristic of a public utility contemplates an entity which conducts its operations in such manner as to be a matter of public concern, that is, a public utility normally occupies a monopolistic or ogopolistic position in the relevant marketplace. Id. at 425-426. Defendants estimate that plaintiff serves some five million Internet users worldwide.

However, there are a number of major Internet service providers that have very large subscriber bases, and with a relatively minor capital investment, anyone can acquire the computer equipment necessary to provide Internet access services on a smallest scale. Furthermore, Internet users are not a "captive audience" to any single service provider, but can transfer from one service to another until they find one that best suits their needs. Finally, the Ohio Supreme Court made clear that a party asserting public utility status is required to support that assertion with evidence going to the relevant aforementioned factors. Id. at 427. Defendants have not argued that CompuServe is a public utility, much less produced evidence tending to support such a conclusion. Therefore, CompuServe is not a public utility as that status is defined under Ohio law and defendants cannot be said to enjoy a special privilege to use
CompuServe's proprietary computer systems.

In response to the trespass claim, defendants argue that they have the right to continue to send unsolicited commercial e-mail to plaintiff's computer systems under the First Amendment to the United States Constitution. The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press." The United States Supreme Court has recognized that "the constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state." Hudgens v. NLRB, 424 U.S. 507, 513 (1976). Indeed, the protection of the First Amendment is not a shield against "merely private conduct." Hurley v. Irish-American Gay Group of Boston, 515 U.S. 567, 115 S.Ct. 2338, 2344 (1995) (citation omitted).

Very recently, in an action filed by Cyber Promotions, Inc. against America Online, Inc. ("AOL") the United States District Court for the Eastern District of Pennsylvania held that AOL, a company selling services that are similar to those of CompuServe, is private actor. Cyber Promotions, Inc. v. America Online, Inc., 1996 WL 633702, *9 (E.D.Pa. 1996). That case involved the question of whether Cyber Promotions had the First Amendment right to send unobstructed e-mail to AOL subscribers. The court held that Cyber Promotions had no such right and that, inter alia, AOL was not exercising powers that are traditionally the exclusive prerogative of the state, such as where a private company exercises municipal powers by running a company town. Id. at *7; Blum v. Yaretsky, 457 U.S. 911, 1004-05 (1982); Marsh v. Alabama, 326 U.S. 501 (1946). This Court agrees with the conclusions reached by the United States District Court for the Eastern District of Pennsylvania.

In the present action, CompuServe is a private company. Moreover, the mere judicial enforcement of neutral trespass laws by the public owner of property does not alone render it a state actor. Rotunda & Nowak, Treatise on Constitutional Law §16.3, 546 (West 1992). Defendants do not argue that CompuServe is anything other than a private actor. Instead, defendants urge that because CompuServe is so intimately involved in this new medium it might be subject to some special form of regulation. Defendants cite Associated Press v. United States, 326 U.S. 1 (1945), and Turner Broadcasting Sys. Inc. v. FCC, 462 U.S. ___, 114 S.Ct. 2445 (1994), which stand for the proposition that when a private actor has a certain quantum of control over a central avenue of communication, then the First Amendment might not prevent the government from enacting legislation requiring public access to private property. No such legislation yet exists that is applicable to CompuServe. Further, defendants' discussion concerning the extent to which the Internet may be regulated (or should be regulated) is irrelevant because no government entity has undertaken to regulate the Internet in a manner that is applicable to this action. Indeed, if there were some applicable statutory scheme in place this Court would not be required to apply paradigms of common law to the case at hand.

In Lloyd Corp. v. Tanner, 407 U.S. 551 (1972), protesters of the Vietnam War sought to pass out written materials in a private shopping center. Even though the customers of the shopping center were the intended recipients of the communication, the Supreme Court held that allowing the First Amendment to trump private property rights is unwarranted where there are adequate alternative avenues of communication. Id. at 567. The Supreme Court stated that:

Although ... the courts properly have shown a special solicitude for the guarantees of the First Amendment, this Court has never held that a trespasser or an uninvited guest make exercise general rights of free speech on property privately owned and used nondiscriminatorily for private purposes only.

Id. at 567-68 (emphasis added). Defendants in the present action have adequate alternative means of communication available to them. Not only are they free to send e-mail advertisements to those on the Internet who do not use CompuServe accounts, but they can communicate to CompuServe subscribers as well through online bulletin boards, web page advertisements, or facsimile transmissions, as well as through more conventional means such as the U.S. mail or telemarketing. Defendants' contention, referring to the low cost of the electronic mail medium, that there are no adequate alternative means of communication is unpersuasive. There is no constitutional requirement that the incremental cost of sending massive quantities of unsolicited advertisements must be borne by the recipients. The legal
concept in Lloyd that private citizens are entitled to enforce laws of trespass against would-be communicators is applicable to this case.

Defendants assert that CompuServe has assumed the role of a postmaster, to whom all of the strictures of the First Amendment apply, and that to allow it to enjoy a legally protected interest in its computer equipment in this context is to license a form of censorship which violates the First Amendment. However, such an assertion must be accompanied by a showing that CompuServe is a state actor. As earlier mentioned, defendants have neither specifically argued this point nor provided any evidence to support it. CompuServe is entitled to restrict access to its private property.

"The First and Fourteenth Amendments have never been treated as absolutes. Freedom of speech or press does not mean that one can talk or distribute where, when and how one chooses." Breard v. City of Alexandria, 341 U.S. 622, 642 (1951) (upholding local ordinances banning commercial solicitations over First Amendment objections) (footnote omitted). In Rowan v. U.S. Post Office Dept., 397 U.S. 728 (1970) the United States Supreme Court held that the First Amendment did not forbid federal legislation that allowed addressees to remove themselves from mailing lists and stop all future mailings. The Court stated that the "mailer's right to communicate must stop at the mailbox of an un receptive addressee .... [t]o hold less would be to license a form of trespass [.]" Id. at 736-37.

In Tillman v. Distribution Sys. Of America, Inc., 648 N.Y.S.2d 630 (N.Y.A.D. 1996) the plaintiff complained that the defendant continued to throw newspapers on his property after being warned not to do so. The court held that the defendant newspaper distributor had no First Amendment right to continue to throw newspapers onto the property of the plaintiff. After discussing the Supreme Court cases of Rowan and Breard, supra, the court pointed out that:

The most critical and fundamental distinction between the cases cited above, on the one hand, and the present case, on the other, is based on the fact that here we are not dealing with a government agency which seeks to preempt in some way the ability of a publisher to contact a potential reader; rather, we are dealing with a reader who is familiar with a publisher's product, and who is attempting to prevent the unwanted dumping of this product on his property. None of the cases cited by the defendants stands for the proposition that the Free Speech Clause prohibits such a landowner from resorting to his common-law remedies in order to prevent such unwanted dumping. There is, in our view, nothing in either the Federal or State Constitutions which requires a landowner to tolerate a trespass whenever the trespasser is a speaker, or the distributor of written speech, who is unsatisfied with the fora which may be available on public property, and who thus attempts to carry his message to private property against the will of the owner.

Id. at 635. The court concluded, relying on Lloyd, supra, that the property rights of the private owner could not be overwhelmed by the First Amendment. Id. at 636.

In the present case, plaintiff is physically the recipient of the defendants' messages and is the owner of the property upon which the transgression is occurring. As has been discussed, plaintiff is not a government agency or state actor which seeks to preempt defendants' ability to communicate but is instead a private actor trying to tailor the nuances of its service to provide the maximum utility to its customers.

Defendants' intentional use of plaintiff's proprietary computer equipment exceeds plaintiff's consent and, indeed, continued after repeated demands that defendants cease. Such use is an actionable trespass to plaintiff's chattel. The First Amendment to the United States Constitution provides no defense for such conduct.

Plaintiff has demonstrated a likelihood of success on the merits which is sufficient to warrant the issuance of the preliminary injunction it has requested.

As already discussed at some length, plaintiff has submitted affidavits supporting its contention that it will suffer irreparable harm without the grant of the preliminary injunction. As an initial matter, it is important to point out that the Court may accept affidavits as evidence of irreparable harm. Wounded
Knee Legal Defense/Offense Committee v. Federal Bureau of Investigation, 507 F.2d 1281, 1287 (8th Cir. 1984); see generally Wright, Miller & Kane, Federal Practice and Procedure §2949, at 218-220 (West 1995). Defendant suggest that there are other reasons why CompuServe subscribers terminate their accounts, but do not offer any evidence which contradicts plaintiff's affidavits.

Normally, a preliminary injunction is not appropriate where an ultimate award of monetary damages will suffice. Montgomery v. Carr, 848 F.Sup. 770 (S.D. Ohio 1993). However, money damages are only adequate if they can be reasonably computed and collected. Plaintiff has demonstrated that defendants' intrusions into their computer systems harm plaintiff's business reputation and goodwill. This is the sort of injury that warrants the issuance of a preliminary injunction because the actual loss is impossible to compute. Basicomputer Corp. v. Scott, 973 F.2d 507 (6th Cir. 1992); Economou v. Physician's Weight Loss Centers of America, 756 F.Sup. 1024 (N.D. Ohio 1991).

Plaintiff has shown that it will suffer irreparable harm without the grant of the preliminary injunction.

It is improbable that granting the injunction will cause substantial harm to defendant. Even with the grant of this injunction, defendants are free to disseminate their advertisements in other ways not constituting trespass to plaintiff's computer equipment. Further, defendants may continue to send electronic mail messages to the tens of millions of Internet users who are not connected through CompuServe's computer systems.

Finally, the public interest is advanced by the Court's protection of the common law rights of individuals and entities to their personal property. Defendants raise First Amendment concerns and argue that an injunction will adversely impact the public interest. High volumes of junk e-mail devour computer processing and storage capacity, slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and cause recipients to spend time and money wading through messages that they do not want. It is ironic that if defendants were to prevail on their First Amendment arguments, the viability of electronic mail as an effective means of communication for the rest of society would be put at risk. In light of the foregoing discussion, those arguments are without merit. Further, those subscribing to CompuServe are not injured by the issuance of this injunction. Plaintiff has made a business decision to forbid Cyber Promotions and Mr. Wallace from using its computers to transmit messages to CompuServe subscribers. If CompuServe subscribers are unhappy with that decision, then they may make that known, perhaps by terminating their accounts and transferring to an Internet service provider which accepts unsolicited e-mail advertisements. That is a business risk which plaintiff has assumed.

Having considered the relevant factors, this Court concludes that the preliminary injunction that plaintiff requests is appropriate.

V.

Based on the foregoing, plaintiff's motion for a preliminary injunction is GRANTED. The temporary restraining order filed on October 24, 1996 by this Court is hereby extended in duration until final judgment is entered in this case. Further, defendants Cyber Promotions, Inc. and its president Sanford Wallace are enjoined from sending any unsolicited advertisements to any electronic mail address maintained by plaintiff CompuServe during the pendency of this action.

It is so ORDERED.

JAMES L. GRAHAM

United States District Judge

DATE: February 3, 1997

End Notes
1. Return to Text This term is derived from a skit performed on the British television show Monty Python's Flying Circus, in which the word "spam" is repeated to the point of absurdity in restaurant menu. That consent is apparently subject to express limitations. See Kolehmainen Dec. at ¶2 and discussion infra.

© 1997 The Bureau of National Affairs, Inc., All Rights Reserved
UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK  

AMERICAN LIBRARY  
ASSOCIATION; FREEDOM TO  
READ FOUNDATION, INC.; NEW  
YORK LIBRARY ASSOCIATION;  
WESTCHESTER LIBRARY  
SYSTEM; AMERICAN  
BOOKSELLERS FOUNDATION  
FOR FREE EXPRESSION;  
ASSOCIATION OF AMERICAN  
PUBLISHERS, INC.;  
BIBLIOBYTES, INC.; MAGAZINE  
PUBLISHERS OF AMERICA, INC.;  
INTERACTIVE DIGITAL  
SOFTWARE ASSOCIATION;  
PUBLIC ACCESS NETWORKS  
CORPORATION; ECHO; NEW  
YORK CITY NET; ART ON THE  
NET; PEACEFIRE; and AMERICAN  
CIVIL LIBERTIES UNION,  
Plaintiffs,  

97 Civ. 0222 (LAP)  

OPINION  

against  

GEORGE PATAKI, in his official  
capacity as Governor of the State of  
New York; and DENNIS VACCO, in  
his official capacity as Attorney  
General of the State of New York,  
Defendants.  

LORETTA A. PRESKA, United States District Judge:  

The Internet may well be the premier technological innovation of the present age. Judges  
and legislators faced with adapting existing legal standards to the novel environment of  
cyberspace struggle with terms and concepts that the average American five-year-old tosses  
about with breezy familiarity.¹ Not surprisingly, much of the legal analysis of  
Internet-related issues has focused on seeking a familiar analogy for the unfamiliar.  
Commentators reporting on the recent oral argument before the Supreme Court of the  
United States, which is considering a First Amendment challenge to the Communications  
Decency Act, noted that the Justices seemed bent on finding the appropriate analogy which  
would tie the Internet to some existing line of First Amendment jurisprudence: is the  
Internet more like a television? a radio? a newspaper? a 900-line? a village green? See. e.g.,  
Linda Greenhouse, What Level of Protection for Internet Speech? High Court Weighs  
Decency-Act Case, N. Y. Times, March 24, 1997, at C5; see also Denver Area Educ.  
Telecommunications Consortium v. Federal Communics. Comm'n, 116 S. Ct. 2374,  
2419-21 (1996) (Thomas, J., concurring in the judgment and dissenting in part) (criticizing  
development for declining to determine whether cable television is more closely analogous,  
for purposes of First Amendment analysis, to a print medium or a broadcast medium).
case, too, depends on the appropriate analogy. I find, as described more fully below, that the Internet is analogous to a highway or railroad. This determination means that the phrase "information superhighway" is more than a mere buzzword; it has legal significance, because the similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause.

BACKGROUND

The plaintiffs in the present case filed this action challenging New York Penal Law § 235.21(3) (the "Act" or the "New York Act"), seeking declaratory and injunctive relief. Plaintiffs contend that the Act is unconstitutional both because it unduly burdens free speech in violation of the First Amendment and because it unduly burdens interstate commerce in violation of the Commerce Clause. Plaintiffs moved for a preliminary injunction enjoining enforcement of the Act; defendants opposed the motion. A factual hearing was held from April 3 to April 7, 1997 and oral argument conducted on April 22, 1997. For the reasons that follow, the motion for a preliminary injunction is granted.

I. Parties to the Action

Plaintiffs in the present action represent a spectrum of individuals and organizations who use the Internet to communicate, disseminate, display, and access a broad range of communications. All of the plaintiffs communicate online both within and outside the State of New York, and each plaintiff's communications are accessible from within and outside New York. Plaintiffs include:

· American Library Association, Freedom to Read Foundation, Inc., New York Library Association, and Westchester Library System are organizations representing the interests of libraries. Libraries serve as both access and content providers on the Internet, providing their patrons with facilities to access the Internet. Libraries also post their card catalogues, information about upcoming events and online versions of text or art from their collections, as well as sponsoring chat rooms.

· American Booksellers Foundation For Free Expression ("ABFFE") is a national association of general interest and specialized bookstores formed to protect free expression rights. ABFFE has many members who use the Internet and electronic communications to obtain from publishers information and excerpts, some of which may contain sexually explicit passages.

· Association of American Publishers ("AAP") is a national association of publishers of general books, textbooks, and educational materials. AAP has many members who actively use and provide content on the Internet, both creating and posting electronic products and using the Internet as a communication and promotional tool for their print publishing activities.

· BiblioBytes is a private, profit-seeking enterprise that uses the World Wide Web (the "Web") to provide information about and to sell electronic books. BiblioBytes offers titles in a variety of genres, including romance, erotica, classics, adventure, and horror.

· Magazine Publishers of America ("MPA") is a national association of publishers of consumer magazines. MPA's members publish magazines in print form, but are also beginning to offer publications in electronic formats available to the public on the Internet or through online service providers.

· Interactive Digital Software Association ("IDSA") is a non-profit trade association of United States publishers of entertainment software. IDSA has many members who both sell their software in retail outlets and make their entertainment software available to the public on the Internet for demonstration, purchase, and play.
· Public Access Networks Corporation ("Panix") is an Internet service provider serving subscribers located in the New York area. Panix also hosts various organizational Web pages, assists its subscribers in creating individual Web pages, and hosts online discussion groups and chat rooms.

· ECHO is a for-profit Internet service provider that offers a "virtual salon" to Internet users. ECHO and its subscribers provide content on the Internet through the posting of Web sites, including personal home pages, and through over 50 discussion groups oriented to subscribers' interests.

· New York City Net ("NYC Net") is a for-profit Internet service provider catering primarily to lesbians and gay men in the New York area. NYC Net provides access services and content specifically oriented to gay and lesbian interests, including a large number of online discussion groups and chat rooms.

· Art on the Net is a non-profit organization with an international artist site ("art.net") on the Web. Art on the Net assists over 110 artists from all over the world in maintaining online studios.

· Peacefire is an organization whose membership consists primarily of minors. It was formed to protect the rights of citizens under the age of 18 to use the Internet. Peacefire's members use the Internet to communicate and access a wide variety of information. Peacefire's founder points out in his Declaration that Internet access is particularly important to those members who are too young to drive and might otherwise be unable to view materials from museums, libraries, and other institutions to which their families are unwilling to transport them. (See Declaration of Bennett Haselton, sworn to on March 12, 1997, at p. 4.

· American Civil Liberties Union ("ACLU") is a national civil rights organization. The ACLU maintains a Web site on which it posts civil liberties information and resources, including material about arts censorship, obscenity laws, discrimination against lesbians and gays, and reproductive choice. In addition, the ACLU hosts unmoderated online discussion groups that allow citizens to discuss and debate a variety of civil liberties issues.

Defendants in this case are the Governor and the Attorney General of New York. Defendants have raised the question of whether an injunction against those parties would also bind the sixty-two District Attorneys in New York who would actually be mounting prosecutions against alleged violators of the Act. Fed. R. Civ. P. 65(d) provides:

Every order granting an injunction . . . is binding only upon the parties to the action, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise.

Thus, parties such as the local District Attorneys who "participate" in the enjoined activities with defendants and who have actual notice of the injunction would be bound. See American Booksellers v. Webb, 590 F. Supp. 677, 693-94 (N.D. Ga. 1984) (holding that an injunction against the Attorney General also binds state law enforcement officials who might seek to enforce the challenged Act); see also United Transportation Union v. Long Island RR Co., 634 F.2d 19, 22 (2d Cir. 1980) (binding non-party Attorney General to the terms of an injunction against the defendants because Attorney General "undoubtedly had knowledge of the instant action and could have participated therein had he chosen to do so"), rev'd on other grounds, 455 U.S. 678 (1982). Thus, a preliminary injunction would effectively bar enforcement of the Act whether the prosecution happened to be brought directly by the Attorney General's office or by one of the individual District Attorneys.
II. The Challenged Statute

The Act in question amended N.Y. Penal Law § 235.21 by adding a new subdivision. The amendment makes it a crime for an individual:

Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, [to] intentionally use[] any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.

Violation of the Act is a Class E felony, punishable by one to four years of incarceration. The Act applies to both commercial and non-commercial disseminations of material.

Section 235.20(6) defines "harmful to minors" as:

that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado- masochistic abuse, when it:

(a) Considered as a whole, appeals to the prurient interest in sex of minors; an

(b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and

(c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20 (6).

The statute provides six defenses to liability. First, Section 235.15(1) provides the following affirmative defense to prosecution under § 235.21(3):

In any prosecution for obscenity, or disseminating indecent material to minors in the second degree in violation of subdivision three of section 235.21 of this article, it is an affirmative defense that the persons to whom the allegedly obscene or indecent material was disseminated, or the audience to an allegedly obscene performance, consisted of persons or institutions having scientific, educational, governmental or other similar justification for possessing, disseminating or viewing the same.

The statute further provides four regular defenses to prosecution:

(a) The defendant made a reasonable effort to ascertain the true age of the minor and was unable to do so as a result of the actions taken by the minor; or

(b) The defendant has taken, in good faith, reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to materials specified in such subdivision, which may involve any appropriate measures to restrict minors from access to such communications, including any method which is feasible under available technology; or

(c) The defendant has restricted access to such materials by requiring use of a verified credit card, debit account, adult access code or adult personal identification number; or

(d) The defendant has in good faith established a mechanism such that the
labelling, segregation or other mechanism enables such material to be automatically blocked or screened by software or other capabilities reasonably available to responsible adults wishing to effect such blocking or screening and the defendant has not otherwise solicited minors not subject to such screening or blocking capabilities to access that material or circumvent any such screening or blocking.

N.Y. Penal Law § 235.23(3). And, finally, Section 235.24 provides that no individual shall be held liable:

[S]olely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that do not include the creation of the content of the communication.

N.Y. Penal Law § 235.24. Exceptions to this defense for conspirators or co-owners and an additional employer liability defense are set forth in Section 235.24(1)(a)-(b) and (2).

III. The Internet

The Internet is a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), prob. juris. noted, 117 S. Ct. 554 (1996), argued, March 19, 1997; Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996), argued, March 19, 1997. The nature of the Internet makes it very difficult, if not impossible, to determine its size at any given moment. Undoubtedly, however, the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet; in 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, 60% of them located in the United States, are linked to the Internet. This count does not include users who access the Internet via modem link-up from their personal computers. As many as 40 million people worldwide currently enjoy access to the Internet's rich variety of resources, and that number is expected to grow to 200 million by the year 1999.

The Internet is a network of networks -- a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls the Internet; in fact, the chaotic, random structure of the Internet precludes any exercise of such control.

The information available on the Internet is "as diverse as human thought," ACLU, 929 F. Supp. at 842. Every facet of art, literature, music, news, and debate is represented. There can be no question that the overwhelming variety of available information includes some sexually explicit materials. Sexually-oriented content is, however, not "the primary type of content on this new medium." Id.

Individuals obtain access to the Internet via a number of avenues. Students and faculty often obtain access via their educational institutions; similarly, some corporations provide their employees with direct or modem access to the Internet. Individuals in some communities can access the Internet via a community network or a local library that provides direct or modem access to library patrons. Storefront "computer coffee shops" offer another option, serving up access to cyberspace accompanied by coffee and snacks for a small hourly fee. "Internet service providers" typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including plaintiffs Panix, Echo, and NYC NET -- are commercial entities offering Internet access for a monthly or hourly fee. Another common way for individuals to access the Internet is through one of the
major national commercial "online services" such as America Online, Compuserve, the Microsoft Network, or Prodigy, which collectively service almost twelve million individual subscribers across the United States. These online services offer nationwide computer networks (allowing subscribers to dial in via a local telephone number) and provide both proprietary content and links to the even more extensive resources of the Internet for a monthly or hourly fee. Finally, local dial-in computer services, called "bulletin board systems" or "BBSs" provide Internet access via direct or indirect links.

The Internet permits a user to communicate pictures and text in several ways including:

1. one-to-one messaging (such as "e-mail");
2. one-to-many messaging (such as "listserv" or "mail exploder");
3. distributed message databases (such as "USENET newsgroups");
4. real time remote computer utilization (such as "Internet Relay Chat");
5. real time remote computer utilization - (such as "telnet"); and
6. remote information retrieval (such as "ftp", "gopher," and the Web).

In addition to transmitting pictures and text, many of these communication methods can be used to transmit data, computer programs, sound, and moving video images.

Most users of the Internet are provided with a username, password and e-mail address that allow them to sign on to the Internet and communicate with other users. Many usernames are pseudonyms, known as "handles," which provide users with a distinct online identity and preserve anonymity. For example, Ms. Kovacs testified that she uses the handle "Harriet Vane" when communicating with fellow mystery aficionados in the "Dorothy L" listserv and the nom de cyber "Mrs. Archangel" when she's just "goofing off" on the Internet. (4/4/97 Tr., at 58). The username and e-mail address are the only indicators of a user's identity; generally speaking, neither datum discloses a party's age or geographic location.

E-mail is the simplest method of Internet communication. E-mail allows an online user to address and transmit an electronic message to one or more people. The ACLU court noted that e-mail is "comparable in principle to sending a first class letter." ACLU, 929 F. Supp. at 834. The analogy is not a perfect one, however, for two reasons. First, the sender directs his message to a logical rather than geographic address, and therefore need not know the location of his correspondent in real space. Second, most programs provide for a "reply" option which enables the recipient to respond to the sender's message simply by clicking on a button; the recipient will therefore not even need to type in the sender's e-mail address. A further distinction concerns the level of security that protects a communication. While first-class letters are sealed, e-mail communications are more easily intercepted. Concerns about the relatively easy accessiblility of e-mail communications have led bar associations in some states to require that lawyers encrypt sensitive e-mail messages in order to protect client confidentiality. See Carey Ramos & Curtis Carmack, Beware of Cyberspace Marauders: Internet Security Addressed, N.Y.L.J., February 24, 1997, at S1.

The Internet also includes a wide variety of online discussion fora that allow groups of users to discuss and debate subjects of interest. The three most common means by which such discussion groups come together are through mail exploders, USENET newsgroups, and chat rooms.

Mail exploders, also known as "listservs," allow online users to subscribe to automated mailing lists that disseminate information on particular subjects. Subscribers send an e-mail message to the "list," and the mail exploder automatically and simultaneously sends the message to all of the other subscribers on the list. Users of mailing lists can add or delete their names from the list automatically, without any direct human involvement. Id. at 834; Shea, 930 F. Supp. at 927.
USENET newsgroups are a very popular set of discussion groups arranged according to subject matter and automatically disseminated "using ad hoc peer to peer connections between approximately 200,000 computers . . . around the world." ACLU, 929 F. Supp. at 834-35. Users may read or send messages to newsgroups without any prior subscription, and there is no way for a speaker who posts an article to a newsgroup to know who is reading the message. Id.; Shea, 930 F. Supp. at 927-28. Currently, more than 15,000 different subjects are represented in USENET newsgroups, and over 100,000 new messages are posted to these groups every day. ACLU, 929 F. Supp. at 835.

Chat rooms allow online discussion in real time. Users are able to engage in simultaneous conversations with one or many "occupants" by typing in messages and reading the messages typed by others participating in the chat; the ACLU court analogized this Internet application to a telephone party line. ACLU, 929 F. Supp. at 835; Shea, 930 F. Supp. at 928. There are thousands of different chat rooms available "in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects." ACLU, 929 F. Supp. at 835.

Finally, perhaps the most well-known method of communicating information online is the Web; many laypeople erroneously believe that the Internet is co-extensive with the Web. The Web is really a publishing forum; it is comprised of millions of separate "Web sites" that display content provided by particular persons or organizations. Any Internet user anywhere in the world with the proper software can create a Web page, view Web pages posted by others, and then read text, look at images and video, and listen to sounds posted at these sites. Many large corporations, banks, brokerage houses, newspapers and magazines provide online editions of their reports and publications or operate independent Web sites. Government agencies and even courts use the Web to disseminate information to the public. At the same time, many individual users and small community organizations have established individual "home pages" on the Web that provide information to any interested person who "surfs by."

Although information on the Web is contained on innumerable Web sites located on individual computers around the world, each of these Web sites and computers is connected to the Internet by means of protocols that permit the information to become part of a single body of knowledge accessible by all Web visitors. ACLU, 929 F. Supp. at 836, 837. To gain access to the resources of the Web, an individual employs a "browser." A browser is software, such as Netscape Navigator, Mosaic, or Internet Explorer, that allows the user to display, print, and download documents that are formatted in the standard Web formatting language. Shea, 930 F. Supp. at 929.

There are a number of different ways that Internet users can browse or search for content on the Web. First, every document on the Web has an address that allows users to find and retrieve it, and a user can simply type in the address and go directly to that site. Again, however, the address is a logical rather than geographic concept, and the user will not necessarily know where the site is located in real space. Additionally, a user who wants to conduct a generalized search or wants to reach a particular site but does not know the address, can use a "search engine," which is available free of charge to help users navigate the Web. ACLU, 929 F. Supp. at 837. The user simply types a word or string of words as a search request, and the search engine provides a list of sites that match the search string. Id.

Finally, online users may "surf" the Web by "linking" from one Web page to another. Almost all Web documents contain "links," segments of text or images that refer to another Web document. Id. at 836. When the user clicks on the link, the linked document is automatically displayed, wherever in the world it is stored. Id. For example, the American Library Association ("ALA") home page contains several links. Some of these links are to other Web pages or documents within the ALA site, including documents entitled "Libraries Online," "Library Promotional Events," and the "ALA Bookstore." Other links from the ALA home page connect the user to sites maintained by other organizations or individuals.
and stored on other computers around the world. The ALA Web site, for example, provides links to the American Association of Law Libraries, the Art Libraries Society of North America, and the Medical Library Association. "These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique." Id. at 836-37.

Regardless of the aspect of the Internet they are using, Internet users have no way to determine the characteristics of their audience that are salient under the New York Act -- age and geographic location. In fact, in online communications through newsgroups, mailing lists, chat rooms, and the Web, the user has no way to determine with certainty that any particular person has accessed the user's speech. "Once a provider posts content on the Internet, it is available to all other Internet users worldwide." Id. at 844. A speaker thus has no way of knowing the location of the recipient of his or her communication. As the poet said, "I shot an arrow into the air; it fell to the earth I know not where."

This highly simplified description of the Internet is not intended to minimize its marvels. While no one should lose sight of the inventiveness that has made this complex of resources available to just about anyone, the innovativeness of the technology does not preclude the application of traditional legal principles -- provided that those principles are adaptable to cyberspace. In the present case, as discussed more fully below, the Internet fits easily within the parameters of interests traditionally protected by the Commerce Clause. The New York Act represents an unconstitutional intrusion into interstate commerce; plaintiffs are therefore entitled to the preliminary injunction that they seek.

DISCUSSION

I. Standard Applicable to a Preliminary Injunction

To demonstrate their entitlement to a preliminary injunction, plaintiffs must show (a) that they will suffer irreparable harm and (b) either (i) a likelihood of success on the merits or (ii) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in the plaintiffs' favor. Paulsen v. County of Nassau, 925 F.2d 65, 68 (2d Cir. 1991); Streetwatch v. National R.R. Passenger Corp., 875 F. Supp. 1055, 1058 (S.D.N.Y. 1995). In the present case, as discussed more fully below, plaintiffs have amply demonstrated the likelihood of their successful prosecution of their claim that the Act violates the Commerce Clause because it seeks to regulate communications occurring wholly outside New York, imposes a burden on interstate commerce that is disproportionate to the local benefits it is likely to engender, and subjects plaintiffs, as well as other Internet users, to inconsistent state obligations. See Healy v. Beer Institute, 491 U.S. 324, 332 (1989); Pike v. Bruce Church. Inc., 397 U.S. 137, 142 (1970); Southern Pac. Co. v. Arizona ex rel. Sullivan, 325 U.S. 761, 767 (1945).

Plaintiffs have also shown that they face irreparable injury in the absence of an injunction. Irreparable injury means "the kind of injury for which money cannot compensate," Sperry Intl Trade. Inc. v. Government of Israel, 670 F.2d 8, 12 (2d Cir. 1982), and which is "neither remote nor speculative, but actual and imminent." Tucker Anthony Realty Corp. v. Schlesinger, 888 F.2d 969, 975 (2d Cir. 1989). Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury. C & A Carbine. Inc. v. Town of Clarkstown, 770 F. Supp. 848, 854 (S.D.N.Y. 1991) (holding that a local waste disposal law caused irreparable injury to the plaintiffs' rights under the Commerce Clause). Thus, by demonstrating that the Act threatens their rights under the Commerce Clause, as will be discussed more fully below, the plaintiffs have shown both irreparable injury and a likelihood of success on the merits.

II. Federalism and the Internet: The Commerce Clause

The borderless world of the Internet raises profound questions concerning the relationship
among the several states and the relationship of the federal government to each state, questions that go to the heart of "our federalism." See Younker v. Harris, 401 U.S. 37, 44 (1971) ("[O]ne familiar with the profound debates that ushered our Federal Constitution into existence is bound to respect those who remain loyal to the ideals and dreams of 'Our Federalism.' The concept does not mean blind deference to 'States' Rights' any more than it means centralization of control over every important issue in our National Government and its courts. The Framers rejected both these courses.") The Act at issue in the present case is only one of many efforts by state legislators to control the chaotic environment of the Internet. For example, the Georgia legislature has enacted a recent law prohibiting Internet users from "falsely identifying" themselves online. Ga. Stat. 16-9-9.1. Similar legislation is pending in California. California Senate Bill SB-1533 (1996); see also Ilana DeBare, State Trademark Bill Ignites Net Turmoil, The Sacramento Bee, March 2, 1991, at F1. Texas and Florida have concluded that law firm web pages (apparently including those of out of state firms) are subject to the rules of professional conduct applicable to attorney advertising. See Texas Bar Advertising Comm., Interpretive Comment on Attorney Internet Advertising (1996); see also Texans Against Censorship v. State Bar of Texas, 888 F. Supp. 1328, 1369-70 (E.D. Tex. 1995) (discussing applicability of Texas lawyers advertising regulation to the Internet), aff'd, 100 F.3d 953 (5th Cir. 1996); Ethics Update, Fla. Bar News, January 1, 1996. Further, states have adopted widely varying approaches in the application of general laws to communications taking place over the Internet. Minnesota has aggressively pursued out-of-state advertisers and service providers who reach Minnesotans via the Internet; Illinois has also been assertive in using existing laws to reach out-of-state actors whose connection to Illinois occurs only by virtue of an Internet communication. See Mark Eckenwiler, States Get Entangled in the Web, Legal Times, Jan. 22, 1996, at S35, S37. Florida has taken the opposite route, declining to venture into online law enforcement until various legal issues (including, perhaps, the one discussed in the present opinion) have been determined. Id. at S37.4

The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation -- and in particular, the national infrastructure of communications and trade -- as a whole. See Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992) ("Under the Articles of Confederation, state taxes and duties hindered and suppressed interstate commerce; the Framers intended the Commerce Clause as a cure for these structural ills."); see also The Federalist Nos. 7, 11 (A. Hamilton).

The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in Gibbons v. Ogden, 9 Wheat. 1, 231-32, 239 (1824), recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, see, e.g., Philadelphia v. New Jersey, 437 U.S. 617 (1978), and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce, see, e.g., Kassel v. Consolidated Freightways Corp. of Del., 450 U.S. 662 (1981). Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause. See e.g., Wabash St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557 (1887) (holding railroad rates exempt from state regulation).

Thus, as will be discussed in more detail below, the New York Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons. First, the Act
represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.

A. The Act Concerns Interstate Commerce

At oral argument, the defendants advanced the theory that the Act is aimed solely at intrastate conduct. This argument is unsupportable in light of the text of the statute itself, its legislative history, and the reality of Internet communications. The section in question contains no such limitation; it reads:

A person is guilty of disseminating indecent material to minors in the second degree when:

....

(3) Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sadomasochistic abuse, and which is harmful to minors, he intentionally uses any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.

N.Y. Penal Law § 235.21(3) (McKinney's 1997). Section 235.20, which contains the definitions applicable to thecharged portion of the Act, does not import any restriction that the criminal communication must take place entirely within the State of New York. By its terms, the Act applies to any communication, intrastate or interstate, that fits within the prohibition and over which New York has the capacity to exercise criminal jurisdiction. See Boyd v. Meachum, 77 F.3d 60, 65 (2d Cir. 1996) (holding that a criminal court "has personal jurisdiction over any party who appears before it, regardless of how his appearance was obtained"), cert. denied, 117 S. Ct. 114 (1996); see also United States v. Lussier, 929 F.2d 25, 27 (1st Cir. 1991); United States v. Stuart, 689 F.2d 759, 762 (8th Cir. 1982), cert. denied, 460 U.S. 1037 (1983).

Further, the legislative history of the Act clearly evidences the legislators' understanding and intent that the Act would apply to communications between New Yorkers and parties outside the State, despite occasional glib references to the Act's "intrastate" applicability. The New York State Senate Introducer's Memorandum in Support of the Act contains a paragraph under the subtitle, "Justification," which states:

Law enforcement agencies around the nation are becoming increasingly alarmed at the growing use of computer networks and other communications by pedophiles. As one observer noted, "perverts are moving from the playground to the internet." Several cases have come to light wherein a pedophile has traveled clear across the country to have sexual relations with a minor initially contacted and engaged through various computer networks.

(Affidavit of James Hershler, Exh. D) (emphasis added). A letter from the Bill's sponsor to Governor Pataki characterized sexually-infused Internet communications between adults and minors as "long-distance, high-tech sexual abuse." (See Letter dated July 11, 1996 from...
William Sears to Governor Pataki, designated page 3 in the Bill Jacket, Hershler Aff., Exh. A). Jeanine Pirro, the Westchester County District Attorney, wrote a letter to Governor Pataki dated February 13, 1996 that similarly reflects the expectations of the Act's proponents that it would apply to interstate communications. Ms. Pirro's letter states:

This bill was proposed partly in response to a Westchester County case wherein an adult male resident of Seattle, Washington, [one Alan Paul Barlow,] communicated about sexually explicit matters by computer with a thirteen year old girl over several months.

(Hershler Aff., Exh. F); see also John Heileman, The Crusader, The New Yorker, February 24 and March 3, 1997 (detailing Ms. Pirro's "crusade" to achieve the passage of the Act in the aftermath of the Barlow incident).\(^5\) Ms. Pirro's references to this incident, known as the Barlow case, are echoed throughout defendants' memorandum of law. (See Defendants' Memorandum of Law in Opposition to Preliminary Injunction, pp. 15, 16, 17-18).

Obviously, however, the Act would be completely ineffective in forestalling a pedophile like Barlow if it applied only to purely intrastate communications. The conclusion that the Act must apply to interstate as well as intrastate communications receives perhaps its strongest support from the nature of the Internet itself. The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading. For example, in his article, Federalism in Cyberspace, 28 Conn. L. Rev. 1095, 1112 (1996), Professor Dan Burk described how he uses Seton Hall University's computer system to access the Internet, providing anyone who communicates with him (and is aware of Seton Hall's locale) a hint that he is in New Jersey. However, Professor Burk also has a guest account at a university in California which he continues to use even when he is in New Jersey; any clue derived from the California university's name within the Internet address would therefore be deceptive. In a similar vein, Ms. Kovacs testified that as she was using her computer to give an in-court demonstration of various Internet applications, she received an e-mail from a colleague who believed she was sending the message to Cincinnati, Ohio (where Ms. Kovacs is normally located); in fact, Ms. Kovacs was in New York and received the message here. (4/4/97 Tr., p. 61).

Moreover, no aspect of the Internet can feasibly be closed off to users from another state. An internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail. Nor can a participant in a chat room prevent other participants from a particular state from joining the conversation. Someone who uses a mail exploder is similarly unaware of the precise contours of the mailing list that will ultimately determine the recipients of his or her message, because users can add or remove their names from a mailing list automatically. Thus, a person could choose a list believed not to include any New Yorkers, but an after-added New Yorker would still receive the message.\(^6\)

E-mail, because it is a one-to-one messaging system, stands on a slightly different footing than the other aspects of the Internet. Even in the context of e-mail, however, a message from one New Yorker to another New Yorker may well pass through a number of states en route. The Internet is, as described above, a redundant series of linked computers. Thus, a message from an Internet user sitting at a computer in New York may travel via one or more other states before reaching a recipient who is also sitting at a terminal in New York.

The system is further complicated by two Internet practices: packet switching and caching. "Packet switching" protocols subdivide individual messages into smaller packets that are
then sent independently to the destination, where they are automatically reassembled by the receiving computer. If computers along the route become overloaded, packets may be rerouted to computers with greater capacity. A single message may -- but does not always -- travel several different pathways before reaching the receiving computer. "Caching" is the Internet practice of storing partial or complete duplicates of materials from frequently accessed sites to avoid repeatedly requesting copies from the original server. The recipient has no means of distinguishing between the cached materials and the original. Thus, the user may be accessing materials at the original site, or he may be accessing copies of those materials cached on a different machine located anywhere in the world.

The New York Act, therefore, cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist. No user could reliably restrict her communications only to New York recipients. Moreover, no user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a Web site, receiving a mail exploder message or a newsgroup posting, or participating in a chat room. Similarly, a user has no way to ensure that an e-mail does not pass through New York even if the ultimate recipient is not located there, or that a message never leaves New York even if both sender and recipient are located there.

This conclusion receives further support from the unchallenged testimony that plaintiffs introduced in the form of declarations. For example, Stacy Horn, the president of ECHO, an electronic cultural salon, testified that "[c]onference participants do not know, and have no way to determine, the . . . geographic location of other participants." (Decl. of Stacy Horn, sworn to on March 12, 1997, at p. 6). Oren Teicher, the President of the American Booksellers Foundation for Free Expression, indicated that:

Much of the Internet use by booksellers is interstate in nature. For example, any bookseller's Web page can be accessed by Internet users not only throughout the United States, but throughout the world. Similarly, ABFFE members from across the country communicate with one another as well as Internet users across the country via e-mail. Moreover, ABFFE users cannot effectively prevent their Web sites or discussion groups from being accessed by New York users.

(Decl. of Oren Teicher, sworn to on March 26, 1997, at p. 4). Lawrence J. Kaufman, the Vice President of the Magazine Publishers of America, Inc., a trade association for the consumer magazine industry, noted that "On-line users anywhere in the world can access the content provided by MPA members on the Web and via e-mail. These members cannot effectively prevent their Web sites from being accessed by New York users." (Decl. of Lawrence J. Kaufman, sworn to on March 26, 1997, at p.2).

The Act is therefore necessarily concerned with interstate communications. See Virginia v. American Booksellers Assn., Inc., 484 U.S. 383, 397 (1988) (holding that only if a statute is "readily susceptible" to a narrowing construction will the court apply such a construction to save an otherwise unconstitutional law). The next question that requires an answer as a threshold matter is whether the types of communication involved constitute "commerce" within the meaning of the Clause.

The definition of commerce in the Supreme Court's decisions has been notably broad. Most recently, in Camps Newfound Owatonna, Inc. v. Town of Harrison, Maine, 1997 WL 255351 (May 19, 1997), the Court rejected defendant's arguments that the Commerce Clause was inapplicable to a discriminatory real estate tax deduction, either because "campers are not 'articles of commerce'" or because the plaintiff camp's "product is delivered and 'consumed' entirely within Maine." Id. at *5. In the past, the Court has held that interstate commerce is affected by private race discrimination that limited access to a hotel and thereby impeded interstate commerce in the form of travel. Heart of Atlanta
Motel, Inc. v. United States, 379 U.S. 241, 244, 258 (1964).

In the present case, the parties have stipulated that:

The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The other forms of Internet communication -- e-mail, bulletin boards, newsgroups, and chat rooms -- frequently have non-commercial goals. For the economic and technical reasons set forth in the following paragraphs, the Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences. There are examples in the plaintiffs' affidavits of some of the non-commercial uses that the Internet serves. Plaintiff Peacefire offers information on its Internet site regarding the rights of minors on the Internet. Plaintiff Art on the Net allows artists to post their works on the World Wide Web. Plaintiff American Civil Liberties Union offers information on civil liberties issues.

(Joint Stipulation of Facts, ¶ 79). This stipulation, however inartfully worded, cannot insulate the statute at issue from Commerce Clause scrutiny. The non-profit nature of certain entities that use the Internet or of certain transactions that take place over the Internet does not take the Internet outside the Commerce Clause. See Camps Newfoundland, at *6; Hughes v. Oklahoma, 441 U.S. 322, 326 n.2 (1979); Philadelphia v. New Jersey, 437 U.S. 617, 621-23 (1978).

The Supreme Court has expressly held that the dormant commerce clause is applicable to activities undertaken without a profit motive. In Edwards v. California, 314 U.S. 160 (1941), the Court examined the constitutionality of a California statute prohibiting the transport of indigent people into the state. The Court struck the statute as violative of the dormant Commerce Clause, reasoning that "the transportation of persons is 'commerce,'" and that the California law at issue raised an "unconstitutional barrier to that commerce." Id. at 172-73. In making its threshold determination, the Court emphasized that "[i]t is immaterial whether or not the transportation is commercial in character." Id. at 172, n.1; see also Caminetti v. United States, 242 U.S. 470, 491 (1917); Hoke v. United States, 227 U.S. 308, 320 (1913).

Commercial use of the Internet, moreover, is a growing phenomenon. See, e.g., Don Clark, Disney Launching Children's Web Site Only on Microsoft's On-Line Service, Wall St. Journal, March 31, 1997 (describing Disney's efforts to create and market a fee-based Web service); see also Andrew Bowser, Advertising on the Net, New Orleans Citybusiness, March 6, 1995; John Casey, Growing Potential of World Wide Web, Business & Finance, The Irish Times, June 3, 1996. In addition, many of those users who are communicating for private, noncommercial purposes are nonetheless participants in interstate commerce by virtue of their Internet consumption. Many users obtain access to the Internet by means of an on-line service provider, such as America Online, which charges a fee for its services. "Internet service providers," including plaintiffs Panix, Echo, and NYC NET, also offer Internet access for a monthly or hourly fee. Patrons of storefront "computer coffee shops," such as New York's own CyberCafe, similarly pay for their access to the Internist, in addition to partaking of food and beverages sold by the cafe. Dial-in bulletin board systems often charge a fee for access. See Katzenbach v. McClung, 379 U.S. 294, 300-301 (1964) (holding that an entity that purchases goods used in the provision of its services from interstate sources is an actor in interstate commerce even in connection with the provision of services within a single state).

The courts have long recognized that railroads, trucks, and highways are themselves "instruments of commerce," because they serve as conduits for the transport of products and
services. See Kassel v. Consolidated Freightways Corp., 450 U.S. 662 (1981); Southern Pacific Co. v. Arizona, 325 U.S. 761, 780 (1945). The Internet is more than a means of communication; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos which can be downloaded from the provider's site to the Internet user's computer. For example, plaintiff BiblioBytes and members of plaintiff IDSA both sell and deliver their products over the Internet.

The inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations. The New York Act is therefore closely concerned with interstate commerce, and scrutiny of the Act under the Commerce Clause is entirely appropriate. As discussed in the following sections, the Act cannot survive such scrutiny, because it places an undue burden on interstate traffic, whether that traffic be in goods, services, or ideas.

B. New York Has Overreached by Enacting a Law That Seeks To Regulate Conduct Occurring Outside its Borders

The interdiction against direct interference with interstate commerce by state legislative overreaching is apparent in a number of the Supreme Court's decisions. In Baldwin v. G.A.F. Seelig Inc., 294 U.S. 511, 521 (1935), for example, Justice Cardozo authored an opinion enjoining enforcement of a law that prohibited a dealer from selling within New York milk purchased from the producer in Vermont at less than the minimum price fixed for milk produced in New York. Justice Cardozo sternly admonished, "New York has no power to project its legislation into Vermont by regulating the price to be paid in that state for milk," finding that "[s]uch a power, if exerted, [would] set a barrier to traffic between one state and another as effective as if customs duties, equal to the price differential, had been laid upon the thing transported." Id.

The Court has more recently confirmed that the Commerce Clause precludes a state from enacting legislation that has the practical effect of exporting that state's domestic policies. In Edgar v. MITE, 457 U.S. 624 (1982), the Court examined the constitutionality of an Illinois anti-takeover statute that required a tender offeror to notify the Secretary of State and the target company of its intent to make a tender offer and the terms of the offer 20 days before the offer became effective. During the twenty-day period, the offeror was barred from communicating its offer to the shareholders, but the target company was free to disseminate information to its shareholders concerning the impending offer. Id. at 633. The statute defined "target company" as a corporation of which Illinois shareholders own 10% of the class of securities subject to the takeover offer, or for which any two of the following conditions are met: the corporation has its principal office in Illinois, is organized under Illinois law, or has at least 10% of its stated capital and paid-in surplus within Illinois. Id. at 625. The Court acknowledged that states traditionally retained the power to regulate intrastate securities transactions by enacting "blue-sky laws." Id. at 641. Nonetheless, the Court asserted that "[t]he Illinois Act differs substantially from state blue-sky laws in that it directly regulates transactions which take place across state lines, even if wholly outside the State of Illinois." Id. In striking the law as violative of the Commerce Clause, the Court found particularly egregious the fact that the Illinois law on its face would apply to a transaction that would not affect a single Illinois shareholder if a corporation fit within the definition of a "target company." Id. at 642. The Court concluded "the Illinois statute is a direct restraint on interstate commerce and has a sweeping extraterritorial effect," because the statute would prevent a tender offeror from communicating its offer to shareholders both within and outside Illinois. Acceptance of the offer by any of the shareholders would result in interstate transactions; the Illinois statute effectively stifled such transactions during the waiting period and thereby disrupted prospective interstate commerce. Under the Commerce Clause, the projection of these extraterritorial "practical effect[s]," regardless of the legislators' intentions, "exceed the inherent limits of the State's power." Id. at 642-43 (quoting Shaffer v. Heitner, 433 U.S. 186, 197 (1977)).
In the present case, a number of witnesses testified to the chill that they felt as a result of the enactment of the New York statute; these witnesses refrained from engaging in particular types of interstate commerce. In particular, I note the testimony of Rudolf Kinsky, an artist with a virtual studio on Art on the Net's Website. Mr. Kinsky testified that he removed several images from his virtual studio because he feared prosecution under the New York Act. (4/7/97 Tr., at 231-35). As described above, no Web siteholder is able to close his site to New Yorkers. Thus, even if Mr. Kinsky were located in California and wanted to display his work to a prospective purchaser in Oregon, he could not employ his virtual studio to do so without risking prosecution under the New York law.

Oren Teicher, the President of the American Booksellers Foundation for Free Expression, similarly testified to the stifling effects that the Act will have on prospective interstate commerce in books, stating that:

The Internet is an important source of interstate business for ABFFE members . . . Booksellers conduct business over the Internet in a variety of ways. If the Act is not enjoined and ABFFE members are forced to self-censor rather than be subject to criminal liability, they will suffer immeasurable injury because they will lose significant sales and goodwill generated by their use of the Internet with respect to both censored and uncensored and resources. If a bookstore must self-censor certain books, it loses the profits from the sale of those particular books generated from the books' listing on the booksellers' Web sites. In addition, the bookstore will lose even more business because it will appear that the bookstore has an incomplete or inadequate listing of books in its inventory and Internet users will choose to buy their books elsewhere.

(Tricher Decl., pp. 4-5). Lawrence Kaufman, the Vice President of the Magazine Publishers of America, also testified to the interstate nature of the business conducted by MPA over the Internet and to the loss of sales and goodwill that MPA members will suffer if forced to self-censor in order to avoid criminal liability under the Act. In particular, Mr. Kaufman noted that Playboy magazine, an MPA member, occasionally posts electronic versions or excerpts from its magazines that might fall within the Act's prohibition, presumably in an effort to attract new readership and subscribers. (Kaufman Decl. pp. 2-3). Edgar teaches that for New York to attempt to strangle prospective interstate transactions between parties from states other than New York by this means offends the Commerce Clause.

The "extraterritorial" analysis of the Edgar opinion commanded only a plurality of the Court. Later majority holdings, however, expressly adopted the underlying principles on which Justice White relied in Edgar. See Healy v. The Beer Institute, 491 U.S. 324 (1989); Brown-Forman Distillers Corp. v New York State Liquor Authority, 476 U.S. 573 (1986). In Healy the Court assessed the constitutionality of a Connecticut statute that required that out-of-state beer shippers affirm that their prices were no higher than the prices being charged in the bordering states at the time of the affirmation. The Court derived three guiding principles from its prior cases. First, the Court emphasized that the ""Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside the State's borders, whether or not the commerce has effects within the state." (Healy, 491 U.S. at 336 totting Edgar, 457 U.S. at 642-43; Brown-Forman, 476 U.S. at 581-583). Second, the Court instructed that "a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State." (Id. citing Brown-Forman, 476 U.S. at 579). Finally, "the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted
similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." Id.; cf. CTS Corp. v. Dynamics Corp. of America, 481 U.S. 69, 88-89 (1987).

Applying these principles to the Connecticut price affirmation statute, the Court held that the statute had the undeniable and impermissible effect of controlling commercial activity occurring wholly outside Connecticut. In particular, the Court examined the practical impact of the statute, in light of the regulations prevailing in the neighboring states of Massachusetts and New York and determined that the affirmation law, when taken in conjunction with the laws that had been or might be enacted in neighboring states, created "just the kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude." Healy, 491 U.S. at 337.

The Edgar/Healy extraterritoriality analysis rests on the premise that the Commerce Clause has two aspects: it subordinates each state's authority over interstate commerce to the federal power of regulation (a vertical limitation), and it embodies a principle of comity that mandates that one state not expand its regulatory powers in a manner that encroaches upon the sovereignty of its fellow states (a horizontal limitation). The Court most recently recognized this duality in BMW of North America, Inc. v. Gore, 116 S. Ct. 1589 (1996). In a seminal case concerning an American's most precious possession (if not his most precious rights), a BMW purchaser in Alabama sued after discovering that his new BMW had been repainted prior to sale, alleging that the failure to disclose the repainting constituted fraud under Alabama law. Although the difference caused by the repainting was apparently imperceptible to the layperson, when the purchaser brought his car to "Slick Finish," an independent detailer, to make it look "snazzier than it normally would appear," 646 So.2d 619, 621 (Ala. 1994), Mr. Slick, the aptly yclept proprietor, detected evidence that the car had been repainted. The plaintiff alleged that he had suffered $4,000 in actual damages, relying on the testimony of a former BMW dealer who estimated that the value of a repainted BMW was approximately 10% less than one that was "showroom new." Plaintiff further argued that a punitive damage award of $4 million was an appropriate penalty in light of evidence he introduced that BMW had sold 983 refinished cars as new, including 14 in Alabama.

At trial, BMW acknowledged that it had adopted a nationwide policy of disclosing predelivery repairs only when the cost of the repairs exceeded 3% of the car's suggested retail price. The jury returned a verdict finding BMW liable for compensatory damages of $4,000 and punitive damages of $4 million, apparently calculated by multiplying the number of sales in all states of refinished cars by $4,000. BMW filed a post-trial motion to set aside the punitive damages award, contending that its nondisclosure policy was consistent with the laws of 25 states defining the disclosure obligations of automobile manufacturers; BMW asserted that the punitive damages were excessive because they were computed on the basis of sales that took place in jurisdictions where its conduct was perfectly legal.

The Supreme Court agreed. The Court indicated that while Congress could enact a law requiring full disclosure of every presale repair to an automobile, no single state could impose such a policy nationwide by imposing economic sanctions aimed at changing the conduct of a tortfeasor in other states. Id. at 1596. Speaking emphatically of the need to confine state legislation to its proper constitutional sphere, the Court stated:

[O]ne State's power to impose burdens on the interstate market for automobiles is not only subordinate to the federal power over interstate commerce, Gibbons v. Ogden, 9 Wheat. 1, 194-96, 6 L.Ed. 23 (1824), but is also constrained by the need to respect the interests of other States, see, e.g., Healy v. Beer Institute, 491 U.S. 324, 335-36, 109 S. Ct. 2491, 2498-99, 105 L.Ed. 275 (1989) (the Constitution has a "special concern both with the maintenance of a national
economic union unfettered by state-imposed limitations on interstate commerce and with the autonomy of the individual States within their respective spheres (footnote omitted); Edgar v. MITE Corp., 457 U.S. 624, 643, 102 S. Ct. 2629, 2641, 73 L.Ed.2d 269 (1982).

Id. The need to contain individual state overreaching thus arises not from any disrespect for the plenary authority of each state over its own internal affairs but out of a recognition that true protection of each state's respective authority is only possible when such limits are observed by all states. 7

The nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder. Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state's policy -- perhaps favoring freedom of expression over a more protective stance -- to New York's local concerns. See Bigelow v. Virginia, 421 U.S. 309, 824 (1975) ("A State does not acquire power or supervision over the internal affairs of another State merely because the welfare and health of its own citizens may be affected when they travel to that State."). New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net. See Southern Pacific Co. v. Arizona ex ref. Sullivan, 325 U.S. 761, 774 (1945) ("If one state may regulate train lengths, so may all others, and they need not prescribe the same maximum limitation. The practical effect of [a law limiting train lengths] is to control train operations beyond the boundaries of the state exacting it because of the necessity of breaking up and reassembling long trains at the nearest terminal points before entering and after leaving the regulating state."). This encroachment upon the authority which the Constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states is per se violative of the Commerce Clause.

C. The Burdens the Act Imposes on Interstate Commerce Exceed Any Local Benefit

Even if the Act were not a per se violation of the Commerce Clause by virtue of its extraterritorial effects, the Act would nonetheless be an invalid indirect regulation of interstate commerce, because the burdens it imposes on interstate commerce are excessive in relation to the local benefits it confers. The Supreme Court set forth the balancing test applicable to indirect regulations of interstate commerce in Pike v. Bruce Church, 397 U.S. 137, 142 (1970). 8 Pike requires a two fold inquiry. The first level of examination is directed at the legitimacy of the state's interest. The next, and more difficult, determination weighs the burden on interstate commerce in light of the local benefit derived from the statute.

In the present case, I accept that the protection of children against pedophilia is a quintessentially legitimate state objective -- a proposition with which I believe even the plaintiffs have expressed no quarrel. See New York v. Ferber, 458 U.S. 747, 756-57 (1982) ("It is evident beyond the need for elaboration that a State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'") (quoting Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)); see also Sable v. Federal Communications Commission, 492 U.S. 115, 126 (1989) ("[T]here is a compelling interest in protecting the physical and psychological well-being of minors. This interest extends to shielding minors from the influence of literature that is not obscene by adult standards."). The defendants spent considerable time in their Memorandum and at argument asserting the legitimacy of the state's interest. Even with the fullest recognition that the protection of children from sexual exploitation is an indisputably valid state goal, however, the present statute cannot survive even the lesser scrutiny to which indirect regulations of interstate commerce are subject under the Constitution. The State cannot avoid the second stage of the inquiry simply by invoking the legitimate state interest underlying the Act. See Hunt v.
Washington State Apple Advertising Comm'n, 432 U.S. 333, 350 (1977) ("[A] finding that state legislation furthers matters of legitimate local concern, even in the health and consumer protection areas, does not end the inquiry."); Bibb v. Navajo Freight Lines, 359 U.S. 520, 528 (1959) (holding that "local safety measures that are nondiscriminatory [can] place an unconstitutional burden on interstate commerce"); see also Dean Milk Co. v. Madison, 340 U.S. 349, 354 (1951) (holding that permitting a state to discriminate against interstate commerce to promote the health and safety of its citizens "would mean that the Commerce Clause of itself imposes no limitations on state action . . . save for the rare instances where a state artlessly discloses an avowed purpose to discriminate against interstate goods."); Southern Pac. Co. v. Arizona, ex rel. Sullivan, 325 U.S. 761, 779 (1945) ("The principle that, without controlling Congressional action, a state may not regulate interstate commerce so as substantially to affect its flow or deprive it of needed uniformity in its regulation is not to be avoided by 'simply invoking the convenient apologetics of the police power.'") (quoting Kansas City Southern Ry. v. Kaw Valley Drainage Dist., 233 U.S. 76, 79 (1914)).

The local benefits likely to result from the New York Act are not overwhelming. The Act can have no effect on communications originating outside the United States. As the three-judge panel that struck the federal analog of the New York Act, the Communications Decency Act, on First Amendment grounds concluded:

[The Act] will almost certainly fail to accomplish the Government's interest in shielding children from pornography on the Internet. Nearly half of Internet communications originate outside the United States, and some percentage of that figure represents pornography. Pornography from, say, Amsterdam, will be no less appealing to a child on the Internet than pornography from New York City, and residents of Amsterdam have little incentive to comply with the [Act].

American Civil Liberties Union v. Reno, 929 F. Supp. 824, 882 (E.D. Pa. 1996). Further, in the present case, New York's prosecution of parties from out of state who have allegedly violated the Act, but whose only contact with New York occurs via the Internet, is beset with practical difficulties, even if New York is able to exercise criminal jurisdiction over such parties. The prospect of New York bounty hunters dragging pedophiles from the other 49 states into New York is not consistent with traditional concepts of comity.

Moreover, the State has espoused an interpretation of the Act that, if accepted, would further undermine its effectiveness. According to defendant, the Act reaches only pictorial messages that are harmful to minors and has no impact on purely textual communications. Were this interpretation adopted, Mr. Barlow, whose conduct supposedly motivated the supporters of the Act, would escape prosecution because his messages were verbal. See The Crusader, supra, at 122 (reporting Barlow's message to New York girl as "I'm feeling really horny--I think Oscar is making a 'statement.' We both want you very much. I'm thinking about you, & he's thinking about Love Bunny & tingling like mad.")

The Act is, of course, not the only law in New York's statute books designed to protect children against sexual exploitation. The State is able to protect children through vigorous enforcement of the existing laws criminalizing obscenity and child pornography. See United States v. Thomas, 74 F.3d 701, 704-05 (6th Cir. 1995), cert. denied, 117 S. Ct. 74 (1996). Moreover, plaintiffs do not challenge the sections of the statute that criminalize the sale of obscene materials to children, over the Internet or otherwise, and prohibit adults from luring children into sexual contact by communicating with them via the Internet. See N.Y. Penal Law § 235.21(1); N.Y. Penal Law § 235.22(2). The local benefit to be derived from the challenged section of the statute is therefore confined to that narrow class of cases that does not fit within the parameters of any other law. The efficacy of the statute is further limited, as discussed above, to those cases which New York is realistically able to prosecute.

The conclusion that the New York Act has a very limited effect was bolstered by the
testimony of Michael McCartney, an investigator with the New York State Attorney General's office. Mr. McCartney testified that he personally had logged over 600 hours investigating on-line criminal activity. (4/3/97 Tr., p. 12). Despite this extensive investment of time, Mr. McCartney admitted that he had investigated only two cases involving the dissemination of indecent materials to minors over the Internet that did not fall into the category of child pornography (which is, of course, subject to prosecution under other laws). (Id., p. 36). In one case, further investigation disclosed that the e-mail conversation actually took place between two adults and thus was outside the terms of the Act. (Id.). In the second case, Mr. McCartney was never able to determine which of the people in the household that held the Internet access account was responsible for sending the messages and pictures in question; he therefore never determined whether the sender was an adult. (Id., p. 37). In neither case did the Attorney General's office institute a prosecution. In fact, the Attorney General to date has not brought any prosecutions under the Act at all. (Id., p. 15). By contrast, Mr. McCartney described with justifiable pride his participation in the sting operation that resulted in the arrest of a student at SUNY who was using the Internet to contact a child; the defendant in that case, however, was charged under N.Y. Penal Law § 263, which prohibits an adult from promoting the sexual performance of a child. (Id., p. 12).

Balanced against the limited local benefits resulting from the Act is an extreme burden on interstate commerce. The New York Act casts its net worldwide; moreover, the chilling effect that it produces is bound to exceed the actual cases that are likely to be prosecuted, as Internet users will steer clear of the Act by significant margin. See ACLU, 929 F. Supp. at 863 (holding that individuals, uncertain of the reach of the CDA, will undoubtedly "steer far wider of the unlawful zone") (citing Bassett v. Bullitt, 377 U.S. 360, 372 (1964)); see also testimony of Maurice J. Freedman, Director of Westchester Library System, 4/7/97 Tr., at p. 209 ("My concern about prosecution in the context of this court proceeding is in relation to this Act. When I became aware of this Act and its implications for public libraries, as I perceived those implications, I at that point became quite concerned -- and scared might be another word -- for being arrested or being in violation."). At oral argument, the State asserted that only a small percentage of Internet communications are "harmful to minors" and would fall within the proscriptions of the statute; therefore, the State argued, the burden on interstate commerce is small. On the record before me, I conclude that the range of Internet communications potentially affected by the Act is far broader than the State suggests. I note that in the past, various communities within the United States have found works including I Know Why the Caged Bird Sings by Maya Angelou, Funhouse by Dean Koontz, The Adventures of Huckleberry Finn by Mark Twain, and The Color Purple by Alice Walker to be indecent. (Teicher Decl., p. 3). Even assuming, arguendo, that the Act applies only to pictures, a number of Internet users take advantage of the medium's capabilities to communicate images to one another and, again, I find that the range of images that might subject the communicator to prosecution (or reasonably cause a communicator to fear prosecution) is far broader than defendants assert. For example, many libraries, museums and academic institutions post art on the Internet that some might conclude was "harmful to minors." Famous nude works by Botticelli, Manet, Matisse, Cezanne and others can be found on the Internet. In this regard, I point out that a famous painting by Manet which shows a nude woman having lunch with two fully clothed men was the subject of considerable protest when it first was unveiled in Paris, as many observers believed that it was "scandalous." (Declaration of Judith F. Krug, sworn to in March, 1997, at p. 5). Lesser known artists who post work over the Internet may face an even greater risk of prosecution, because the mantle of respectability that has descended on Manet is not associated with their as yet obscure names. Lile Elam, the founder of Art on the Net, submitted a Declaration that included samples of the types of work found on Art on the Net's site; certain of the images might be considered harmful to minors in some communities, including several nudes and a very dark, disturbing short story entitled "Two Running Rails of Mercury," accompanied by a picture of a woman's nude body dissolving into railroad tracks. (Declaration of Lile Elam, sworn to on March 13, 1997, Exh. 6). Rudolf Kinsky testified to his perception of the greater risk run by an unrenowned artist who posts controversial images on the Internet; when he was asked by defendants if a work by Corbet
could subject the artist to prosecution, he answered, "His works are established; they are
known. This is a different situation. Could be or could not, but my situation, when I am at
the beginning of my career, and someone can, because I am not known, I have no
established name and everything, I can still be prosecuted." (4/7/97 Tr., at 250). Individuals
who wish to communicate images that might fall within the Act's proscriptions must thus
self-censor or risk prosecution, a Hobson's choice that imposes an unreasonable restriction
on interstate commerce. See Allen B. Dumont Labs., Inc. v. Carroll, 86 F. Supp. 813, 816
(1949) (holding that Pennsylvania state law requiring that motion pictures be submitted for
review by a censorship board prior to being exhibited in the state imposed an undue and
unreasonable burden on interstate commerce), aff'd, 184 F.2d 153 (3d Cir. 1950), cert.

Moreover, as both three-judge panels that struck the federal statute have found, the costs
associated with Internet users' attempts to comply with the terms of the defenses that the Act
provides are excessive. Both courts that addressed the Communications Decency Act found
that these costs of compliance, coupled with the threat of serious criminal sanctions for
failure to comply, could drive some Internet users off the Internet altogether. See ACLU,
929 F. Supp. at 855-56 ("Many speakers who display arguably indecent content on the
Internet must choose between silence and the risk of prosecution ... [the] defenses are not
technologically or economically feasible for most providers"); Shea, 930 F. Supp. at 942-48
(finding that the defenses provided by the CDA do not offer a safe harbor to Internet users,
who are then faced with the choice between complying, despite economic and technological
barriers, or refraining from the Internet posting that potentially subjects them to
prosecution). While the defenses in the Act are not identical to those present in the CDA,
the cost analysis undertaken by the ACLU and Shea courts is equally applicable to both
statutes.

The severe burden on interstate commerce resulting from the New York statute is not
justifiable in light of the attenuated local benefits arising from it. The alternative analysis of
the Act as an indirect regulation on interstate commerce therefore also mandates the
issuance of the preliminary injunction sought by plaintiffs.

D. The Act Unconstitutionally Subjects Interstate Use of the Internet to Inconsistent
Regulations

Finally, a third mode of Commerce Clause analysis further confirms that the plaintiffs are
likely to succeed on the merits of their claim that the New York Act is unconstitutional. The
courts have long recognized that certain types of commerce demand consistent treatment
and are therefore susceptible to regulation only on a national level. The Internet represents
one of those areas; effective regulation will require national, and more likely global,
cooperation. Regulation by any single state can only result in chaos, because at least some
states will likely enact laws subjecting Internet users to conflicting obligations. Without the
limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could
paralyze the development of the Internet altogether.

In numerous cases, the Supreme Court has acknowledged the need for coordination in the
regulation of certain areas of commerce. As long ago as 1886, the Supreme Court stated:

Commerce with foreign countries and among the states, strictly considered,
consists in intercourse and traffic, including in these terms navigation, and the
transportation and transit of persons and property, as well as the purchase, sale,
and exchange of commodities. For the regulation of commerce, as thus defined,
there can be only one system of rules, applicable alike to the whole country;
and the authority which can act for the whole country can alone adopt such a
system. Action upon it by separate states is not, therefore, permissible.

struck the Illinois statute at issue, which purported to establish interstate railway rates, stating "[t]hat this species of regulation is one which must be, if established at all, of a general and national character, and cannot be safely and wisely remitted to local rules and regulations, we think is clear from what has already been said." Id. at 577.

Similarly, in Southern Pac. Co. v. Arizona ex rel. Sullivan, 325 U.S. 761 (1945), the Court addressed the constitutionality of an Arizona statute that limited the length of trains within the state to fourteen passenger and seventy freight cars. The lower court’s findings demonstrated that 93% of the freight traffic and 95% of the passenger traffic in Arizona was interstate; moreover, the Court endorsed the findings that travel by trains of more than fourteen passenger cars and more than seventy freight cars over the main lines of the United States was standard practice, and that the Arizona law had the effect of forcing railroads to decouple their trains in Texas or New Mexico and reform the train at full length in California. Id. at 774. Thus, the practical impact of the Arizona law was to control the length of trains, as the Court put it, "all the way from Los Angeles to El Paso." Id. The Court concluded that the Arizona train limit law imposed a serious burden on interstate commerce, noting that various states had imposed varying limits. The Court stated:

With such laws in force in states which are interspersed with those having no limit on train lengths, the confusion and difficulty with which interstate operations would be burdened under the varied system of state regulation and the unsatisfied need for uniformity in such regulation, if any, are evident.

Id. at 773-74. In striking the Arizona law as an unconstitutional intrusion on interstate commerce, the Court relied on a long-established rule barring the states from regulating "those phases of the national commerce which, because of the need of national uniformity, demand that their regulation, if any, be prescribed by a single authority." Id. at 766 (citing Gibbons v. Ogden, 9 Wheat. 1 (1824); Cooley v. Board of Wardens, 12 How. 299, 319 (1851); Leisy v. Hardin, 135 U.S. 100, 108-09 (1890); Minnesota Rate Cases, 230 U.S. 399, 400 (1913); Edwards v. People of State of California, 314 U.S. 160, 176 (1941)).

In Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959), the Court examined an Illinois statute that required the use of contour mudguards on trucks in Illinois. The Court took note of the fact that straight or conventional mudguards were permissible in most other states and actually required in Arkansas. Id. at 526. Recognizing the need for coordinated legislation, the Court stated that "[t]he conflict between the Arkansas regulation and the Illinois regulation . . . suggests that this regulation of mudguards is not one of those matters admitting of diversity of treatment, according to the special requirements of local conditions." Id. at 528 (quoting Sproles v. Binford, 286 U.S. 374, 390 (1932)). The Court struck the Illinois law as imposing an undue burden on interstate commerce, in part because Illinois was insisting upon "a design out of line with the requirements of almost all the other states." Id.

The Internet, like the rail and highway traffic at issue in the cited cases, requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities. New York is not the only state to enact a law purporting to regulate the content of communications on the Internet. Already Oklahoma and Georgia have enacted laws designed to protect minors from indecent communications over the Internet; as might be expected, the states have selected different methods to accomplish their aims. Georgia has made it a crime to communicate anonymously over the Internet, while Oklahoma, like New York, has prohibited the online transmittaion of material deemed harmful to minors. See Ga. Code Ann. § 16-19-93.1 (1996); Okla. Stat. tit. 21, § 1040.76 (1996).

Moreover, the regulation of communications that may be "harmful to minors" taking place over the Internet poses particular difficulties. New York has defined "harmful to minors" as
including:

that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
(a) Considered as a whole, appeals to the prurient interest in sex of minors; and
(b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
(c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20(6). Courts have long recognized, however, that there is no single "prevailing community standard" in the United States. Thus, even were all 50 states to enact laws that were verbatim copies of the New York Act, Internet users would still be subject to discordant responsibilities. To use an example cited by the court in ACLU v. Reno, the Broadway play Angels in America, which concerns homosexuality and AIDS and features graphic language, was immensely popular in New York and in fact earned two Tony awards and a Pulitzer prize. ACLU, 929 F. Supp. at 852-53. In Charlotte, North Carolina, however, a production of the drama caused such a public outcry that the Mecklenberg County Commission voted to withhold all public funding from arts organizations whose works "expose the public to perverted forms of sexuality," Eric Harrison, Charlotte Ban on Funding Questions Community Culture Commission -- Boycotts "Perverted Sexuality", Milwaukee J. & Sentinel, April 21, 1997, at 3. The Supreme Court has always recognized that "our nation is simply too big and too diverse for this Court to reasonably expect that such standards [of what is patently offensive] could be articulated for all 50 states in a single formulation." Miller, 413 U.S. at 30.

As discussed at length above, an Internet user cannot foreclose access to her work from certain states or send differing versions of her communication to different jurisdictions. In this sense, the Internet user is in a worse position than the truck driver or train engineer who can steer around Illinois or Arizona, or change the mudguard or train configuration at the state line; the Internet user has no ability to bypass any particular state. The user must thus comply with the regulation imposed by the state with the most stringent standard or forego Internet communication of the message that might or might not subject her to prosecution. For example, a teacher might invite discussion of Angels In America from a Usenet newsgroup dedicated to the literary interests of high school students. Quotations from the play might not subject her to prosecution in New York but could qualify as "harmful to minors." according to the community standards prevailing in Oklahoma. The teacher cannot tailor her message on a community specific basis and thus must take her chances or avoid the discussion altogether.

Further development of the Internet requires that users be able to predict the results of their Internet use with some degree of assurance. Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace. The need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the Commerce Clause.

III. The First Amendment and the Internet

Plaintiffs have also asserted their entitlement to a preliminary injunction on the grounds that the Act unconstitutionally burdens free speech. Plaintiffs' ready ability to demonstrate the Act's unconstitutionality under the Commerce Clause, however, provides fully adequate support for the issuance of a preliminary injunction at this time. Moreover, the Supreme Court heard argument on a First Amendment challenge to the federal statute, the CDA, on March 19, 1997. The State vigorously argues that its law was designed to avoid the constitutional pitfalls presented by the CDA; however, the New York Act was clearly modelled on the CDA, and numerous provisions of the New York Act mirror their federal counterparts. See New York State Executive Charter Memorandum, annexed as Exhibit A
to Declaration of Anat Hakim, sworn to on March 21, 1997 ("This bill . . . is consistent with the federal statute"); Letter from William Sears to Governor Pataki, dated July 11, 1996, annexed as Exhibit A to Hersher Affidavit ("This bill is consistent with the Federal Communications Decency Act"); Introducer's Memorandum in Support of Amended Senate Bill S. 210-E and Assembly Bill A. 3967-C, annexed as Exhibit G to Hersher Affidavit ("Amendments were necessary for the bill to be consistent with the recently passed Federal Communications Decency Act . . ."). Furthermore, it should be noted that the 'harmful to minors' standard contained in the charging language of the offense is consistent with the Federal law . . ."). I believe any determination of plaintiffs' First Amendment challenge should therefore await the guidance to be provided by the Supreme Court's forthcoming opinion.

CONCLUSION

The protection of children from pedophilia is an entirely valid and laudable goal of state legislation. The New York Act's attempts to effectuate that goal, however, fall afoul of the Commerce Clause for three reasons. First, the practical impact of the New York Act results in the extraterritorial application of New York law to transactions involving citizens of other states and is therefore per se violative of the Commerce Clause. Second, the benefits derived from the Act are inconsequential in relation to the severe burdens it imposes on interstate commerce. Finally, the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes. Because plaintiffs have demonstrated that they are likely to succeed on the merits of their claim under the Commerce Clause and that they face irreparable injury in the absence of an injunction, the motion for a preliminary injunction is granted.

Defendants are enjoined from instituting any prosecutions under the Act, until further Order of this Court. Plaintiffs shall submit a proposed form of injunction on two days' notice.

SO ORDERED:

Dated: New York, New York, June 20, 1997

LORETTA A. PRESKA, U.S.D.J.

NOTES

1. I recall in this respect a particularly confusing item of testimony elicited at the evidentiary hearing. Ms. Kovacs, plaintiffs' expert witness with respect to the Internet, testified that on one occasion while she was in a MUD (a Multi User Dungeon), a malefactor sicc'd his "virtual dog" on her because she had trespassed on his domain. Fortunately, the other inhabitants of the MUD came to her rescue, vehemently protesting the unfriendliness of the virtual canine attack. Relieved as I was that the story had a happy ending, I must admit that it afforded me a window into an entirely unknown world. (4/4/97 Tr., p. 95).

2. Where information in this subsection is not cited to ACLU or Shea, it was derived from the parties' Joint Stipulation of Facts.

3. Because I find, as discussed below, that plaintiffs have demonstrated a likelihood of success on the merits of their claim that the New York Act violates the Commerce Clause, I do not rely on the "fair ground for litigation" standard. I note, however, that the standard would be applicable to this case because; (1) the action alleges constitutional violations, Almonte v. Pierce, 666 F. Supp. 517, 526 (S.D.N.Y. 1987); (2) the public interest in a free flow of interstate commerce served by an injunction against enforcement of the Act counterbalances the public interest in protecting children served by the Act, see Carey v.
Klutznick, 637 F.2d 834, 839 (2d Cir. 1980); and (3) the New York Legislature did not engage in any fact-finding regarding the public interest served by the Act before promulgating it. Able v. United States, 44 F.3d 128, 131 (2d Cir. 1995).

4. Other jurisdictions internationally have also gotten into the act. In January, 1997, two associations dedicated to the preservation of France's linguistic purity filed suit against two private corporations and Georgia Tech Lorraine, a French university affiliated with the Georgia Institute of Technology, claiming that the defendants violated a French law that prohibits advertising in any language other than French by operating English-language sites on the World Wide Web. See Complaint filed by L' Association "Avenir de la Langue Francaise" and L'Association "Defense de La Langue Francaise," Jan. 6, 1996; see also E. Schneiderman & R. Kornreich, Personal Jurisdiction and Internet Commerce, N.Y.L.J., June 4, 1997, at 1. The French court dismissed the action as to Georgia Tech, but other efforts by foreign jurisdictions to regulate the Internet are likely to follow. In addition, Germany made headlines recently when its anti-pornography laws forced Compuserve to close access to over 200 Internet sites from anywhere in the world. See John Markoff, Compuserve Bars Access to Internet Sex: German Laws Prompt the Provider to Block Pictures and Chat Groups, Orange County Register, December 29, 1995.

5. The defendants proposed Ms. Pirro as a witness for the evidentiary hearing, but then withdrew the proposal. Ms. Pirro's letter, which preceded the bill's signature into law by the Governor, is properly considered as part of the legislative history. See Civil Service Employees Association, Inc. v. Oneida, 78 A.D.2d 1004, 1005 (4th Dep't 1980), appeal denied, 53 N.Y.2d 603 (1981). Ms. Pirro's testimony, on the other hand, would be a hindsight, post-enactment review of legislative intent by a non-legislator and would carry no probative weight. See Bread Political Action Committee v. Federal Election Committee, 455 U.S. 577, 580 n.3 (1982); Frontier Ins. Co. v. New York, 609 N.Y.S.2d 748, 752 (N.Y. Ct. C1. 1993), aff'd, 197 A.D.2d 177 (3d Dep't 1994).

6. Judge Stein recently concluded that these realities meant that one whose only contact with the forum occurs via the Internet is not susceptible to suit there. Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996).

7. The Court's injunction against extraterritorial regulation is long-established. See Huntington v. Attrill, 146 U.S. 657, 669 (1892) ("Laws have no force of themselves beyond the jurisdiction of the State which enacts them, and can have extraterritorial effect only by the comity of other States); New York Life Ins. Co. v. Head, 234 U.S. 149, 161 (1914) ("[I]t would be impossible to permit the statutes of Missouri to operate beyond the jurisdiction of that State . . . without throwing down the constitutional barriers by which all the States are restricted within the orbits of their lawful authority and upon the preservation of which the Government under the Constitution depends. This is so obviously the necessary result of the Constitution that it has rarely been called in question and hence authorities dealing directly with it do not abound.").

8. The distinction between direct regulations of interstate commerce, which are subject to a per se rule of invalidation, and indirect regulations subject to the less stringent balancing test has never been sharply defined. In either situation, however, the "critical consideration is the overall effect of the statute on both local and interstate activity." See Brown-Forman, 476 U.S. at 579; Raymond Motor Transportation Inc. v. Rice, 434 U.S. 429, 440-41 (1978).

9. The state's construction of the Act is unsupported in light of the plain language of the statute and the interpretation that has been applied to closely related statutes. The Act applies to "communication[s] which, in whole or in part, depict[] actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which [are] harmful to minors." The defendants contend that "depict" embraces only pictorial images. The dictionary definition of "depict," however, includes both visual representations and "description." Webster's Third New International Dictionary 605 (1981). The Act itself defines material that is
harmful to minors as including any "description or representation," supporting an interpretation of the word "depict" that includes both text and pictures. Further, the Act is intended to extend liability under the statute as it existed prior to amendment. Cases brought under the prior law confirmed its applicability to sexually frank text, as well as pictures. See People v. Lida, 247 N.Y.S.2d 421 (N.Y. City Crim. Ct.) (finding that magazine containing short stories dealing with sex as well as photographs showing nude and partially nude women fell within the prohibition of Penal Law 1909 § 484-h [now Penal Law § 235.21], proscribing sale of magazines to minors), aff'd, 252 N.Y.S.2d 142 (N.Y. Sup. 1964); see also People v. Ginsberg, 290 N.Y.S.2d 239 (N.Y. Dist. 1966) (holding that evidence demonstrating that defendant, knowing buyer to be under 17, sold material containing pictures and photographs depicting female nudity and verbal descriptions and narrative accounts of sexual conduct and excitement was sufficient to sustain conviction for selling material harmful to minors), aff'd, 390 U.S. 619 (1968).

10. Further distinctions may exist within the state of New York. The community standards prevailing in New York City may well be different than the community standards prevailing in, for example, Rensselaer County. See, e.g., United States v. Various Articles of Obscene Merchandise Schedule No. 2102, 709 F.2d 132, 134, 137 (2d Cir. 1983) (upholding the district court's conclusion that "detailed portrayals of genitalia, sexual intercourse, fellatio, and masturbation" including the film "Deep Throat" and other pornographic films and magazines, are not obscene, "in light of the community standards prevailing in New York City.")
IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ZIPPO MANUFACTURING COMPANY Plaintiff

v.

ZIPPO DOT COM, INC. Defendant.

Civil Action No. 96-397 Erie

January 16, 1997

MEMORANDUM OPINION

McLAUGHLIN, J.

This is an Internet domain name [1] dispute. At this stage of the controversy, we must decide the Constitutionally permissible reach of Pennsylvania's Long Arm Statute, 42 Pa.C.S.A. §5322, through cyberspace. Plaintiff Zippo Manufacturing Corporation ("Manufacturing") has filed a five count complaint against Zippo Dot Com, Inc. ("Dot Com") alleging trademark dilution, infringement, and false designation under the Federal Trademark Act, 15 U.S.C. §§1051-1127. In addition, the Complaint alleges causes of action based on state law trademark dilution under 54 Pa.C.S.A. §1124, and seeks equitable accounting and imposition of a constructive trust. Dot Com has moved to dismiss for lack of personal jurisdiction and improper venue pursuant to Fed.R.Civ.P. 12(b)(2) and (3) or, in the alternative, to transfer the case pursuant to 28 U.S.C. §1406(a). For the reasons set forth below, Defendant's motion is denied.

I. BACKGROUND

The facts relevant to this motion are as follows. Manufacturing is a Pennsylvania corporation with its principal place of business in Bradford, Pennsylvania. Manufacturing makes, among other things, well known "Zippo" tobacco lighters. Dot Com is a California corporation with its principal place of business in Sunnyvale, California. Dot Com operates an Internet Web Site [2] and an Internet news service and has obtained the exclusive right to use the domain names "zippo.com", "zippo.net" and "zipponews.com" on the Internet. [3]

Dot Com's Web site contains information about the company, advertisements and an application for its Internet news service. The news service itself consists of three levels of membership -- public/free, "Original" and "Super." Each successive level offers access to a greater number of Internet newsgroups. A customer who wants to subscribe to either the "Original" or "Super" level of service fills out an on-line application that asks for a variety of information including the person's name and address. Payment is made by credit card over the Internet or the telephone. The application is then processed and the subscriber is assigned a password which permits the subscriber to view and/or download Internet newsgroup messages that are stored on the Defendant's server in California.
Dot Com's contacts with Pennsylvania have occurred almost exclusively over the Internet. Dot Com's offices, employees and Internet servers are located in California. Dot Com maintains no offices, employees or agents in Pennsylvania. Dot Com's advertising for its service to Pennsylvania residents involves posting information about its service on its Web page, which is accessible to Pennsylvania residents via the Internet. Defendant has approximately 140,000 paying subscribers worldwide. Approximately two percent (3,000) of those subscribers are Pennsylvania residents. These subscribers have contracted to receive Dot Com's service by visiting its Web site and filling out the application. Additionally, Dot Com has entered into agreements with seven Internet access providers in Pennsylvania to permit their subscribers to access Dot Com's news service. Two of these providers are located in the Western District of Pennsylvania.

The basis of the trademark claims is Dot Com's use of the word "Zippo" in the domain names it holds, in numerous locations in its Web site and in the heading of Internet newsgroup messages that have been posted by Dot Com subscribers. When an Internet user views or downloads a newsgroup message posted by a Dot Com subscriber, the word "Zippo" appears in the "Message-Id" and "Organization" sections of the heading. The news message itself, containing text and/or pictures, follows. Manufacturing points out that some of the messages contain adult oriented, sexually explicit subject matter.

II. STANDARD OF REVIEW

When a defendant raises the defense of the court's lack of personal jurisdiction, the burden falls upon the plaintiff to come forward with sufficient facts to establish that jurisdiction is proper. Mellon Bank (East) PSFS, N.A. v. Farino, 960 F.2d 1217, 1223 (3d Cir. 1992) (citing Carteret Savings Bank v. Shusan, 954 F.2d 141 (3d Cir. 1992), cert. denied 506 U.S. 817 (1992)). The plaintiff meets this burden by making a prima facie showing of "sufficient contacts between the defendant and the forum state." Mellon East, 960 F.2d at 1223 (citing Provident Nat. Bank v. California Fed. Sav. & Loan Assoc., 819 F.2d 434 (3d Cir. 1987)).

III. DISCUSSION

A. Personal Jurisdiction

1. The Traditional Framework

Our authority to exercise personal jurisdiction in this case is conferred by state law. Fed.R.Civ.P. 4(e); *Mellon*, 960 F.2d at 1221. The extent to which we may exercise that authority is governed by the Due Process Clause of the Fourteenth Amendment to the Federal Constitution. *Kulko v. California Supreme Court*, 436 U.S. 84, 91 (1978).

Pennsylvania's long arm jurisdiction statute is codified at 42 Pa.C.S.A. §5322(a). The portion of the statute authorizing us to exercise jurisdiction here permits the exercise of jurisdiction over non-resident defendants upon:

(2) Contracting to supply services or things in this Commonwealth.

42 Pa.C.S.A. §5322(a). It is undisputed that Dot Com contracted to supply Internet news services to approximately 3,000 Pennsylvania residents and also entered into agreements with seven Internet access providers in Pennsylvania. Moreover, even if Dot Com's conduct did not satisfy a specific provision of the statute, we would nevertheless be authorized to exercise jurisdiction to the "fullest extent allowed under the Constitution of the United States." 42 Pa.C.S.A. §5322(b).

The Constitutional limitations on the exercise of personal jurisdiction differ depending upon whether a court seeks to exercise general or specific jurisdiction over a non-resident defendant. *Mellon*, 960 F.2d at 1221. General jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for non-forum related activities when the defendant has engaged in "systematic and
continuous" activities in the forum state. Helicopteros Nacionales de Columbia, S.A. v. Hall, 466 U.S. 408, 414-16 (1984). In the absence of general jurisdiction, specific jurisdiction permits a court to exercise personal jurisdiction over a non-resident defendant for forum-related activities where the "relationship between the defendant and the forum falls within the 'minimum contacts' framework" of International Shoe Co. v. Washington, 326 U.S. 310 (1945) and its progeny. Mellon, 960 F.2d at 1221. Manufacturing does not contend that we should exercise general personal jurisdiction over Dot Com. Manufacturing concedes that if personal jurisdiction exists in this case, it must be specific.

A three-pronged test has emerged for determining whether the exercise of specific personal jurisdiction over a non-resident defendant is appropriate: (1) the defendant must have sufficient "minimum contacts" with the forum state, (2) the claim asserted against the defendant must arise out of those contacts, and (3) the exercise of jurisdiction must be reasonable. Id. The "Constitutional touchstone" of the minimum contacts analysis is embodied in the first prong, "whether the defendant purposefully established" contacts with the forum state. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985) (citing International Shoe Co. v. Washington, 326 U.S. 310, 319 (1945)). Defendants who "reach out beyond one state' and create continuing relationships and obligations with the citizens of another state are subject to regulation and sanctions in the other State for consequences of their actions." Id. (citing Travelers Health Assn. v. Virginia, 339 U.S. 643, 647 (1950)). "]The foreseeability that is critical to the due process analysis is ... that the defendant's conduct and connection with the forum State are such that he should reasonably expect to be haled into court there." World Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 295 (1980). This protects defendants from being forced to answer for their actions in a foreign jurisdiction based on "random, fortuitous or attenuated" contacts. Keeton v. Hustler Magazine, Inc., 465 U.S. 770, 774 (1984). "Jurisdiction is proper, however, where contacts proximately result from actions by the defendant himself that create a 'substantial connection' with the forum State." Burger King, 471 U.S. at 475 (citing McGee v. International Life Insurance Co., 355 U.S. 220, 223 (1957)).

The "reasonableness" prong exists to protect defendants against unfairly inconvenient litigation. World Wide Volkswagen, 444 U.S. at 292. Under this prong, the exercise of jurisdiction will be reasonable if it does not offend "traditional notions of fair play and substantial justice." International Shoe, 326 U.S. at 316. When determining the reasonableness of a particular forum, the court must consider the burden on the defendant in light of other factors including: "the forum state's interest in adjudicating the dispute; the plaintiff's interest in obtaining convenient and effective relief, at least when that interest is not adequately protected by the plaintiff's right to choose the forum; the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and the shared interest of the several states in furthering fundamental substantive social policies." World Wide Volkswagen, 444 U.S. at 292 (internal citations omitted).

2. The Internet and Jurisdiction

In Hanson v. Denckla, the Supreme Court noted that "[a]s technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase." Hanson v. Denckla, 357 U.S. 235, 250-51 (1958). Twenty seven years later, the Court observed that jurisdiction could not be avoided "merely because the defendant did not physically enter the forum state. Burger King, 471 U.S. at 476.

The Court observed that:

[I]t is an inescapable fact of modern commercial life that a substantial amount of commercial business is transacted solely by mail and wire communications across state lines, thus obviating the need for physical presence within a State in which business is conducted.

Id.

Enter the Internet, a global "super-network' of over 15,000 computer networks used by over 30 million individuals, corporations, organizations, and educational institutions worldwide." Panavision Intern., L.P. v. Toeppen, 938 F.Supp. 616 (S.D.Cal. 1996) (citing American Civil Liberties Union v. Reno,
929 F.Supp. 824, 830-48 (E.D.Pa. 1996). "In recent years, businesses have begun to use the Internet to provide information and products to consumers and other businesses." Id. The Internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials [5] reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction if proper. E.g. Compuserve, Inc. v. Patterson, 89 F.2d 1257 (6th Cir. 1996). At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. E.g. Bensusan Restaurant Corp., v. King, 937 F.Supp. 296 (S.N.D.Y. 1996). The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. E.g. Maritz, Inc. v. Cybergold, Inc., 1996 U.S. Dist. Lexis 14976 (E.D.Mo. Aug. 19, 1996).

Traditionally, when an entity intentionally reaches beyond its boundaries to conduct business with foreign residents, the exercise of specific jurisdiction is proper. Burger King, 471 U.S. at 475. Different results should not be reached simply because business is conducted over the Internet. In Compuserve, Inc. v. Patterson, 89 F.2d 1257 (6th Cir. 1996), the Sixth Circuit addressed the significance of doing business over the Internet. In that case, Patterson, a Texas resident, entered into a contract to distribute shareware [6] through Compuserve's Internet server located in Ohio. Compuserve, 89 F.2d at 1260. From Texas, Patterson electronically uploaded thirty-two master software files to Compuserve's server in Ohio via the Internet. Id. at 1261. One of Patterson's software products was designed to help people navigate the Internet. Id. When Compuserve later began to market a product that Patterson believed to be similar to his own, he threatened to sue. Id. Compuserve brought an action in the Southern District of Ohio, seeking a declaratory judgment. Id. The District Court granted Patterson's motion to dismiss for lack of personal jurisdiction and Compuserve appealed. Id. The Sixth Circuit reversed, reasoning that Patterson had purposefully directed his business activities toward Ohio by knowingly entering into a contract with an Ohio resident and then "deliberately and repeatedly" transmitted files to Ohio. Id. at 1264-66.

In Maritz, Inc. v. Cybergold, Inc., 1996 U.S. Dist. Lexis 14976 (E.D.Mo. Aug. 19, 1996), the defendant had put up a Web site as a promotion for its upcoming Internet service. The service consisted of assigning users an electronic mailbox and then forwarding advertisements for products and services that matched the users' interests to those electronic mailboxes. Maritz, 1996 U.S. Dist. Lexis 14976 at *7. The defendant planned to charge advertisers and provide users with incentives to view the advertisements. Id. Although the service was not yet operational, users were encouraged to add their address to a mailing list to receive updates about the service. Id. The court rejected the defendant's contention that it operated a "passive Web site." Id. at * 16. The court reasoned that the defendant's conduct amounted to "active solicitations" and "promotional activities" designed to "develop a mailing list of Internet users" and that the defendant "indiscriminately responded to every user" who accessed the site. Id. at *14-17.

Inset Systems, Inc. v. Instruction Set, 937 F.Supp. 161 (D. Conn. 1996) represents the outer limits of the exercise of personal jurisdiction based on the Internet. In Inset Systems, a Connecticut corporation sued a Massachusetts corporation in the District of Connecticut for trademark infringement based on the use of an Internet domain name. Inset Systems, 937 F.Supp. at 162. The defendant's contacts with Connecticut consisted of posting a Web site that was accessible to approximately 10,000 Connecticut residents and maintaining a toll free number. Id. at 165. The court exercised personal jurisdiction, reasoning that advertising on the Internet constituted the purposeful doing of business in Connecticut because "unlike television and radio advertising, the advertisement is available continuously to any
Internet user." Id. at 165.

Bensusan Restaurant Corp., v. King, 937 F.Supp. 296 (S.D.N.Y. 1996) reached a different conclusion based on a similar Web site. In Bensusan, the operator of a New York jazz club sued the operator of a Missouri jazz club for trademark infringement. Bensusan, 937 F.Supp. at 297. The Internet Web site at issue contained general information about the defendant's club, a calendar of events and ticket information. Id. However, the site was not interactive. Id. If a user wanted to go to the club, she would have to call or visit a ticket outlet and then pick up tickets at the club on the night of the show. Id. The court refused to exercise jurisdiction based on the Web site alone, reasoning that it did not rise to the level of purposeful availment of that jurisdiction's laws. The court distinguished the case from Compuserve, supra, where the user had "reached out from Texas to Ohio and 'originated and maintained' contacts with Ohio." Id. at 301.

Pres-Kap, Inc. v. System One Direct Access, Inc., 636 So.2d 1351 (Fla. App. 1994), review denied, 645 So.2d 455 (Fla. 1994) is not inconsistent with the above cases. In Pres-Kap, a majority of a three-judge intermediate state appeals court refused to exercise jurisdiction over a consumer of an on-line airline ticketing service. Pres-Kap involved a suit on a contract dispute in a Florida court by a Delaware corporation against its New York customer. Pres-Kap, 636 So.2d at 1351-52. The defendant had leased computer equipment which it used to access an airline ticketing computer located in Florida. Id. The contract was solicited, negotiated, executed and serviced in New York. Id. at 1252. The defendant's only contact with Florida consisted of logging onto the computer located in Florida and mailing payments for the leased equipment to Florida. Id. at 1253. Pres-Kap is distinguishable from the above cases and the case at bar because it addressed the exercise of jurisdiction over a consumer of on-line services as opposed to a provider. When a consumer logs onto a server in a foreign jurisdiction he is engaging in a fundamentally different type of contact than an entity that is using the Internet to sell or market products or services to residents of foreign jurisdictions. The Pres-Kap court specifically expressed concern over the implications of subjecting users of "on-line" services with contracts with out-of-state networks to suit in foreign jurisdictions. Id. at 1353.

3. Application to this Case

First, we note that this is not an Internet advertising case in the line of Inset Systems and Bensusan, supra. Dot Com has not just posted information on a Web site that is accessible to Pennsylvania residents who are connected to the Internet. This is not even an interactivity case in the line of Maritz, supra. Dot Com has done more than create an interactive Web site through which it exchanges information with Pennsylvania residents in hopes of using that information for commercial gain later. We are not being asked to determine whether Dot Com's Web site alone constitutes the purposeful availment of doing business in Pennsylvania. This is a "doing business over the Internet" case in the line of Compuserve, supra. We are being asked to determine whether Dot Com's conducting of electronic commerce with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania. We conclude that it does. Dot Com has contracted with approximately 3,000 individuals and seven Internet access providers in Pennsylvania. The intended object of these transactions has been the downloading of the electronic messages that form the basis of this suit in Pennsylvania.

We find Dot Com's efforts to characterize its conduct as falling short of purposeful availment of doing business in Pennsylvania wholly unpersuasive. At oral argument, Defendant repeatedly characterized its actions as merely "operating a Web site" or "advertising." Dot Com also cites to a number of cases from this Circuit which, it claims, stand for the proposition that merely advertising in a forum, without more, is not a sufficient minimal contact. [7] This argument is misplaced. Dot Com has done more than advertise on the Internet in Pennsylvania. Defendant has sold passwords to approximately 3,000 Subscribers in Pennsylvania and entered into seven contracts with Internet access providers to furnish its services to their customers in Pennsylvania.

Dot Com also contends that its contacts with Pennsylvania residents are "fortuitous" within the meaning of World Wide Volkswagen, 444 U.S. 286 (1980). Defendant argues that it has not "actively" solicited business in Pennsylvania and that any business it conducts with Pennsylvania residents has resulted from contacts that were initiated by Pennsylvanians who visited the Defendant's Web site. The fact that Dot
Com's services have been consumed in Pennsylvania is not "fortuitous" within the meaning of World Wide Volkswagen. In World Wide Volkswagen, a couple that had purchased a vehicle in New York, while they were New York residents, were injured while driving that vehicle through Oklahoma and brought suit in an Oklahoma state court. World Wide Volkswagen, 444 U.S. at 288. The manufacturer did not sell its vehicles in Oklahoma and had not made an effort to establish business relationships in Oklahoma. Id. at 295. The Supreme Court characterized the manufacturer's ties with Oklahoma as fortuitous because they resulted entirely out the fact that the plaintiffs had driven their car into that state. Id.

Here, Dot Com argues that its contacts with Pennsylvania residents are fortuitous because Pennsylvanians happened to find its Web site or heard about its news service elsewhere and decided to subscribe. This argument misconstrues the concept of fortuitous contacts embodied in World Wide Volkswagen. Dot Com's contacts with Pennsylvania would be fortuitous within the meaning of World Wide Volkswagen if it had no Pennsylvania subscribers and an Ohio subscriber forwarded a copy of a file he obtained from Dot Com to a friend in Pennsylvania or an Ohio subscriber brought his computer along on a trip to Pennsylvania and used it to access Dot Com's service. That is not the situation here. Dot Com repeatedly and consciously chose to process Pennsylvania residents' applications and to assign them passwords. Dot Com knew that the result of these contracts would be the transmission of electronic messages into Pennsylvania. The transmission of these files was entirely within its control. Dot Com cannot maintain that these contracts are "fortuitous" or "coincidental" within the meaning of World Wide Volkswagen. When a defendant makes a conscious choice to conduct business with the residents of a forum state, "it has clear notice that it is subject to suit there." World Wide Volkswagen, 444 U.S. at 297. Dot Com was under no obligation to sell its services to Pennsylvania residents. It freely chose to do so, presumably in order to profit from those transactions. If a corporation determines that the risk of being subject to personal jurisdiction in a particular forum is too great, it can choose to sever its connection to the state. Id. If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple -- it could have chosen not to sell its services to Pennsylvania residents.

Next, Dot Com argues that its forum-related activities are not numerous or significant enough to create a "substantial connection" with Pennsylvania. Defendant points to the fact that only two percent of its subscribers are Pennsylvania residents. However, the Supreme Court has made clear that even a single contact can be sufficient. McGee, 355 U.S. at 223. The test has always focused on the "nature and quality" of the contacts with the forum and not the quantity of those contacts. International Shoe, 326 U.S. at 320. The Sixth Circuit also rejected a similar argument in Compuserve when it wrote that the contacts were "deliberate and repeated even if they yielded little revenue." Compuserve, 89 F.2d at 1265.

We also conclude that the cause of action arises out of Dot Com's forum-related conduct in this case. The Third Circuit has stated that "a cause of action for trademark infringement occurs where the passing off occurs." Cottman Transmission Systems Inc. v. Martino, 36 F.3d 291, 294 (citing Tefal, S.A. v. Products Int'l Co., 529 F.2d 495, 496 n.1 (3d Cir. 1976); Indianapolis Colts v. Metro. Baltimore Football, 34 F.3d 410 (7th Cir. 1994). In Tefal, the maker and distributor of T-Fal cookware sued a partnership of California corporations in the District of New Jersey for trademark infringement. Tefal, 529 F.2d at 496. The defendants objected to venue in New Jersey, arguing that the contested trademark accounted for only about five percent of national sales. Id. On appeal, the Third Circuit concluded that since substantial sales of the product bearing the allegedly infringing mark took place in New Jersey, the cause of action arose in New Jersey and venue was proper. Tefal, 529 F.2d at 496-97.

In Indianapolis Colts, also case cited by the Third Circuit in Cottman, an Indiana National Football League franchise sued a Maryland Canadian Football League franchise in the Southern District of Indiana, alleging trademark infringement. Indianapolis Colts, 34 F.3d at 411. On appeal, the Seventh Circuit held that personal jurisdiction was appropriate in Indiana because trademark infringement is a tort-like injury and a substantial amount of the injury from the alleged infringement was likely to occur in Indiana. Id. at 412.

In the instant case, both a significant amount of the alleged infringement and dilution, and resulting
injury have occurred in Pennsylvania. The object of Dot Com's contracts with Pennsylvania residents is the transmission of the messages that Plaintiff claims dilute and infringe upon its trademark. When these messages are transmitted into Pennsylvania and viewed by Pennsylvania residents on their computers, there can be no question that the alleged infringement and dilution occur in Pennsylvania. Moreover, since Manufacturing is a Pennsylvania corporation, a substantial amount of the injury from the alleged wrongdoing is likely to occur in Pennsylvania. Thus, we conclude that the cause of action arises out of Dot Com's forum-related activities under the authority of both Tefal and Indianapolis Colts, supra.

Finally, Dot Com argues that the exercise of jurisdiction would be unreasonable in this case. We disagree. There can be no question that Pennsylvania has a strong interest in adjudicating disputes involving the alleged infringement of trademarks owned by resident corporations. We must also give due regard to the Plaintiff's choice to seek relief in Pennsylvania. Kulko, 436 U.S. at 92. These concerns outweigh the burden created by forcing the Defendant to defend the suit in Pennsylvania, especially when Dot Com knowingly chose to conduct business in Pennsylvania, pursuing profits from the actions that are now in question. The Due Process Clause is not a "territorial shield to interstate obligations that have been voluntarily assumed." Burger King, 471 U.S. at 474.


Defendant argues that, under the law of this Circuit, venue is only proper in trademark cases in the judicial district in which "a substantial part of the events or omissions giving rise to the claim occurred." In support of this proposition, Defendant cites Cottman Transmission Systems, Inc. v. Martino, 36 F.3d 291 (3d Cir. 1994). We cannot agree.

Venue in this case is governed by 28 U.S.C. §1391(b), the relevant portion of which provides:

(b) A civil action wherein jurisdiction is not founded solely on diversity of citizenship may, except as otherwise provided by law, be brought only in (1) a judicial district where any defendant resides, if all defendants reside in the same State, (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of the property that is the subject of the action is situated, or (3) a judicial district in which the defendant may be found if there is no district in which the action may otherwise be brought.

28 U.S.C. §1391(b). Subsection (c) further provides that a corporate defendant is "deemed to reside in any judicial district in which it is subject to personal jurisdiction at the time the action is commenced." 28 U.S.C. §1391(c). Dot Com is the only defendant in this case and it is a corporation. Thus, under the plain language of 28 U.S.C. §1391(b)(1), our previous discussion of personal jurisdiction is dispositive of the venue issue. Contrary to Dot Com's contention, Cottman does not command a different result.

Cottman involved a suit by a Pennsylvania corporation against a former Michigan franchisee and his wholly owned corporation for trademark infringement arising out of the continued use of the plaintiff's trademark after termination of the franchise agreement. The suit was brought in the Eastern District of Pennsylvania. Both defendants were Michigan residents and the corporation did business exclusively in Michigan. In the district court, the plaintiff relied exclusively on 28 U.S.C. §1391(b)(2) to establish venue. The district court found venue proper, reasoning that a "substantial part of the events or omissions giving rise to the claim occurred" in Pennsylvania. Cottman Transmission v. Metro Distributing, 796 F.Supp. 838, 844 (E.D. Pa. 1992). Thus, on appeal, the only issue before the Third Circuit was the propriety of venue under §1391(b)(2). In fact, the Third Circuit expressly stated that it was analyzing the case under §1391(b)(2). Cottman, 36 F.3d at 294. The Third Circuit read the record as only capable of supporting the contention that the defendants attempted to pass off the trademarks at issue in the Eastern District of Michigan. Id. at 296. Thus, the Third Circuit reversed, because a "substantial part of the events or omissions giving rise to the claim" had not occurred in the Eastern District of Pennsylvania. Id.

The fact that the Third Circuit analyzed Cottman under the standard in §1391(b)(2) does not mean that it applies to every trademark case. In fact, at oral argument, Dot Com conceded that if its reading of Cottman were the law, it would effectively render §1391(b)(1) inapplicable to trademark cases and
require the plaintiff to always satisfy §1391(b)(2) in order to lay venue. If the Third Circuit had intended to create such a radical departure from the plain language of §1391, it would have said so.

Since venue has been properly laid in this District, we cannot dismiss the action under 28 U.S.C. §1406(a). Jumara v. State Farm Inc. Co., 55 F.3d 873, 877 (3d Cir. 1995). We are also not permitted to compel the Plaintiff to accept a transfer against its wishes. Carteret v. Shusan, 919 F.2d 225, 232 (3d Cir. 1990).

IV. CONCLUSION

We conclude that this Court may appropriately exercise personal jurisdiction over the Defendant and that venue is proper in this judicial district. An appropriate order follows.

ORDER

McLAUGHLIN, J.

AND NOW, this 16th day of January 1997, IT IS HEREBY ORDERED that Defendant Zippo Dot Com's Motion to Dismiss for Improper Venue and Transfer under 28 U.S.C. §1406(a); Alternatively to Dismiss for Lack of Personal Jurisdiction [Doc. No. 9] is DENIED.

Sean J. McLaughlin

United States District Judge

cm: All parties of record.

End Notes

1. Return to Text Domain names serve as a primary identifier of an Internet user. Panavision Intern., L.P. v. Toeppen, 938 F.Supp. 616 (S.D. Cal. 1996). Businesses using the Internet commonly use their business names as part of the domain name (e.g. IBM.com). Id. The designation ".com" identifies the user as a commercial entity. Id.

2. Return to Text A "site" is an Internet address that permits the exchange of information with a host computer. Bensusan Restaurant Corp. v. King, 937 F.Supp. 295 (S.D.N.Y. 1996). The "Web" or "World Wide Web" refers to the collection of sites available on the Internet. Id.

3. Return to Text Dot Com has registered these domain names with Network Solutions, Inc. which has contracted with the National Science Foundation to provide registration services for Internet domain names. Once a domain name is registered to one user, it may not be used by another.

4. Return to Text For example, a typical message heading might appear as:

Subject: subject of the message From: name of person posting message Date: date posted Message-Id: identifying#ews.zippo.com Reference: reference# Organization: Zippo Newsgroups: news groups to which sender has subscribed The italicized text represents a generic description of specific information appearing in the message.


6. Return to Text "Shareware" is software which a user is permitted to download and use for a trial
period, after which the user is asked to pay a fee to the author for continued use. Compuserve, 89 F.2d at 1260. 7 Defendant has cited to: Gehling v. St. George's School of Medicine, Ltd., 773 F.2d 539 (1985); Fields v. Ramada Inn Inc., 816 F.Supp. 1033 (E.D. Pa. 1993); and Garofalo v. Praiss, 1990 WL 97800 (E.D.Pa. 1990). We note that these cases all involve the issue of whether advertising can rise to the level of "systematic and continuous" contacts for the purpose of general jurisdiction.

© 1997 The Bureau of National Affairs, Inc., All Rights Reserved
U.S. District Court for the District of New Jersey

Eileen WEBER, Plaintiff,
v.  
JOLLY HOTELS, et al., Defendants.

No. CIV a 96-2582

Sept. 12, 1997

No. CIV. A. 96-2582.

United States District Court,

D. New Jersey.


OPINION

WOLIN, District Judge.

This case arises out of an accident plaintiff, Eileen Weber, had while a guest at one of defendant's, Itajolly Compagnia Italiana Dei Jolly Hotels, hotels in Italy. Defendant moves this Court to dismiss the action for lack of personal jurisdiction pursuant to Rule 12(b)(2) of the Federal Rules of Civil Procedure. The Court will not grant the motion to dismiss despite concluding that it does not have jurisdiction over defendant. Instead, the Court will grant plaintiff's request to transfer the case to the Southern District of New York because the statute of limitations governing plaintiff's claim prevents the Court from dismissing the case without prejudice.

BACKGROUND

Defendant is an Italian corporation and its principal place of business is in Valdagno, Italy. (Zanuso Cert. ¶ 2). Defendant owns and operates thirty-two hotels in Italy, and independent subsidiaries own and operate hotels in Holland, France, Belgium, and New York. (Def.'s Resp. to Pl.'s Interrog. No. 2). (Zanuso Cert. ¶ 2). Defendant does not conduct any business in New Jersey. (Zanuso Cert. ¶ 4).

However, it does provide "photographs of hotel rooms, descriptions of hotel facilities, information about numbers of rooms and telephone numbers" on the Internet. (Pl's Br. in Opp. at 10).

In July 1993, defendant and Grand Circle Travel, a Massachusetts corporation, entered into an agreement whereby one of defendant's hotels, the Jolly Diodoro Hotel in Taormina, Sicily, Italy, would allot a certain number of rooms per week at the hotel for Grand Circle Travel during the 1994 calendar year. (Def. Ex. C). The agreement provided that defendant would bill Grand Circle Travel for the rooms
that it booked. (Def. Ex. C). Defendant also promised not to accept any bookings for the Jolly Diodoro Hotel from five enumerated tour groups or any other company claiming to represent the American Association of Retired Persons ("AARP"). (Def. Ex. C).

Grand Circle Travel and plaintiff have a relationship that dates back to 1976 when plaintiff embarked on a travel tour arranged by Grand Circle Travel. (Pl. Aff. ¶ 5). After the first trip, Grand Circle Travel sent plaintiff information and brochures about trips, tours, and travel attractions. (Pl. Aff. ¶ 7). Through the years, plaintiff went on trips arranged by Grand Circle Travel. (Pl. Aff. ¶ 8). In late 1993 or early 1994, Grand Circle Travel sent plaintiff a brochure that described a tour of Italy. (Pl. Aff. ¶ 9). On February 25, 1994, plaintiff booked a trip to Italy through Grand Circle Travel. (Pl. Aff. ¶ 10). Included in the trip was a stay at the Jolly Diodoro Hotel. (Pl. Aff. ¶ 10)

On December 7, 1994, plaintiff sustained injuries when she fell at the Jolly Diodoro Hotel. (Pl. Aff. ¶ 13). At the time of the accident, plaintiff was a guest of the hotel. Plaintiff is a citizen of New Jersey and a member of AARP. (Pl. Aff. ¶ 6). On June 26, 1995, plaintiff filed a Complaint and Jury Demand in the Superior Court of New Jersey, Law Division, Bergen County. She alleged that defendant knew or should have known of the dangerous condition on its premises. (Pl. Compl. ¶ 4). The case was removed to the United States District Court for the District of New Jersey on diversity grounds.

Defendant now moves the Court to dismiss the case for lack of personal jurisdiction.

**DISCUSSION**

1. **Personal Jurisdiction: Standards**


The purpose of restricting personal jurisdiction is to protect the individual interests of non-resident defendants. See United States v. Morton, 467 U.S. 822, 828 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291 (1980). A court may exercise personal jurisdiction over a non-resident defendant only where "minimum contacts" exist such that the exercise of jurisdiction "does not offend 'traditional notions of fair play and substantial justice.' " International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)). A defendant establishes minimum contacts with a forum state by committing some act by which he purposefully avails himself of the privilege of conducting activities within the forum state, thus invoking the benefits and protection of its laws. See Hanson v. Denckla, 357 U.S. 235, 253 (1958). These contacts must be of the nature such that the individual non-resident defendant "should reasonably anticipate being haled into court there." Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985) (citing World-Wide Volkswagen, 444 U.S. at 297). What constitutes minimum contacts varies with the "quality and the nature of defendant's activity." Hanson, 357 U.S. at 253.

A defendant can be subject to either specific or general personal jurisdiction in a forum state. To assert "general" jurisdiction, a plaintiff must establish that defendant's contacts with the forum state are so "continuous and substantial" with the forum state that the defendant should expect to be haled into court on any cause of action. Helicopteros Nacionales de Colombia. S.A. v. Hall, 466 U.S. 408, 414-16 & 414 n. 9 (1984); Provident Nat'l Bank v. California Fed. Say. & Loan Ass'n, 819 F.2d 434, 437 (3d Cir. 1987).

To establish specific jurisdiction, a defendant must have purposefully directed his activities at residents
of the forum, sufficient to establish minimum contacts under International Shoe. See Henry Heide, Inc. v. WRH Prods. Co., 766 F.2d 105, 108 (3d Cir. 1985). Specific personal jurisdiction may arise from particular or sporadic contacts if the "claim is related to or arises out of the defendant's contacts with the forum." Mellon Bank (East) PSFS Nat'l Ass'n v. Farino, 960 F.2d 1217, 1221 (3d Cir. 1992) (citations omitted); see also Helicopteros, 466 U.S. at 414 & 414 n. 8.

Once the defendant properly disputes the existence of personal jurisdiction, the plaintiff bears the burden to establish, by a preponderance of the evidence, sufficient facts demonstrating the court's jurisdiction. See Carteret Sav. Bank. FA v. Shushan, 954 F.2d 141, 146 (3d Cir.), cert. denied, 506 U.S. 817 (1992). In doing so, plaintiff must present a prima facie case for the exercise of personal jurisdiction by "establishing with reasonable particularity sufficient contacts between the defendant and the forum state." Mellon Bank (East) PSFS, 960 F.2d at 1223 (citing Provident Nat'l Bank, 819 F.2d at 437). The court must accept as true the allegations of the complaint, and resolve disputed issues of fact in favor of the plaintiff. See Carteret Sav. Bank, 954 F.2d at 142 n. 1.

If the plaintiff establishes a prima facie case supporting personal jurisdiction, the defendant then "bear[s] the burden of showing the unreasonableness of an otherwise constitutional assertion of jurisdiction ... ." Mellon Bank (East) PSFS, 960 F.2d at 1223. In assessing the reasonableness of the court's assertion of jurisdiction, the court evaluates several factors, including: the burden on the defendant, the forum state's interest in the litigation, the plaintiff's interest in pursuing its claims in the state, and the interstate judicial system's interest in the efficient resolution of claims. Burger King Corp., 471 U.S. at 477.

In examining personal jurisdiction under Rule 12(b)(2), the Court must look beyond the pleadings:

A Rule 12(b)(2) motion ... is inherently a matter which requires resolution of factual issues outside the pleadings, i.e. whether in personam jurisdiction actually lies. Once the defense has been raised, then the plaintiff must sustain its burden of proof in establishing jurisdictional facts through sworn affidavits or other competent evidence ... [A]t no point may a plaintiff rely on the bare pleadings alone in order to withstand a defendant's Rule 12(b)(2) motion to dismiss for lack of in personam jurisdiction. Once the motion is made, plaintiff must respond with actual proofs, not mere allegations.

Time Share Vacation Club v. Atlantic Resorts. Ltd., 735 F.2d 61, 67 n. 9 (3d Cir.1984); see also Mellon Bank (East) PSFS, 960 F.2d at 1223; Carteret Sav. Bank, 954 F.2d at 146.

2. Analysis

Plaintiff asserts that the Court has personal jurisdiction over defendant for two reasons: (1) defendant stands in the shoes of Grand Circle Travel because Grand Circle Travel is defendant's independent contractor; and (2) defendant's use of the Internet is equivalent to advertising in New Jersey. The first argument attempts to invoke specific jurisdiction whereas the second argument tries to invoke general jurisdiction. The Court rejects both arguments.

a. Specific Jurisdiction

Plaintiff asserts that a foreign company is subject to personal jurisdiction of a court that has jurisdiction over the company's independent contractor when the company has given the independent contractor the exclusive right to solicit and sell its product. She claims that the Court has jurisdiction over defendant because Grand Circle Travel directly solicited her with advertisements and brochures. Plaintiff relies on Van Eeuwen v. Heidelberg Eastern, Inc., 124 N.J.Super. 251 (App. Div.1973), and Rutherford v. Sherburne Corp., 616 F.Supp. 1456 (D.N.J.1985), to support her conclusion that jurisdiction is proper in this case. This assertion lacks merit for three reasons.

First, in this case, Grand Circle Travel does not have an exclusive right to solicit and sell defendant's rooms. The agreement provides that Grand Circle Travel will be allotted a certain number of rooms per week at one of defendant's hotels, the Jolly Diodoro Hotel, and that defendant would not accept bookings for the Jolly Diodoro Hotel from five enumerated tour groups or any other group claiming to represent the AARP. Moreover, if Grand Circle did not book the given number of rooms, defendant had
the option of accepting reservations from other people.

Second, plaintiff's reliance on Van Eeuwen, supra, is misplaced. In Van Eeuwen, the defendant gave Heidelberg Eastern, Inc., the exclusive right to distribute its printing press in more than seventy percent of the United States. 124 N.J.Super. at 254. The plaintiffs filed suit against the defendant and Heidelberg after they were injured while operating the printing press. Id. at 253. The Appellate Division concluded that it had jurisdiction over the defendant because it gave Heidelberg an exclusive right to sell its printing press in certain parts of the United States, because the defendant prepared advertisements and promotional publications for Heidelberg to distribute, and because a substantial amount of business occurred in New Jersey. Id. at 256-57. The panel reasoned that Heidelberg was an "integral spoke in a wheel in which [the defendant] is the hub" because the defendant created the exclusive distributorship agreement so that its product would be marketed and sold in the United States, including New Jersey. Id. at 258,59.

Van Eeuwen does not support plaintiff's position for three reasons. First, that case involved a product that was sold in New Jersey whereas this case involves a service that occurred in Italy. Second, Heidelberg had an exclusive distributorship for more than seventy percent of the United States whereas defendant gave Grand Circle Travel the exclusive rights to book rooms for members of the AARP at one of its hotels. Moreover, defendant allotted Grand Circle Travel a limited number of rooms at one of its hotels, and those rooms could be booked to other people if Grand Circle Travel did not book the rooms. Third, defendant did not supply Grand Circle Travel with advertisements or promotional materials. Thus, Grand Circle Travel is not an integral spoke in a wheel in which defendant is the hub. Moreover, Van Eeuwen is better suited for cases that arise out of the "stream of commerce" as opposed to a case like the one before the Court that deals with a service.

Finally, the facts of Rutherford, supra, substantially differ from those in this case. In Rutherford, the plaintiff was injured while skiing in Killington, Vermont. 616 F.Supp. at 1457. The plaintiff was a member of a New Jersey ski club that organized the trip to Killington. Id. The defendant, which owned the ski area where the plaintiff was injured, employed a representative to visit ski shops and clubs in New Jersey in order to solicit business for the ski area in Killington. Id. In addition, the defendant advertised in four New Jersey newspapers and two national magazines, which were distributed in New Jersey. Id. Finally, the defendant estimated how many patrons from New Jersey visited its ski area each year. Id. at 1458. Ultimately, the Court concluded that the plaintiff's injury was related to the defendant's forum activities and that the defendant had purposefully directed its activities at New Jersey residents. Id. at 1461.

In this case, defendant did not advertise in newspapers, send an employee into New Jersey to solicit business, or calculate how many of its guests were from New Jersey. In addition, this Court would be hard pressed to find that defendant's affiliation with Grand Circle Travel is tantamount to purposeful availment of New Jersey's laws and benefits. Therefore, the Court finds that specific jurisdiction does not exist.

b. General Jurisdiction

The Supreme Court has long recognized that personal jurisdiction must adapt to progress in technology. See Hanson, 357 at U.S. 250-51. Litigation involving the Internet has increased as the Internet has developed and expanded. Although the Internet is a new medium that raises new issues for the courts, district courts have successfully applied the principles established by International Shoe and its progeny to cases involving the Internet. See, e.g., CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996). The cases that have addressed the relationship between the Internet and personal jurisdiction "reveal[] that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." Zippo Manuf. Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119, 1124 (W.D.Pa. 1996).

The case dealing with this issue can be divided into three categories. See id. The first category includes cases where defendants actively do business on the Internet. See, e.g., CompuServe, 89 F.3d 1257. In those instances, personal jurisdiction is found because defendants "enter[] into contracts with residents
of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet." See Zippo, 962 F.Supp. at 1124 (citing Compuserve, 89 F.3d 1257). The second category deals with situations "where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site." Zippo, 962 F.Supp. at 1124 (citing Maritz, Inc. v. Cybergold, Inc., 947 F.Supp. 1328 (E.D.Mo.1996)). The third category involves passive Web sites; i.e., sites that merely provide information or advertisement to users. See Bensusan Restaurant Corp. v. King, 937 F.Supp. 295 (S.D.N.Y. 1996). Districts courts do not exercise jurisdiction in the latter cases because "a finding of jurisdiction ... 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 ...." Hearst Corp. v. Goldberger, 1997 WL 97097, at *1 (S.D.N.Y. Feb. 27, 1997).

Despite plaintiff's attempts to the contrary, this case clearly belongs in category three. Defendant placed information about its hotels on the Internet as an advertisement, not as a means of conducting business. In the past year, two district courts have refused to exercise jurisdiction over defendants who have a passive connection to the Internet. In Smith v. Hobby Lobby Stores, Inc., 968 F.Supp. 1356 (W.D.Ark. 1997), the Court found that an advertisement in a trade publication was an insufficient contact with the forum state because the defendant "did not contract to sell any goods or services to any citizens of Arkansas over the Internet site." Id. at 1365. In Hearst, supra, the Court concluded that advertising services on the Internet was equivalent to advertising in a national magazine, and that under New York law, such advertisements do not provide the requisite contacts to provide personal jurisdiction. 1997 WL 97097 at *10; see also Bensusan, 937 F.Supp. at 301 (finding that creation of Web site is not sufficient to find that defendant purposefully availed himself of forum).

This Court agrees with the finding in Hearst that advertising on the Internet falls under the same rubric as advertising in a national magazine. This Circuit has consistently held that advertising in national publications "does not constitute "continuous and substantial" contacts with the forum state." See, e.g., Gehling v. St. George's School of Medicine, 773 F.2d 539, 542 (3d Cir. 1985); see also Gianolo v. Walt Disney World Co., 753 F.Supp. 148, 156 (D.N.J. 1990) ("In an age of modern advertising and national media publications and markets, plaintiffs' argument that such conduct would make a defendant amenable to suit wherever the advertisements were aired would substantially undermine the law of personal jurisdiction."). In addition, advertising on the Internet is not tantamount to directing activity at or to purposefully availing oneself of a particular forum.

Thus, the Court finds that exercising jurisdiction over a defendant who merely advertises its services or product on the Internet would violate the Due Process Clause of the Fourteenth Amendment. Exercising jurisdiction in such a case would be unjust and would disrespect the principles established by International Shoe and its progeny.

3. Plaintiff's Request to Transfer

Plaintiff requests that the Court transfer the case to the Southern District of New York if it concludes that it does not have jurisdiction. Twenty-eight U.S.C. §1406(a) provides: "The district court of a district in which is filed a case laying venue in the wrong division or district shall dismiss, or if it be in the interest of justice, transfer such case to any district or division in which it could have been brought." Thus, section 1406(a) mandates that a district court can transfer a case to another district only if the other district has personal jurisdiction over the defendant.

In this instance, defendant has a subsidiary, Migdal Madison N.V., that owns a hotel in New York City. Migdal Madison is a Curacao corporation. (Def. Resp. to Pl.'s Interrog. No. 2). Plaintiff claims that the New York hotel accepts reservations for all of defendant's hotels in Italy. (Farber Cert. ¶ 6). Thus, plaintiff concludes that a New York court would have jurisdiction over defendant.

Courts have consistently found that a subsidiary corporation's contacts with the forum are not sufficient grounds to exercise jurisdiction over the parent corporation without a showing of something more than ownership. See, e.g., Lucas v. Gulf & Western Indus., Inc., 666 F.2d 800, 805-06 (3d Cir. 1981);
Pfundstein v. Omnicon Group, 285 N.J.Super. 245, 253 (App. Div. 1995). "Other factors which may have a bearing on the jurisdictional issue are whether the subsidiary played any part in the transactions at issue, whether the subsidiary was merely the alter ego or agent of the parent, and whether the independence of the separate corporate entities was disregarded." Lucas, 666 F.2d at 806. In this case, the evidence is far too scant to determine whether Migdal Madison, N.V., is the alter ego or agent of defendant or whether it is independent of defendant. Thus, the Court cannot determine whether a district court in New York has personal jurisdiction over defendant.

The Court normally does not transfer cases to other districts unless it is certain that the other district has personal jurisdiction over the defendant. If the Court is unsure whether the other district has personal jurisdiction over the defendant, it usually dismisses without prejudice so that the plaintiff does not lose his cause of action. This case, however, presents an unusual situation because if the Court dismisses without prejudice, the statute of limitations will bar plaintiff from bringing a claim.

Although the Court is sensitive to the policies underlying section 1406(a) and to the dockets in other districts, the interests of justice dictate that this case be transferred to the Southern District of New York. The question of whether personal jurisdiction exists in New York should be decided after the transfer.

CONCLUSION

Thus, the Court finds that it does not have personal jurisdiction over defendant, but will order that the case be transferred to the Southern District of New York. An appropriate Order is attached.

ORDER

In accordance with the Court's Opinion filed

herewith,

It is on this 12th day of September, 1997

ORDERED that this case be transferred to the Southern District of New York.

© 1997 The Bureau of National Affairs Inc., All Rights Reserved
U.S. 9th Circuit Court of Appeals

CYBERSELL INC. v CYBERSELL, INC.
9617087

CYBERSELL, INC., an Arizona corporation,
Plaintiff-Appellant,

v.

CYBERSELL, INC., a Florida corporation; WEBHORIZONS, INC., a D.C. No.
Florida corporation; WEBSOLVERS, INC., a Florida corporation;
SAMUEL C. CERTO, husband; JANE DOE CERTO, wife; MATT CERTO,
husband; JANE DOE II CERTO, wife;
CYBERGATE, INC., a corporation;
SPRINTNET, a corporation,
Defendants-Appellees.

Appeal from the United States District Court
for the District of Arizona
Earl H. Carroll, District Judge, Presiding

Argued and Submitted
November 6, 1997--San Francisco, California

Filed December 2, 1997

Before: Harlington Wood, Jr.,* Pamela Ann Rymer, and
A. Wallace Tashima, Circuit Judges.

Opinion By Judge Rymer

SUMMARY

COUNSEL

Connie J. Mableson, Phoenix, Arizona, for the plaintiff-appellant.
Michael R. Levin and Christopher T. Hill, Rumberger, Kirk & Caldwell, Orlando, Florida, for the defendants-appellees.

---

OPINION

RYMER, Circuit Judge:

We are asked to hold that the allegedly infringing use of a service mark in a home page on the World Wide Web suffices for personal jurisdiction in the state where the holder of the mark has its principal place of business. Cybersell, Inc., an Arizona corporation that advertises for commercial services over the Internet, claims that Cybersell, Inc., a Florida corporation that offers web page construction services over the Internet, infringed its federally registered mark and should be amenable to suit in Arizona because cyberspace is without borders and a web site which advertises a product or service is necessarily intended for use on a world wide basis. The district court disagreed, and so do we. Instead, applying our normal "minimum contacts" analysis, we conclude that it would not comport with "traditional notions of fair play and substantial justice," Core-Vent Corp. v. Nobel Indus. AB, 11 F.3d 1482, 1485 (9th Cir. 1993) (quoting International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945)), for Arizona to exercise personal jurisdiction over an allegedly infringing Florida web site advertiser who has no contacts with Arizona other than maintaining a home page that is accessible to Arizonans, and everyone else, over the Internet. We therefore affirm.

I

Cybersell, Inc. is an Arizona corporation, which we will refer to as Cybersell AZ. It was incorporated in May 1994 to provide Internet and web advertising and marketing services, including consulting. The principals of Cybersell AZ are Laurence Canter and Martha Siegel, known among web users for first "spamming" the Internet.1 Mainstream print media carried the story of Canter and Siegel and their various efforts to commercialize the web.

On August 8, 1994, Cybersell AZ filed an application to register the name "cybersell" as a service mark. The application was approved and the grant was published on October 30, 1995. Cybersell AZ operated a web site using the mark from August 1994 through February 1995. The site was then taken down for reconstruction.

Meanwhile, in the summer of 1995, Matt Certo and his father, Dr. Samuel C. Certo, both Florida residents, formed Cybersell, Inc., a Florida corporation (Cybersell FL), with its principal place of business in Orlando. Matt was a business school student at Rollins College, where his father was a professor; Matt was particularly interested in the Internet, and their company was to provide business consulting services for strategic management and marketing on the web. At the time the Certos chose the name "Cybersell" for their venture, Cybersell AZ had no home page on the web nor had the PTO granted their application for the service mark.

As part of their marketing effort, the Certos created a web page at http://www.cybersell.com/cybersell/index.htm. The home page has a logo at the top with "CyberSell" over a depiction of the planet earth, with the caption underneath "Professional Services for the World Wide Web" and a local (area code 407) phone number. It proclaims in large letters "Welcome to CyberSell!" A hypertext link2 allows the browser to introduce himself, and invites a company not on the web -- but inter-
himself, and invites a company not on the web -- but interested in getting on the web --- to "Email us to find out how!"

Canter found the Cybersell FL web page and sent an e-mail on November 27, 1995 notifying Dr. Certo that "Cybersell" is a service mark of Cybersell AZ. Trying to disassociate themselves from the Canters, the Certos changed the name of Cybersell FL to WebHorizons, Inc. on December 27 (later it was changed again to WebSolvers, Inc.) and by January 4, 1996, they had replaced the CyberSell logo at the top of their web page with WebHorizons, Inc. The WebHorizons page still said "Welcome to CyberSell!"

Cybersell AZ filed the complaint in this action January 9, 1996 in the District of Arizona, alleging trademark infringement, unfair competition, fraud, and RICO violations. On the same day Cybersell FL filed suit for declaratory relief with regard to use of the name "Cybersell" in the United States District Court for the Middle District of Florida, but that action was transferred to the District of Arizona and consolidated with the Cybersell AZ action. Cybersell FL moved to dismiss for lack of personal jurisdiction. The district court denied Cybersell AZ's request for a preliminary injunction, then granted Cybersell FL's motion to dismiss for lack of personal jurisdiction. Cybersell AZ timely appealed.

II

[1] The general principles that apply to the exercise of personal jurisdiction are well known. As there is no federal statute governing personal jurisdiction in this case, the law of Arizona applies. Under Rule 4.2(a) of the Arizona Rules of Civil Procedure, an Arizona court may exercise personal jurisdiction over parties, whether found within or outside the state, to the maximum extent permitted by the Constitution of this state and the Constitution of the United States.

The Arizona Supreme Court has stated that under Rule 4.2(a), "Arizona will exert personal jurisdiction over a nonresident litigant to the maximum extent allowed by the federal constitution." Uberti v. Leonardo, 181 Ariz. 565, 569, 892 P.2d 1354, 1358, cert. denied, 116 S. Ct. 273 (1995). Thus, Cybersell FL may be subject to personal jurisdiction in Arizona so long as doing so comports with due process.

[2] A court may assert either specific or general jurisdiction over a defendant. See Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 (1984). Cybersell AZ concedes that general jurisdiction over Cybersell FL doesn't exist in Arizona, so the only issue in this case is whether specific jurisdiction is available.

[3] We use a three-part test to determine whether a district court may exercise specific jurisdiction over a nonresident defendant:

(1) The nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections[;] (2) [t]he claim must be one which arises out of or results from the defendant's forum-related activities[; and] (3) [e]xercise of jurisdiction must be reasonable.

Ballard v. Savage, 65 F.3d 1495, 1498 (9th Cir. 1995) (citations omitted).
Cybersell A2 argues that the test is met because trademark infringement occurs when the passing off of the mark occurs, which in this case, it submits, happened when the name "Cybersell" was used on the Internet in connection with advertising. Cybersell FL, on the other hand, contends that a party should not be subject to nationwide, or perhaps worldwide, jurisdiction simply for using the Internet.

A

[4] Since the jurisdictional facts are not in dispute, we turn to the first requirement, which is the most critical. As the Supreme Court emphasized in Hanson v. Denckla, "it is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." 357 U.S. 235, 253 (1958). We recently explained in Ballard that

the "purposeful availment" requirement is satisfied if the defendant has taken deliberate action within the forum state or if he has created continuing obligations to forum residents. "It is not required that a defendant be physically present within, or have physical contacts with, the forum, provided that his efforts 'are purposefully directed' toward forum residents."

Ballard, 65 F.2d at 1498 (citations omitted).

We have not yet considered when personal jurisdiction may be exercised in the context of cyberspace, but the Second and Sixth Circuits have had occasion to decide whether personal jurisdiction was properly exercised over defendants involved in transmissions over the Internet, see CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), aff'd, No. 96-9344, 1383, 1997 WL 560048 (2d Cir. Sept. 10, 1997), as have a number of district courts. Because this is a matter of first impression for us, we have looked to all of these cases for guidance. Not surprisingly, they reflect a broad spectrum of Internet use on the one hand, and contacts with the forum on the other. As CompuServe and Bensusan seem to represent opposite ends of the spectrum, we start with them. 4

CompuServe is a computer information service headquartered in Columbus, Ohio, that contracts with individual subscribers to provide access to computing and information services via the Internet. It also operates as an electronic conduit to provide computer software products to its subscribers. Computer software generated and distributed in this way is often referred to as "shareware." Patterson is a Texas resident who subscribed to CompuServe and placed items of "shareware" on the CompuServe system pursuant to a "Shareware Registration Agreement" with CompuServe, which provided, among other things, that it was "to be governed by and construed in accordance with" Ohio law. During the course of this relationship, Patterson electronically transmitted thirty-two master software files to CompuServe, which CompuServe stored and displayed to its subscribers. Sales were made in Ohio and elsewhere, and funds were transmitted through CompuServe in Ohio to Patterson in Texas. In effect, Patterson used CompuServe as a distribution center to market his software. When Patterson threatened litigation over allegedly infringing CompuServe software, CompuServe filed suit in Ohio seeking a declaratory judgment of noninfringement. The court found that Patterson's relationship with CompuServe as a software provider and marketer was a crucial indicator that Patterson had knowingly reached out to Compu-
Serve's Ohio home and benefitted from CompuServe's handling of his software and fees. Because Patterson had chosen to transmit his product from Texas to CompuServe's system in Ohio, and that system provided access to his software to others to whom he advertised and sold his product, the court concluded that Patterson purposefully availed himself of the privilege of doing business in Ohio.

By contrast, the defendant in Bensusan owned a small jazz club known as "The Blue Note" in Columbia, Missouri. He created a general access5 web page that contained information about the club in Missouri as well as a calendar of events and ticketing information. Tickets were not available through the web site, however. To order tickets, web browsers had to use the names and addresses of ticket outlets in Columbia or a telephone number for charge-by-phone ticket orders, which were available for pick-up on the night of the show at the Blue Note box office in Columbia. Bensusan was a New York corporation that owned "The Blue Note," a popular jazz club in the heart of Greenwich Village. Bensusan owned the rights to the "The Blue Note" mark. Bensusan sued King for trademark infringement in New York. The district court distinguished King's passive web page, which just posted information, from the defendant's use of the Internet in CompuServe by observing that whereas the Texas Internet user specifically targeted Ohio by subscribing to the service, entering into an agreement to sell his software over the Internet, advertising through the service, and sending his software to the service in Ohio,

King has done nothing to purposefully avail himself of the benefits of New York. King, like numerous others, simply created a Web site and permitted anyone who could find it to access it. Creating a site, like placing a product into the stream of commerce, may be felt nationwide-or even worldwide-but, without more, it is not an act purposefully directed toward the forum state.

Bensusan, 937 F. Supp. at 301 (citing the plurality opinion in Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 112 (1992)). Given these facts, the court reasoned that the argument that the defendant "should have foreseen that users could access the site in New York and be confused as to the relationship of the two Blue Note clubs is insufficient to satisfy due process." Id. at 301.

[5] "Interactive" web sites present somewhat different issues. Unlike passive sites such as the defendant's in Bensusan, users can exchange information with the host computer when the site is interactive. Courts that have addressed interactive sites have looked to the "level of interactivity and commercial nature of the exchange of information that occurs on the Web site" to determine if sufficient contacts exist to warrant the exercise of jurisdiction. See, e.g., Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (finding purposeful availment based on Dot Com's interactive web site and contracts with 3000 individuals and seven Internet access providers in Pennsylvania allowing them to download the electronic messages that form the basis of the suit); Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1332-33 (E.D. Mo.) (browsers were encouraged to add their telephone number to a mailing list that basically subscribed the user to the service), reconsideration denied, 947 F. Supp. 2448 (1996).

[6] Cybersell AZ points to several district court decisions which it contends have held that the mere advertisement or solicitation for sale of goods and services on the Internet gives
rise to specific jurisdiction in the plaintiff's forum. However, so far as we are aware, no court has ever held that an Internet advertisement alone is sufficient to subject the advertiser to jurisdiction in the plaintiff's home state. See, e.g., Smith v. Hobby Lobby Stores, 968 F. Supp. 1356 (W.D. Ark. 1997) (no jurisdiction over Hong Kong defendant who advertised in "By Mail" portion posted on the Internet without sale of goods or services in Arkansas). Rather, in each, there has been "something more" to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state.

Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996), is the case most favorable to Cybersell AZ's position. Inset developed and marketed computer software throughout the world; Instruction Set, Inc. (ISI) provided computer technology and support. Inset owned the federal trademark "INSET"; but ISI obtained "INSET.COM" as its Internet domain address for advertising its goods and services. ISI also used the telephone number "1-800-US-INSET." Inset learned of ISI's domain address when it tried to get the same address and filed suit for trademark infringement in Connecticut. The court reasoned that ISI had purposefully availed itself of doing business in Connecticut because it directed its advertising activities via the Internet and its toll-free number toward the state of Connecticut (and all states); Internet sites and toll-free numbers are designed to communicate with people and their businesses in every state; an Internet advertisement could reach as many as 10,000 Internet users within Connecticut alone; and once posted on the Internet, an advertisement is continuously available to any Internet user.

Cybersell AZ further points to the court's statement in EDIAS Software International, L.L.C. v. BASIS International Ltd., 947 F. Supp. 43 (D. Ariz. 1996) that a defendant "should not be permitted to take advantage of modern technology through an Internet Web page and forum and simultaneously escape traditional notions of jurisdiction." Id. at 420. In that case, EDIAS (an Arizona company) alleged that BASIS (a New Mexico company) sent advertising and defamatory statements over the Internet through e-mail, its Web page, and forums. However, the court did not rest its minimum contacts analysis on use of the Internet alone; in addition to the Internet, BASIS had a contract with EDIAS, it made sales to EDIAS and other Arizona customers, and its employees had visited Arizona during the course of the business relationship with EDIAS.

[7] Some courts have also given weight to the number of "hits" received by a Web page from residents in the forum state, and to other evidence that Internet activity was directed at, or bore fruit in, the forum state. See, e.g., Heroes, Inc. v. Heroes Found., 958 F. Supp. 1 (D.D.C. 1996) (Web page that solicited contributions and provided toll-free telephone number along with the defendant's use on the Web page of the allegedly infringing trademark and logo, along with other contacts, provided sustained contact with the District), amended by No. Civ.A. 96-1260 (TAP) (1997); Pres-Kap, Inc. v. System One, Direct Access, Inc., 636 So.2d 1351 (Fla. Dist. Ct. App. 1994) (declining jurisdiction where defendant consumer subscribed to plaintiff's travel reservation system but was solicited and serviced instate by the supplier's local representative).

[8] In sum, the common thread, well stated by the district court in Zippo, is that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." Zippo, 952 F. Supp. at 1124.
[9] Here, Cybersell FL has conducted no commercial activity over the Internet in Arizona. All that it did was post an essentially passive home page on the web, using the name "Cybersell," which Cybersell AZ was in the process of registering as a federal service mark. While there is no question that anyone, anywhere could access that home page and thereby learn about the services offered, we cannot see how from that fact alone it can be inferred that Cybersell FL deliberately directed its merchandising efforts toward Arizona residents.

[10] Cybersell FL did nothing to encourage people in Arizona to access its site, and there is no evidence that any part of its business (let alone a continuous part of its business) was sought or achieved in Arizona. To the contrary, it appears to be an operation where business was primarily generated by the personal contacts of one of its founders. While those contacts are not entirely local, they aren't in Arizona either. No Arizonan except for Cybersell AZ "hit" Cybersell FL's web site. There is no evidence that any Arizona resident signed up for Cybersell FL's web construction services. It entered into no contracts in Arizona, made no sales in Arizona, received no telephone calls from Arizona, earned no income from Arizona, and sent no messages over the Internet to Arizona. The only message it received over the Internet from Arizona was from Cybersell AZ. Cybersell FL did not have an "800" number, let alone a toll-free number that also used the "Cybersell" name. The interactivity of its web page is limited to receiving the browser's name and address and an indication of interest -- signing up for the service is not an option, nor did anyone from Arizona do so. No money changed hands on the Internet from (or through) Arizona. In short, Cybersell FL has done no act and has consummated no transaction, nor has it performed any act by which it purposefully availed itself of the privilege of conducting activities in Arizona, thereby invoking the benefits and protections of Arizona law.

[11] We therefore hold that Cybersell FL's contacts are insufficient to establish "purposeful availment." Cybersell AZ has thus failed to satisfy the first prong of our three-part test for specific jurisdiction. We decline to go further solely on the footing that Cybersell AZ has alleged trademark infringement over the Internet by Cybersell FL's use of the registered name "Cybersell" on an essentially passive web page advertisement. Otherwise, every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located. That would not comport with traditional notions of what qualifies as purposeful activity invoking the benefits and protections of the forum state. See Peterson v. Kennedy, 771 F.2d 1244, 1262 (9th Cir. 1985) (series of phone calls and letters to California physician regarding plaintiff's injuries insufficient to satisfy first prong of test).

III

[12] Cybersell AZ also invokes the "effects" test employed in Calder v. Jones, 465 U.S. 783 (1984), and Core-Vent Corp. v. Nobel Industries, 11 F.3d 1482 (9th Cir. 1993), with respect to intentional torts directed to the plaintiff, causing injury where the plaintiff lives. However, we don't see this as a Calder case. Because Shirley Jones was who she was (a famous entertainer who lived and worked in California) and was libeled by a story in the National Enquirer, which was published in Florida but had a nationwide circulation with a
large audience in California, the Court could easily hold that California was the "focal point both of the story and of the harm suffered" and so jurisdiction in California based on the "effects" of the defendants' Florida conduct was proper. Calder, 465 U.S. at 782. There is nothing comparable about Cybersell FL's web page. Nor does the "effects " test apply with the same force to Cybersell AZ as it would to an individual, because a corporation "does not suffer harm in a particular geographic location in the same sense that an individual does." Core-Vent, 11 F.3d at 1486. Cybersell FL's web page simply was not aimed intentionally at Arizona knowing that harm was likely to be caused there to Cybersell AZ. 6

IV

[13] We conclude that the essentially passive nature of Cybersell FL's activity in posting a home page on the World Wide Web that allegedly used the service mark of Cybersell AZ does not qualify as purposeful activity invoking the benefits and protections of Arizona. As it engaged in no commercial activity and had no other contacts via the Internet or otherwise in Arizona, Cybersell FL lacks sufficient minimum contacts with Arizona for personal jurisdiction to be asserted over it there. Accordingly, its motion to dismiss for lack of personal jurisdiction was properly granted.

AFFIRMED.

FOOTNOTES

*Honorable Harlington Wood, Jr., Senior Circuit Judge, United States Court of Appeals for the Seventh Circuit, sitting by designation.

1 Spamming refers to the posting indiscriminately of advertisements to news groups on the web. Unlike crossposting, spamming individually posts the advertisement to each news group, requiring the recipient to delete the message from each news group to which she has subscribed.

2 A hypertext link allows a user to move directly from one web location to another by using the mouse to click twice on the colored link.

3 In its October 21, 1996 judgment, the district court dismissed both of the consolidated actions.

4 Since Bensusan was decided on the basis of New York's long-arm statute (which requires presence in the forum and is therefore more stringent than due process), its holding is not instructive, but the district court's analysis is. The district court dismissed for lack of personal jurisdiction under the long-arm statute as well as on due process grounds, while the Second Circuit affirmed on the statute and did not discuss the constitutional issue.

5 A general access site requires no authentication or access code for entry. Bensusan, 937 F. Supp. at 297. Thus, the site is accessible to anyone who has access to the Internet.

6 Likewise unpersuasive is Cybersell AZ's reliance on Panavision International v. Toeppe, 938 F. Supp. 616 (C.D. Cal. 1996), where the court found the "purposeful availment" prong satisfied by the effects felt in California, the home state of Panavision, from Toeppe's alleged out-of-state scheme to register domain names using the trademarks of California companies, including Panavision, for the purpose of extorting fees from them. Again, there is nothing analogous about Cybersell FL's conduct. the end
IN THE CIRCUIT COURT OF JACKSON COUNTY, MISSOURI AT KANSAS CITY

STATE OF MISSOURI, ex rel. JEREMIAH W. (JAY) NIXON, Attorney General, Plaintiff,
vs.
INTERACTIVE GAMING & COMMUNICATIONS CORP.,
a Delaware corporation, Defendant.

Case No. CV97-7808

ORDER GRANTING PERMANENT INJUNCTION
AND FINAL JUDGMENT

Now on this 22nd day of May, 1997, the Court takes up for hearing Plaintiff's cause of action entitled State of Missouri. ex rel. Jeremiah W. (Jay) Nixon, Attorney General v. Interactive Gaming & Communications Corp., Case No. CV97-7808, for hearing. Plaintiff appears by Assistant Attorneys General J. Dale Youngs and Sue A. Sperry. Defendant Interactive Gaming & Communications Corp. ("IGC") does not appear either by representative or by counsel. Upon Defendant's failure to appear, failure to file an answer or otherwise respond to Plaintiff's petition, hearing the evidence presented, the argument of counsel, being otherwise duly advised in the premises and pursuant to Rule 74.05 of the Missouri Rules of Civil Procedure, the Court finds that an Order Granting a Permanent Injunction and Final Judgment should be GRANTED. Specifically, the Court finds that:

1. On April 7, 1997, Plaintiff, pursuant to Section 407.100 RSMo 1994, filed a Petition for Injunction, Restitution, Penalties and Other Relief in the above styled action alleging that certain violations of the Missouri Merchandising Practices Act, Chapter 407, RSMo 1994, had been committed by Defendant IGC. Defendant IGC was served with summons and that petition on April 14, 1997. A First Amended Petition was filed on April 10, 1997 and was served on April 11, 1997;

2. A hearing on Plaintiff's motion for preliminary injunction was scheduled for 9 a.m., May 22, 1997 in Division 7 of the Jackson County Circuit Court in Kansas City, MO. Prior to that time, Defendant IGC had failed answer or otherwise respond to Plaintiff's petition, despite being served with same on April 14 at the latest. No one appeared for Defendant IGC at the above hearing, and Plaintiff introduced into evidence a letter (Exhibit 28) dated May 22, 1997 from Lawrence Hirsch, an attorney and officer of IGC, which indicated IGC's intention not to appear at the hearing;

3. Plaintiff produced and examined four witnesses and offered 26 exhibits which were admitted into evidence;
4. Plaintiffs evidence showed and the Court finds that:

(a) Jeremiah W. (Jay) Nixon is the duly elected and acting Attorney General of the State of Missouri and that he brought this suit in his official capacity pursuant to §§407.020 and .100, RSMo 1994.

(b) IGC is a Delaware Corporation with its principal place of business in Blue Bell, PA, that Global Casino Ltd., a corporation organized under the laws of Granada, is a wholly owned subsidiary of IGC;

(c) IGC so controls the operation, funding, management and business practices of Global Casino, Ltd., that the subsidiary is merely the "alter ego" of IGC and that this control has used by IGC to commit wrongs and violations of Missouri as more specifically set forth below;

(d) IGC markets, advertises, offers, promotes and sells casino gambling services such as slots, blackjack and roulette through its alter ego Global Casino, Ltd. All of these services are accessed by consumers, including Missouri residents, through IGC's Internet website at "www.gamblenet.com."

(e) Beginning on February 10, 1997, Plaintiff, pursuant to §§407.020, .040 and. 100 RSMo 1994, conducted an investigation of the marketing, advertising, promotion, offering and sale by Defendant IGC of casino gambling global communications network called the Interact to determine services over the if certain violations of the Missouri Merchandising Practices Act, Chapter 407, RSMo 1994, had been committed by Defendant;

(f) During that investigation, an investigator for the Missouri Attorney General's Office accessed IGC's website from a computer located at 3100 Broadway, Kansas City, Jackson County, MO 64111;

(g) On or about February 14, 1997, an investigator for the Consumer Protection Division of the Missouri Attorney General's Office accessed IGC's website from a computer terminal located at 3100 Broadway, Kansas City, Jackson County, Missouri. At that time the website was advertising to Internet consumers, including those located in Missouri, the opportunity to participate in gambling activities called "slot tournaments" to be held on the Internet by IGC. IGC promoted its website, including these slot tournaments, to Missouri consumers by, other among methods, maintaining its website promoting its website, in consumers through its is answered at the company's offices in Pennsylvania, and which consumers could call for more information about the gambling services offered by its wholly owned Subsidiary. In response to consumers' calls to the toll free number advertised by IGC, IGC sends brochures to consumers describing and promoting its gambling services. IGC also transmits press releases and other information about Global Casino and its gambling services into the State of Missouri by e-mail;

(h) According to IGC, Internet users could register to participate in its gambling activities by completing an "Account Application" and mailing it to Global Casino in care of IGC at 595 Skippack Pike, Suite 100, Blue Bell, PA 19422 or faxing it to (215) 540-8176. In addition, participants were required to pay fees of $100, $200 or $500, depending upon which tournament they entered. Methods of payment included sending a bank wire to Madison Bank, Blue Bell, PA or by sending a money order to Global Casino, in care of IGC at the above address. The above referenced "application" in fact constitutes an acceptance by consumers in MISSOURI of IGC's offer to provide access to these gambling activities in exchange for payment of the fees set forth above;

(i) On February 25, 1997, the investigator contacted Global Casino in care of IGC at the telephone number advertised on the website: 1888-BET-NETT. The telephone call was placed from a telephone located at 3100 Broadway, Kansas City, Jackson County, Missouri. The telephone call was answered "Good Afternoon. Global Casino" by a woman named Marjorie who represented that she was speaking on behalf of Global Casino and who indicated in response to questions that she was located in Pennsylvania. Upon being informed that the caller lived in Kansas City, Missouri, and being asked if he would "get in trouble" for participating in the slot tournaments offered by Global Casino. Marjorie said "No." When asked if the gambling services offered by Global Casino and his participation in them were
legal, Marjorie said "Yes;"

(j) On March 12, 1997, as instructed by Marjorie, the investigator completed and faxed his acceptance of the offer to participate in the slot tournament to Global Casino in care of IGC. Also pursuant to Marjorie's instructions, a money order for $100 in the name of Global Casino was sent from Missouri to Global Casino in care of IGC at the above address in Blue Bell, PA. In addition, Marjorie sent the investigator a brochure regarding the sports book operated by IGC through Sports International, as well as an application to become a member. The investigator also received press releases and other information about Global Casino transmitted to his e-mail box located in Kansas City, Jackson County, Missouri;

(k) On March 17, 1997, the investigator received his login name and password from Global Casino and began gambling in the slot tournament operated by Global Casino on behalf of IGC, utilizing a computer with access to the Internet located 3100 Broadway, Kansas City, Jackson County, Missouri. IGC's offer to provide the above described gambling services in exchange for payment of the registration fee was accepted in the State of Missouri, causing a contract to be made within the state, and constituting the further transaction of business within the state pursuant to §506.500, RSMo 1994;

(l) On April 24, 1997, Plaintiff and IGC entered into an agreement whereby IGC agreed not to accept any applications from Missouri residents for casino gambling services and agreed not to open any gambling accounts for Missouri residents until May 22, 1997, the date of the preliminary injunction hearing;

(m) From May 9, to May 20, 1997, IGC accepted the application and opened a gambling account for another investigator for the Attorney General's Office, accepted a $200 deposit into that account and allowed the investigator to participate in IGC's casino gambling services;

(n) "Gambling" is defined by §572.010(4) as the staking or risking of something of "value upon the outcome of a contest of chance or a future contingent event not under his control or influence, upon an agreement or understanding that he will receive something of value in the event of a certain outcome ... Gambling does not include any bona fide business transactions valid under the law of contracts ... any licensed activity, or persons participating in such games which are covered by §§313.800 to 313.840, RSMo." Participation by Missouri consumers in the slot tournaments marketed, advertised, offered, sold and promoted by IGC and its subsidiary constitutes "gambling" under §572.010(4), RSMo 1994. Such gambling activities are declared unlawful by §572.020, RSMo 1994;

(o) Under §572.010(1), a person "advances gambling activity" if, acting other than as a player, he engages in conduct that materially aids any form of gambling activity. Conduct of this nature includes but is not limited to conduct directed toward the creation of establishment of the particular game, lottery, contest, scheme, device or activity involved ...;"

(p) IGC's conduct in advertising, promoting and selling to Missouri consumers access to its gambling services as described above constitutes the "advancement" and/or "promotion", of gambling under §572.010(1). Such activities on the part of IGC and consumers participating in the services promoted, advertised and sold by IGC are declared illegal in the State of Missouri by §§572.030 and 572.040, RSMo 1994;

(q) Nowhere in the information provided by IGC either on the Internet, by telephone or through E-mail is there any notice that the gambling services promoted and sold by IGC through its wholly-owned and controlled subsidiary, as well as a consumer's participation therein, are illegal;

(r) On February 25, 1997, a designated representative of Global Casino which is controlled by IGC, affirmatively stated that the gambling services advertised and sold by IGC, and the investigator's participation in those activities were legal in the State of Missouri;

(s) Section 4097.020, RSMo 1994 provides, in pertinent part:
The act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce or the solicitation of any funds for any charitable purpose, as defined in Section 497.453, in or from the State of Missouri, is declared to be an unlawful practice.

Section 497.100, RSMo 1994, provides:

1. Whenever it appears to the Attorney General that a person has engaged in, is engaging in or is about to engage in any method, act, use, practice or solicitation, or any combination thereof, declared to be unlawful by this chapter, he may seek and obtain, in an action in a circuit court, an injunction prohibiting such person from continuing such methods, acts, uses, practices, or solicitations, or any combination thereof, or engaging therein, or doing anything in furtherance thereof.

2. In any action under subsection of this section, and pursuant to the provisions of the Missouri Rules of Civil Procedure, the attorney general may seek and obtain temporary restraining orders, preliminary injunction, temporary receivers, and the sequestering of any funds or accounts if the court finds that funds or property may be hidden or removed from the state or that such orders or injunctions are otherwise necessary.

3. If court finds that the person has engaged in, is engaging in, or is about to engage in any method, act, use, practice or solicitation, or any combination thereof, declared to be unlawful by this chapter, it may make such orders or judgments as may be necessary to prevent such person from employing or continuing to employ, or to prevent the recurrence of, any prohibited methods, acts, uses, practices or solicitations, or any combination thereof, declared to be unlawful by this chapter.

4. The court in its discretion, may enter an order of restitution, payable to the state, as may be necessary to restore to any person who has suffered any ascertainable loss, including but not limited to, any moneys or property, real or personal which may have been acquired by means of any method, act, use, practice or solicitation, or any combination thereof, declared to be unlawful by this chapter. It shall be the duty of the attorney general to distribute such funds to those persons injured.

5. The court, in its discretion, may appoint a receiver to insure the conformance to any orders issued under subsection 3 of this section or to insure the payment of any damages ordered under subsection 4 of this section.

6. The court may award to the state a civil penalty of not more than one thousand dollars per violation; except that, if the person who would be liable for such penalty shows, by a preponderance of the evidence that a violation resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adopted to avoid the error, no civil penalties shall be imposed.

7. Any action under this section may be brought in the county in which the defendant resides where the violation alleged to have been committed occurred, or where the defendant has his principal place of business.

(t) 15 CSR §60-8.020 defines "unfair practice" as follows:

1. An unfair practice is any practice which

(A) Either --

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions;
2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers; and

(u) By the acts, practices and conduct of Defendant IGC described above it has engaged in the use of misrepresentation, unfair practices and concealment, suppression and omission of material fact in the marketing, advertising, promotion, offering and sale of merchandise, to wit: casino gambling services, in trade or commerce in the State of Missouri. The Court finds that Plaintiff has established 22 separate and distinct violations of the Act.

(v) Through the acts, practices and conduct described above, Defendant IGC has been and continues to be in violation of §407.020, RSMo 1994, and therefore this Permanent Injunction and Final Judgment is warranted and justified pursuant to §407.100, RSMo 1994.

Based on the above evidence and findings IT IS THEREFORE ORDERED ADJUDGED AND DECREED as follows:

I. General

1. Jurisdiction. The Court has subject matter jurisdiction over this action and this action and has personal jurisdiction over the parties hereto. The Court is empowered to enter this Permanent Injunction and Final Judgment pursuant to §407.100, RSMo 1994.

Based on the above evidence and findings IT IS THEREFORE ORDERED, ADJUDGED AND DECREED as follows:

I. General

1. Jurisdiction. The Court has subject matter jurisdiction over this action and this action and has personal jurisdiction over the parties hereto. The Court is empowered to enter this Permanent Injunction and Final Judgment pursuant to §407.100 MSMo 1994.

2. Jurisdiction Retained Jurisdiction is retained for the purpose of enabling any party to this Injunction to apply to the Court at any time for purpose of enforcement of the provisions herein or for the punishment of a violation of this order pursuant to the provisions of §407.110, RSMo 1994 and to fully adjudicate the merits of this cause of action.

3. Severability. If any provision or provisions of this Permanent Injunction is or are declared invalid by a court of competent jurisdiction, the remainder of this Permanent Injunction shall remain in full force and effect and shall not be affected by such declaration.

II. Notice to Employees

Notice. Immediately upon the entry of this Permanent Injunction, Defendant IGC shall provide a copy of this Permanent Injunction to all present and future officers, directors, employees attorneys, representatives, agents, assigns and persons or entities who are acting on behalf of or in concert with the Defendant IGC or any and all of its subsidiaries, including but not limited to Intersphere Communications, Ltd. (Greneda), Intersphere Communications, Ltd., and Global Casinos, Ltd.

III. Injunctive Relief

IT IS THEREFORE ORDERED that Defendant IGC, its successors or assigns, agents, subsidiaries, officers, directors, attorneys, servants and employees, and all those persons and/or entities in active concert or participation with it and all persons or entities having actual notice of this Injunction are
hereby enjoined and prohibited from:

1. Marketing, advertising, offering, and/or promoting by any oral, graphic or pictorial statement, including e-mail, notices, direct mail, brochures, pamphlets, handbills, letters, in or into the State of Missouri and through any conversations with Missouri residents, the opportunity for Missouri residents to participate in any form of casino gambling as that term is defined by §572.010(4), RSMo 1994;

2. Representing in any way by any means that the casino gambling services marketed, advertised, offered, sold and/or promoted by IGC and consumers' participation therein are legal in the State of Missouri; and

3. Concealing, suppressing and omitting the fact that the casino gambling services marketed, advertised, offered, sold and/or promoted by IGC and consumers' participation therein are illegal in the State of Missouri.

IT IS FURTHER ORDERED, ADJUDGED AND DECREED that Defendant IGC, its successors or assigns, agents, subsidiaries, officers, directors, attorneys, servants and employees, and all those persons and/or entities in active concert or participation with it in order to accomplish the provisions of paragraph III. l. above are required and ordered to take actions including but not limited to the following:

A. Immediately reject and refuse all applications from residents of the State of Missouri to participate in online casino gambling through its Global Casino or any other entity by whatever means necessary including, but not limited to, programming its software to perform a validity check for the state of residence of each applicant such that, immediately upon receipt of an online application from a Missouri resident, Defendant IGC will automatically and electronically transmit a message to that resident to be received on the resident's computer and viewable on his or her computer screen notifying that resident of the rejection of his or her application. Said computer or "online" notice shall followed in no more than 2 working days by written notice mailed from Defendant IGC to the Missouri resident notifying the resident of the rejection of his or her application. The written notice shall state without elaboration that the resident's application was rejected pursuant to a Permanent Injunction entered on May 22, 1997, by the Jackson County Circuit Court in Kansas City, MO which prohibits IGC from accepting applications for casino gambling from Missouri residents. A copy of the written notice shall be mailed to the Missouri Attorney General's Office, 3100 Broadway, Kansas City, MO 64111 on the same day it is mailed to the Missouri resident. A copy of the written notice shall be maintained by Defendant IGC at all times. Evidence of the computerized application and rejection transaction shall also be maintained by Defendant IGC at all times in original electronic form. If application are received by IGC or subsidiaries from Missouri residents by some means other than computer transmission, the written notice identified above shall be sent by Defendant IGC to the Missouri resident by express mail on the day the application is received, along with the original application. A copy of said written notice and the application shall be sent by regular mail on that day to the Missouri Attorney General's Office at the above address. Defendant IGC shall maintain copies of all such application and notices at all times.

B. Electronically record and correlate by whatever means necessary, including but not limited to reprogramming its software, the Internet Protocol ("IP") address of each user who applies to he Global Casino by online application and the application.

C. Reject and refuse to open any accounts for residents of the State of Missouri and reject and refuse any funds in any form sent to and received by Defendant IGC or any of its subsidiaries from Missouri residents for the purpose of participating in online casino gambling through IGC's Global Casino or any other entity. Upon receipt of any funds from a Missouri resident, Defendant IGC and its subsidiaries shall return said funds to the resident with a copy of the written notice identified in paragraph A. Above. A copy of the written notice shall be sent to the Missouri Attorney General's Office as provided above and a copy shall be maintained by Defendant IGC as provided above. All funds sent to IGC or subsidiaries by Missouri residents currently in the possession of IGC or its subsidiaries are to be returned immediately to the Missouri residents.
D. Post a prominent notice on the homepage, as well as all pages pertaining to or referencing the application and/or process for applying to Defendant IGC's casino gambling services at http://www.gamblenet.com/main.html (or any other domain name identifying IGC's website,) stating, without elaboration, that IGC and Global Casino are prohibited by a Permanent Injunction entered on May 22, 1997, by the Jackson county Circuit Court in Kansas City, MO, from accepting applications or funds from any Missouri resident to participate in any of the casino gambling activities offered by IGC and that all applications received from Missouri residents will be immediately rejected and any funds received will be immediately returned.

IT IS FURTHER ORDERED, ADJUDGED AND DECREE that Defendant IGC, its successor or assigns, agents, subsidiaries, officers, directors, attorneys, servants and employees, and all those person and/or entities in active concert or participation with it in order to ensure compliance by Defendant IGC with the provisions of this injunction, are required and ordered to:

Provide complete access to all records, documents, files, folders, user files and/or any information whatsoever, whether maintained in hard copy form; by computer through software, program, direct access storage device or any other means; or by any means whatsoever, in any geographic location, belonging to or in the control of Defendant IGC or its subsidiaries, to an independent entity chosen by the Missouri Attorney General's Office to enable that entity to perform periodic audits of Defendant IGC's compliance with the provisions of this Injunction. No advance notice of such audits will be given to Defendant IGC or its subsidiaries. The nature and amount of information necessary to perform these audits to which Defendant IGC shall provide access shall be at the sole designation and discretion of the independent entity. All costs and expenses associated with these audits incurred by the entity shall be borne by and shall be the sole responsibility of Defendant IGC. The entity chosen by the Missouri Attorney General's Office shall prepare a written report memorializing the findings of each audit and shall provide said report to the Missouri Attorney General's Office and to Defendant IGC within 3 working days of the completion of the audit. The Missouri Attorney General's Office may obtain an oral report of the entity's findings by telephoning the entity upon completion of the audit. Any failure to comply with any provision of this Injunction found by he independent entity shall be prima facia evidence of a violation of this Injunction.

IV. Other Relief

The Court finds from the evidence presented by Plaintiff that, in addition to the other relief granted by the Court in Section III., above, plaintiff has shown its entitlement to other relief under Chapter 407, RSMo 1994. Accordingly, FINAL JUDGMENT IS HEREBY ENTERED IN FAVOR OF PLAINTIFF AND AGAINST DEFENDANT IN THE FOLLOWING FURTHER RESPECTS:

1. Pursuant to §407.100.6, the Court awards plaintiff the sum of $1,000.00 per violation by defendant of the Missouri Merchandising Practices Act as shown by Plaintiff for a total of $22,000.00 in civil penalties to be paid by Defendant pursuant to that section.

2. The Court further orders Defendant to make payment to the state in the amount of $10,000.00 for credit to the Merchandising Practices Revolving Fund pursuant to §407.140, RSMo 1994.

3. The Court further orders Defendant to make payment to the State of its costs of investigation and prosecution of this action to enforce the provisions of Chapter 407 in the amount of $34,050.00

Upon proof by Plaintiff of a violation by Defendant IGC of any of the terms or conditions of this Permanent Injunction, the Court shall assess civil penalties of not more than Five Thousand Dollars ($5,000) per violation pursuant to §407.110, RSMo 1994; and/or shall enter an order finding Defendant IGC in civil or criminal contempt, and/or shall enter an order awarding Plaintiff appropriate costs including reasonable attorneys' fees, and/or shall order such other relief as the Court deems appropriate. Furthermore, if Plaintiff believes Defendant IGC has violated any provision of this Permanent Injunction, the Attorney General is not constrained from initiating any further investigations for legal proceedings against Defendant, including those procedures set out in §407.020 et seq., RSMo 1994.
(Slip Opinion: 521 U.S.)

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See United States v. Detroit Timber & Lumber Co., 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al.

v.

AMERICAN CIVIL LIBERTIES UNION et al.

On appeal from the United States District Court for the Eastern District of Pennsylvania

No. 96–511.
Argued March 19, 1997—
Decided June 26, 1997

Two provisions of the Communications Decency Act of 1996 (CDA or Act) seek to protect minors from harmful material on the Internet, an international network of interconnected computers that enables millions of people to communicate with one another in "cyberspace" and to access vast amounts of information from around the world. Title 47 U. S. C. A. §223(a)(1)(B)(ii) (Supp. 1997) criminalizes the "knowing" transmission of "obscene or indecent" messages to any recipient under 18 years of age. Section 223(d) prohibits the "knowing" sending or displaying to a person under 18 of any message "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Affirmative defenses are provided for those who take "good faith... effective... actions" to restrict access by minors to the prohibited communications, §223(e)(5)(A), and those who restrict such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number, §223(e)(5)(B). A number of plaintiffs filed suit challenging the constitutionality of §§223(a)(1) and 223(d). After making extensive findings of fact, a three-judge District Court convened pursuant to the Act entered a preliminary injunction against enforcement of both challenged provisions. The court's judgment enjoins the Government from enforcing §223(a)(1)(B)'s prohibitions insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of §223(d) is unqualified because that section contains no separate reference to obscenity or child pornography. The Government appealed to this Court under the Act's special review provisions, arguing that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague.

Held: The CDA's "indecent transmission" and "patently offensive display" provisions abridge "the freedom of speech" protected by the First Amendment. Pp. 17–40.

(a) Although the CDA's vagueness is relevant to the First Amendment overbreadth inquiry, the judgment should be affirmed without reaching the Fifth Amendment issue. P. 17.

(b) A close look at the precedents relied on by the Government—Ginsberg v. New York, 390 U. S. 629; FCC v. Pacifica Foundation, 438 U. S. 726; and Renton v. Playtime Theatres, Inc., 475 U. S. 41—raises, rather than relieves, doubts about the CDA's constitutionality. The CDA differs from the various laws and orders upheld in those cases in many ways, including that it does not allow parents to consent to their children's use of restricted materials; is not limited to commercial transactions; fails to provide any definition of "indecent" and omits any requirement that "patently offensive" material lack
provide any definition of "indecent" and omits any requirement that "patently offensive" material lack socially redeeming value; neither limits its broad categorical prohibitions to particular times nor bases them on an evaluation by an agency familiar with the medium's unique characteristics; is punitive; applies to a medium that, unlike radio, receives full First Amendment protection; and cannot be properly analyzed as a form of time, place, and manner regulation because it is a content-based blanket restriction on speech. These precedents, then, do not require the Court to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions. Pp. 17–21.

(c) The special factors recognized in some of the Court's cases as justifying regulation of the broadcast media—the history of extensive government regulation of broadcasting, see, e.g., *Red Lion Broadcasting Co. v. FCC*, 395 U. S. 367, 399–400; the scarcity of available frequencies at its inception, see, e.g., *Turner Broadcasting System, Inc. v. FCC*, 512 U. S. 622, 637–638; and its "invasive" nature, see *Sable Communications of Cal., Inc. v. FCC*, 492 U. S. 115, 128—are not present in cyberspace. Thus, these cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to the Internet. Pp. 22–24.

(d) Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for First Amendment purposes. For instance, the use of the undefined terms "indecent" and "patently offensive" will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean. The vagueness of such a content-based regulation, see, e.g., *Gentile v. State Bar of Nev.*, 501 U. S. 1030, coupled with its increased deterrent effect as a criminal statute, see, e.g., *Dombrowski v. Pfister*, 380 U. S. 479, raise special First Amendment concerns because of its obvious chilling effect on free speech. Contrary to the Government's argument, the CDA is not saved from vagueness by the fact that its "patently offensive" standard repeats the second part of the three-prong obscenity test set forth in *Miller v. California*, 413 U. S. 15, 24. The second *Miller* prong reduces the inherent vagueness of its own "patently offensive" term by requiring that the proscribed material be "specifically defined by the applicable state law." In addition, the CDA applies only to "sexual conduct," whereas, the CDA prohibition extends also to "excretory activities" and "organs" of both a sexual and excretory nature. Each of *Miller* 's other two prongs also critically limits the uncertain sweep of the obscenity definition. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing alone, is not vague. The CDA's vagueness undermines the likelihood that it has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials. Pp. 24–28.

(e) The CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. Although the Government has an interest in protecting children from potentially harmful materials, see, e.g., *Ginsberg*, 390 U. S., at 639, the CDA pursues that interest by suppressing a large amount of speech that adults have a constitutional right to send and receive, see, e.g., *Sable*, supra, at 126. Its breadth is wholly unprecedented. The CDA's burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the Act's legitimate purposes. See, e.g., *Sable*, 492 U. S., at 126. The Government has not proved otherwise. On the other hand, the District Court found that currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing material which the parents believe is inappropriate will soon be widely available. Moreover, the arguments in this Court referred to possible alternatives such as requiring that indecent material be "tagged" to facilitate parental control, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet differently than others. Particularly in the light of the absence of any detailed congressional findings, or even hearings addressing the CDA's special problems, the Court is persuaded that the CDA is not narrowly tailored. Pp. 28–33.

(f) The Government's three additional arguments for sustaining the CDA's affirmative prohibitions are rejected. First, the contention that the Act is constitutional because it leaves open ample "alternative channels" of communication is unpersuasive because the CDA regulates speech on the basis of its content, so that a "time, place, and manner" analysis is inapplicable. See, e.g., *Consolidated Edison Co. of N. Y. v. Public Serv. Comm'n of N. Y.*, 447 U. S. 530, 536. Second, the assertion that the CDA's "knowledge" and "specific person" requirements significantly restrict its permissible application to communications to persons the sender knows to be under 18 is untenable, given that most Internet
forums are open to all comers and that even the strongest reading of the "specific person" requirement would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech. Finally, there is no textual support for the submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA's prohibitions. Pp. 33–35.

(g) The §223(e)(5) defenses do not constitute the sort of "narrow tailoring" that would save the CDA. The Government's argument that transmitters may take protective "good faith actio[n]" by "tagging" their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software, is illusory, given the requirement that such action be "effective": The proposed screening software does not currently exist, but, even if it did, there would be no way of knowing whether a potential recipient would actually block the encoded material. The Government also failed to prove that §223(b)(5)'s verification defense would significantly reduce the CDA's heavy burden on adult speech. Although such verification is actually being used by some commercial providers of sexually explicit material, the District Court's findings indicate that it is not economically feasible for most noncommercial speakers. Pp. 35–37.

(h) The Government's argument that this Court should preserve the CDA's constitutionality by honoring its severability clause, §608, and by construing nonseverable terms narrowly, is acceptable in only one respect. Because obscene speech may be banned totally, see Miller, supra, at 18, and §223(a)'s restriction of "obscene" material enjoys a textual manifestation separate from that for "indecent" material, the Court can sever the term "or indecent" from the statute, leaving the rest of §223(a) standing. Pp. 37–39.

(i) The Government's argument that its "significant" interest in fostering the Internet's growth provides an independent basis for upholding the CDA's constitutionality is singularly unpersuasive. The dramatic expansion of this new forum contradicts the factual basis underlying this contention: that the unregulated availability of "indecent" and "patently offensive" material is driving people away from the Internet. P. 40.

929 F. Supp. 824, affirmed.

Stevens, J., delivered the opinion of the Court, in which Scalia, Kennedy, Souter, Thomas, Ginsburg, and Breyer, J., joined. O'Connor, J., filed an opinion concurring in the judgment in part and dissenting in part, in which Rehnquist, C. J., joined.

NOTICE: This opinion is subject to formal revision before publication in the preliminary print of the United States Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D.C. 20543, of any typographical or other formal errors, in order that corrections may be made before the preliminary print goes to press.

SUPREME COURT OF THE UNITED STATES

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al.,
APPELLANTS

v.

AMERICAN CIVIL LIBERTIES UNION et al.
APPELLEES

No. 96–511

On appeal from the United States District Court for the Eastern District of Pennsylvania
[June 26, 1997]

Justice Stevens delivered the opinion of the Court.

At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the legitimacy and importance of the congressional goal of protecting children from harmful materials, we agree with the three-judge District Court that the statute abridges "the freedom of speech" protected by the First Amendment.[1]

I

The District Court made extensive findings of fact, most of which were based on a detailed stipulation prepared by the parties. See 929 F. Supp. 824, 830–849 (ED Pa. 1996).[2] The findings describe the character and the dimensions of the Internet, the availability of sexually explicit material in that medium, and the problems confronting age verification for recipients of Internet communications. Because those findings provide the underpinnings for the legal issues, we begin with a summary of the undisputed facts.

The Internet

The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET;"[3] which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."[4]

The Internet has experienced "extraordinary growth."[5] The number of "host" computers—those that store information and relay communications—increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listervs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addresses. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some
waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects."[6] It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."[7]

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address—"rather like a telephone number."[8] Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text—sometimes images.

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals.[9] Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web."[10]

**Sexually Explicit Material**

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest-core."[11] These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community."[12] Thus, for example, "when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe 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, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague."[13]

Some of the communications over the Internet that originate in foreign countries are also sexually
explicit.[14] Though such material is widely available, users seldom encounter such content accidentally. "A document's title or a description of the document will usually appear before the document itself . . . and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content."[15] For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident.[16] Unlike communications received by radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended."[17]

Systems have been developed to help parents control the material that may be available on a home computer with Internet access. A system may either limit a computer's access to an approved list of sources that have been identified as containing no adult material, it may block designated inappropriate sites, or it may attempt to block messages containing identifiable objectionable features. "Although parental control software currently can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images."[18] Nevertheless, the evidence indicates that "a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be available."[19]

**Age Verification**

The problem of age verification differs for different uses of the Internet. The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms."[20] The Government offered no evidence that there was a reliable way to screen recipients and participants in such fora for age. Moreover, even if it were technologically feasible to block minors' access to newsgroups and chat rooms containing discussions of art, politics or other subjects that potentially elicit "indecent" or "patently offensive" contributions, it would not be possible to block their access to that material and "still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent."[21]

Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card number or an adult password. Credit card verification is only feasible, however, either in connection with a commercial transaction in which the card is used, or by payment to a verification agency. Using credit card possession as a surrogate for proof of age would impose costs on non-commercial Web sites that would require many of them to shut down. For that reason, at the time of the trial, credit card verification was "effectively unavailable to a substantial number of Internet content providers." Id., at 846 (finding 102). Moreover, the imposition of such a requirement "would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material."[22]

Commercial pornographic sites that charge their users for access have assigned them passwords as a method of age verification. The record does not contain any evidence concerning the reliability of these technologies. Even if passwords are effective for commercial purveyors of indecent material, the District Court found that an adult password requirement would impose significant burdens on noncommercial sites, both because they would discourage users from accessing their sites and because the cost of creating and maintaining such screening systems would be "beyond their reach."[23]

In sum, the District Court found:

"Even if credit card verification or adult password verification were implemented, the Government presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18. The burdens imposed by credit card verification and adult password verification systems make them effectively unavailable to a
substantial number of Internet content providers." *Ibid.* (finding 107).

II

The Telecommunications Act of 1996, Pub. L. 104–104, 110 Stat. 56, was an unusually important legislative enactment. As stated on the first of its 103 pages, its primary purpose was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies." The major components of the statute have nothing to do with the Internet; they were designed to promote competition in the local telephone service market, the multichannel video market, and the market for over-the-air broadcasting. The Act includes seven Titles, six of which are the product of extensive committee hearings and the subject of discussion in Reports prepared by Committees of the Senate and the House of Representatives. By contrast, Title V—known as the "Communications Decency Act of 1996" (CDA)—contains provisions that were either added in executive committee after the hearings were concluded or as amendments offered during floor debate on the legislation. An amendment offered in the Senate was the source of the two statutory provisions challenged in this case.[24] They are informally described as the "indecent transmission" provision and the "patently offensive display" provision.[25]

The first, 47 U. S. C. A. §223(a) (Supp. 1997), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

"(a) Whoever—

"(1) in interstate or foreign communications—

..."

"(B) by means of a telecommunications device knowingly—

"(i) makes, creates, or solicits, and

"(ii) initiates the transmission of,

"any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication; stating..."

"(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,"

"shall be fined under Title 18, or imprisoned not more than two years, or both."

The second provision, §223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

"(d) Whoever—

"(1) in interstate or foreign communications knowingly—

"(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

"(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

"any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary
context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

"(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

"shall be fined under Title 18, or imprisoned not more than two years, or both."

The breadth of these prohibitions is qualified by two affirmative defenses. See §223(e)(5).[26] One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. §223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. §223(e)(5)(B).

III

On February 8, 1996, immediately after the President signed the statute, 20 plaintiffs[27] filed suit against the Attorney General of the United States and the Department of Justice challenging the constitutionality of §§223(a)(1) and 223(d). A week later, based on his conclusion that the term "indecent" was too vague to provide the basis for a criminal prosecution, District Judge Buckwalter entered a temporary restraining order against enforcement of §§223(a)(1)(B)(ii) insofar as it applies to indecent communications. A second suit was then filed by 27 additional plaintiffs,[28] the two cases were consolidated, and a three-judge District Court was convened pursuant to §561 of the Act.[29] After an evidentiary hearing, that Court entered a preliminary injunction against enforcement of both of the challenged provisions. Each of the three judges wrote a separate opinion, but their judgment was unanimous.

Chief Judge Sloviter doubted the strength of the Government's interest in regulating "the vast range of online material covered or potentially covered by the CDA," but acknowledged that the interest was "compelling" with respect to some of that material. 929 F. Supp., at 853. She concluded, nonetheless, that the statute "sweeps more broadly than necessary and thereby chills the expression of adults" and that the terms "patently offensive" and "indecent" were "inherently vague." Id., at 854. She also determined that the affirmative defenses were not "technologically or economically feasible for most providers," specifically considering and rejecting an argument that providers could avoid liability by "tagging" their material in a manner that would allow potential readers to screen out unwanted transmissions. Id., at 856. Chief Judge Sloviter also rejected the Government's suggestion that the scope of the statute could be narrowed by construing it to apply only to commercial pornographers. Id., at 854–855.

Judge Buckwalter concluded that the word "indecent" in §223(a)(1)(B) and the terms "patently offensive" and "in context" in §223(d) were so vague that criminal enforcement of either section would violate the "fundamental constitutional principle" of "simple fairness," id., at 861, and the specific protections of the First and Fifth Amendments, id., at 858. He found no statutory basis for the Government's argument that the challenged provisions would be applied only to "pornographic" materials, noting that, unlike obscenity, "indecency has not been defined to exclude works of serious literary, artistic, political or scientific value." Id., at 863. Moreover, the Government's claim that the work must be considered patently offensive "in context" was itself vague because the relevant context might "refer to, among other things, the nature of the communication as a whole, the time of day it was conveyed, the medium used, the identity of the speaker, or whether or not it is accompanied by appropriate warnings." Id., at 864. He believed that the unique nature of the Internet aggravated the vagueness of the statute. Id., at 865, n. 9.

Judge Dalzell's review of "the special attributes of Internet communication" disclosed by the evidence convinced him that the First Amendment denies Congress the power to regulate the content of protected speech on the Internet. Id., at 867. His opinion explained at length why he believed the Act would abridge significant protected speech, particularly by noncommercial speakers, while "[p]erversely, commercial pornographers would remain relatively unaffected." Id., at 879. He construed our cases as
requiring a "medium-specific" approach to the analysis of the regulation of mass communication, id., at 873, and concluded that the Internet—as "the most participatory form of mass speech yet developed," id., at 883—is entitled to "the highest protection from governmental intrusion," ibid.[30]

The judgment of the District Court enjoins the Government from enforcing the prohibitions in §223(a)(1)(B) insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of §§223(d)(1) and (2) is unqualified because those provisions contain no separate reference to obscenity or child pornography.

The Government appealed under the Act's special review provisions, §561, 110 Stat. 142–143, and we noted probable jurisdiction, see 519 U. S. ___ (1996). In its appeal, the Government argues that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague. While we discuss the vagueness of the CDA because of its relevance to the First Amendment overbreadth inquiry, we conclude that the judgment should be affirmed without reaching the Fifth Amendment issue. We begin our analysis by reviewing the principal authorities on which the Government relies. Then, after describing the overbreadth of the CDA, we consider the Government's specific contentions, including its submission that we save portions of the statute either by severance or by fashioning judicial limitations on the scope of its coverage.

IV

In arguing for reversal, the Government contends that the CDA is plainly constitutional under three of our prior decisions: (1) Ginsberg v. New York, 390 U. S. 629 (1968); (2) FCC v. Pacifica Foundation, 438 U. S. 726 (1978); and (3) Renton v. Playtime Theatres, Inc., 475 U. S. 41 (1986). A close look at these cases, however, raises—rather than relieves—doubts concerning the constitutionality of the CDA.

In Ginsberg, we upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene as to them even if not obscene as to adults. We rejected the defendant's broad submission that "the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor." 390 U. S., at 636. In rejecting that contention, we relied not only on the State's independent interest in the well-being of its youth, but also on our consistent recognition of the principle that "the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society."[31] In four important respects, the statute upheld in Ginsberg was narrower than the CDA. First, we noted in Ginsberg that "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children." Id., at 639. Under the CDA, by contrast, neither the parents' consent—nor even their participation—in the communication would avoid the application of the statute.[32] Second, the New York statute applied only to commercial transactions, id., at 647, whereas the CDA contains no such limitation. Third, the New York statute cabined its definition of material that is harmful to minors with the requirement that it be "utterly without redeeming social importance for minors." Id., at 646. The CDA fails to provide us with any definition of the term "indecent" as used in §223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by §223(d) lack serious literary, artistic, political, or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, in applying to all those under 18 years, includes an additional year of those nearest majority.

In Pacifica, we upheld a declaratory order of the Federal Communications Commission, holding that the broadcast of a recording of a 12-minute monologue entitled "Filthy Words" that had previously been delivered to a live audience "could have been the subject of administrative sanctions." 438 U. S., at 730 (internal quotations omitted). The Commission had found that the repetitive use of certain words referring to excretory or sexual activities or organs "in an afternoon broadcast when children are in the audience was patently offensive" and concluded that the monologue was indecent "as broadcast." Id., at 735. The respondent did not quarrel with the finding that the afternoon broadcast was patently offensive, but contended that it was not "indecent" within the meaning of the relevant statutes because it contained no prurient appeal. After rejecting respondent's statutory arguments, we confronted its two constitutional arguments: (1) that the Commission's construction of its authority to ban indecent speech was so broad
that its order had to be set aside even if the broadcast at issue was unprotected; and (2) that since the recording was not obscene, the First Amendment forbade any abridgment of the right to broadcast it on the radio.

In the portion of the lead opinion not joined by Justices Powell and Blackmun, the plurality stated that the First Amendment does not prohibit all governmental regulation that depends on the content of speech. Id., at 742–743. Accordingly, the availability of constitutional protection for a vulgar and offensive monologue that was not obscene depended on the context of the broadcast. Id., at 744–748. Relying on the premise that "of all forms of communication" broadcasting had received the most limited First Amendment protection, id., at 748–749, the Court concluded that the ease with which children may obtain access to broadcasts, "coupled with the concerns recognized in Ginsberg," justified special treatment of indecent broadcasting. Id., at 749–750.

As with the New York statute at issue in Ginsberg, there are significant differences between the order upheld in Pacifica and the CDA. First, the order in Pacifica, issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when—rather than whether—it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet. Second, unlike the CDA, the Commission's declaratory order was not punitive; we expressly refused to decide whether the indecent broadcast "would justify a criminal prosecution." Id., at 750. Finally, the Commission's order applied to a medium which as a matter of history had "received the most limited First Amendment protection," id., at 748, in large part be cause warnings could not adequately protect the listener from unexpected program content. The Internet, however, has no comparable history. Moreover, the District Court found that the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material.

In Renton, we upheld a zoning ordinance that kept adult movie theatres out of residential neighborhoods. The ordinance was aimed, not at the content of the films shown in the theaters, but rather at the "secondary effects"—such as crime and deteriorating property values—that these theaters fostered: "It is the [e] secondary effect which these zoning ordinances attempt to avoid, not the dissemination of "offensive" speech." 475 U. S., at 49 (quoting Young v. American Mini Theatres, Inc., 427 U. S. 50, 71, n. 34 (1976)). According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content-based blanket restriction on speech, and, as such, cannot be "properly analyzed as a form of time, place, and manner regulation." 475 U. S., at 46. See also Boos v. Barry, 485 U. S. 312, 321 (1988) ("Regulations that focus on the direct impact of speech on its audience" are not properly analyzed under Renton); Forsyth County v. Nationalist Movement, 505 U. S. 123, 134 (1992) ("Listeners' reaction to speech is not a content-neutral basis for regulation").

These precedents, then, surely do not require us to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

V

In Southeastern Promotions, Ltd. v. Conrad, 420 U. S. 546, 557 (1975), we observed that "[e]ach medium of expression . . . may present its own problems." Thus, some of our cases have recognized special justifications for regulation of the broadcast media that are not applicable to other speakers, see Red Lion Broadcasting Co. v. FCC, 395 U. S. 367 (1969); FCC v. Pacifica Foundation, 438 U. S. 726 (1978). In these cases, the Court relied on the history of extensive government regulation of the broadcast medium, see, e.g., Red Lion, 395 U. S., at 399–400; the scarcity of available frequencies at its inception, see, e.g., Turner Broadcasting System, Inc. v. FCC, 512 U. S. 622, 637–638 (1994); and its "invasive" nature, see Sable Communications of Cal., Inc. v. FCC, 492 U. S. 115, 128 (1989).

Those factors are not present in cyberspace. Neither before nor after the enactment of the CDA have the
Those factors are not present in cyberspace. Neither before nor after the enactment of the CDA have the vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry.\[33\] Moreover, the Internet is not as "invasive" as radio or television. The District Court specifically found that "[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'" 929 F. Supp., at 844 (finding 88). It also found that "[a]lmost all sexually explicit images are preceded by warnings as to the content," and cited testimony that "'odds are slim' that a user would come across a sexually explicit sight by accident." \textit{Ibid.}

We distinguished \textit{Pacifica} in \textit{Sable}, 492 U. S., at 128, on just this basis. In \textit{Sable}, a company engaged in the business of offering sexually oriented prerecorded telephone messages (popularly known as "dial-a-porn") challenged the constitutionality of an amendment to the Communications Act that imposed a blanket prohibition on indecent as well as obscene interstate commercial telephone messages. We held that the statute was constitutional insofar as it applied to obscene messages but invalid as applied to indecent messages. In attempting to justify the complete ban and criminalization of indecent commercial telephone messages, the Government relied on \textit{Pacifica}, arguing that the ban was necessary to prevent children from gaining access to such messages. We agreed that "there is a compelling interest in protecting the physical and psychological well-being of minors" which extended to shielding them from indecent messages that are not obscene by adult standards, 492 U. S., at 126, but distinguished our "emphatically narrow holding" in \textit{Pacifica} because it did not involve a complete ban and because it involved a different medium of communication, \textit{id.}, at 127. We explained that "the dial-it medium requires the listener to take affirmative steps to receive the communication." \textit{Id.}, at 127–128. "Placing a telephone call," we continued, "is not the same as turning on a radio and being taken by surprise by an indecent message." \textit{Id.}, at 128.

Finally, unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds. The Government estimates that "[a]s many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999."\[34\] This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought." 929 F. Supp., at 842 (finding 74). We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

VI

Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," 47 U. S. C. A. §223(a) (Supp. 1997), while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." §223(d). Given the absence of a definition of either term,\[35\] this difference in language will provoke uncertainty among speakers about how the two standards relate to each other\[36\] and just what they mean.\[37\] Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our \textit{Pacifica} opinion, or the consequences of prison rape would not violate the CDA? This uncertainty undermines the likelihood that the CDA has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials.

The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. \textit{See}, \textit{e.g.}, \textit{Gentile v. State Bar of Nev.}, 501 U. S. 1030, 1048–1051 (1991). Second, the CDA is a criminal statute. In addition to the opprobrium and stigma of a criminal conviction, the CDA threatens violators with penalties including up to two years in
prison for each act of violation. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. See, e.g., Dombrowski v. Pfister, 380 U. S. 479, 494 (1965). As a practical matter, this increased deterrent effect, coupled with the "risk of discriminatory enforcement" of vague regulations, poses greater First Amendment concerns than those implicated by the civil regulation reviewed in Denver Area Ed. Telecommunications Consortium, Inc. v. FCC, 518 U. S. ___ (1996).

The Government argues that the statute is no more vague than the obscenity standard this Court established in Miller v. California, 413 U. S. 15 (1973). But that is not so. In Miller, this Court reviewed a criminal conviction against a commercial vendor who mailed brochures containing pictures of sexually explicit activities to individuals who had not requested such materials. Id., at 18. Having struggled for some time to establish a definition of obscenity, we set forth in Miller the test for obscenity that controls to this day:

"(a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." Id., at 24 (internal quotation marks and citations omitted).

Because the CDA's "patently offensive" standard (and, we assume arguendo, its synonymous "indecent" standard) is one part of the three-prong Miller test, the Government reasons, it cannot be unconstitutionally vague.

The Government's assertion is incorrect as a matter of fact. The second prong of the Miller test—the purportedly analogous standard—contains a critical requirement that is omitted from the CDA: that the proscribed material be "specifically defined by the applicable state law." This requirement reduces the vagueness inherent in the open-ended term "patently offensive" as used in the CDA. Moreover, the Miller definition is limited to "sexual conduct," whereas the CDA extends also to include (1) "excretory activities" as well as (2) "organs" of both a sexual and excretory nature.

The Government's reasoning is also flawed. Just because a definition including three limitations is not vague, it does not follow that all of those limitations, standing by itself, is not vague. Each of Miller's additional two prongs—(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lack[] serious literary, artistic, political, or scientific value"—critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary community standards. See Pope v. Illinois, 481 U. S. 497, 500 (1987). This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value. The Government's contention that courts will be able to give such legal limitations to the CDA's standards is belied by Miller's own rationale for having juries determine whether material is "patently offensive" according to community standards: that such questions are essentially ones of fact.

In contrast to Miller and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

VII

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would
address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

In evaluating the free speech rights of adults, we have made it perfectly clear that "[s]exual expression which is indecent but not obscene is protected by the First Amendment." Sable, 492 U. S., at 126. See also Carey v. Population Services Int'l, 431 U. S. 678, 701 (1977) ("[W]here obscenity is not involved, we have consistently held that the fact that protected speech may be offensive to some does not justify its suppression"). Indeed, Pacifica itself admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it." 438 U. S., at 745.

It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. See Ginsberg, 390 U. S., at 639; Pacifica, 438 U. S., at 749. But that interest does not justify an unnecessarily broad suppression of speech addressed to adults. As we have explained, the Government may not "reduce[e] the adult population . . . to . . . only what is fit for children." Denver, 518 U. S., at ___ (slip op., at 29) (internal quotation marks omitted) (quoting Sable, 492 U. S., at 128).[40] "[R]egardless of the strength of the government's interest" in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox." Bolger v. Youngs Drug Products Corp., 463 U. S. 60, 74–75 (1983).

The District Court was correct to conclude that the CDA effectively resembles the ban on "dial-a-porn" invalidated in Sable, 929 F. Supp., at 854. In Sable, 492 U. S., at 129, this Court rejected the argument that we should defer to the congressional judgment that nothing less than a total ban would be effective in preventing enterprising youngsters from gaining access to indecent communications. Sable thus made clear that the mere fact that a statutory regulation of speech was enacted for the important purpose of protecting children from exposure to sexually explicit material does not foreclose inquiry into its validity.[41] As we pointed out last Term, that inquiry embodies an "over-arching commitment" to make sure that Congress has designed its statute to accomplish its purpose "without imposing an unnecessarily great restriction on speech." Denver, 518 U. S., at ___ (slip op., at 11).

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult-to-adult communication. The findings of the District Court make clear that this premise is untenable. Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults.[42]

The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms. 929 F. Supp., at 845 (findings 90–94). As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults. Id., at 845–848 (findings 95–116).[43] These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "[d]espite its limitations, currently available user-based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available." Id., at 842 (finding 73) (emphases added).

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in Ginsberg and Pacifica, the scope of the CDA is not limited to commercial speech or commercial entities. Its open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value.[44] Moreover, the "community standards" criterion as applied to the Internet means that any communication available to a nation-wide audience will be judged by the standards of
the community most likely to be offended by the message.[45] The regulated subject matter includes any of the seven "dirty words" used in the Pacifica monologue, the use of which the Government's expert acknowledged could constitute a felony. See Olsen Test., Tr. Vol. V, 53:16–54:10. It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library.

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and "patently offensive" messages communicated to a 17-year old—no matter how much value the message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute. Under the CDA, a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. See 47 U.S.C. A. §223(a)(2) (Supp. 1997). Similarly, a parent who sent his 17-year-old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

The breadth of this content-based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet—such as commercial web sites—differently than others, such as chat rooms. Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.

VIII

In an attempt to curtail the CDA's facial overbreadth, the Government advances three additional arguments for sustaining the Act's affirmative prohibitions: (1) that the CDA is constitutional because it leaves open ample "alternative channels" of communication; (2) that the plain meaning of the Act's "knowledge" and "specific person" requirement significantly restricts its permissible applications; and (3) that the Act's prohibitions are "almost always" limited to material lacking redeeming social value.

The Government first contends that, even though the CDA effectively censors discourse on many of the Internet's modalities—such as chat groups, newsgroups, and mail explorers—it is nonetheless constitutional because it provides a "reasonable opportunity" for speakers to engage in the restricted speech on the World Wide Web. Brief for Appellants 39. This argument is unpersuasive because the CDA regulates speech on the basis of its content. A "time, place, and manner" analysis is therefore inapplicable. See Consolidated Edison Co. of N. Y. v. Public Serv. Comm'n of N. Y., 447 U.S. 530, 536 (1980). It is thus immaterial whether such speech would be feasible on the Web (which, as the Government's own expert acknowledged, would cost up to $10,000 if the speaker's interests were not accommodated by an existing Web site, not including costs for database management and age verification). The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books. In invalidating a number of laws that banned leafletting on the streets regardless of their content—we explained that "one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised in some other place." Schneider v. State (Town of Irvington), 308 U.S. 147, 163 (1939).

The Government also asserts that the "knowledge" requirement of both §§223(a) and (d), especially when coupled with the "specific child" element found in §223(d), saves the CDA from overbreadth. Because both sections prohibit the dissemination of indecent messages only to persons known to be under 18, the Government argues, it does not require transmitters to "refrain from communicating indecent material to adults; they need only refrain from disseminating such materials to persons they know to be under 18." Brief for Appellants 24. This argument ignores the fact that most Internet
fora—including chat rooms, newsgroups, mail exploders, and the Web—are open to all comers. The Government's assertion that the knowledge requirement somehow protects the communications of adults is therefore untenable. Even the strongest reading of the "specific person" requirement of §223(d) cannot save the statute. It would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech who might simply log on and inform the would-be discussers that his 17-year-old child—a "specific person . . . under 18 years of age," 47 U. S. C. A. §223(d)(1)(A) (Supp. 1997)—would be present.

Finally, we find no textual support for the Government's submission that material having scientific, educational, or other redeeming social value will necessarily fall outside the CDA's "patently offensive" and "indecent" prohibitions. See also n. 37, supra.

IX

The Government's three remaining arguments focus on the defenses provided in §223(e)(5).[46] First, relying on the "good faith, reasonable, effective, and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the Act. The suggestion assumes that transmitters may encode their indecent communications in a way that would indicate their contents, thus permitting recipients to block their reception with appropriate software. It is the requirement that the good faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."

For its second and third arguments concerning defenses—which we can consider together—the Government relies on the latter half of §223(e)(5), which applies when the transmitter has restricted access by requiring use of a verified credit card or adult identification. Such verification is not only technologically available but actually is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense. Under the findings of the District Court, however, it is not economically feasible for most noncommercial speakers to employ such verification. Accordingly, this defense would not significantly narrow the statute's burden on noncommercial speech. Even with respect to the commercial pornographers that would be protected by the defense, the Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults.[47] Given that the risk of criminal sanctions "hovers over each content provider, like the proverbial sword of Damocles,"[48] the District Court correctly refused to rely on unproven future technology to save the statute. The Government thus failed to prove that the proffered defense would significantly reduce the heavy burden on adult speech produced by the prohibition on offensive displays.

We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise patently invalid unconstitutional provision. In Sable, 492 U. S., at 127, we remarked that the speech restriction at issue there amounted to "burn[ing] the house to roast the pig." The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

X

At oral argument, the Government relied heavily on its ultimate fall-back position: If this Court should conclude that the CDA is insufficiently tailored, it urged, we should save the statute's constitutionality by honoring the severability clause, see 47 U. S. C. §608, and construing nonseverable terms narrowly. In only one respect is this argument acceptable.

A severability clause requires textual provisions that can be severed. We will follow §608's guidance by leaving constitutional textual elements of the statute intact in the one place where they are, in fact, severable. The "indecency" provision, 47 U. S. C. A. §223(a) (Supp. 1997), applies to "any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent." (Emphasis added.) Appellees do not challenge the application of the statute to obscene speech, which, they
Appellees do not challenge the application of the statute to obscene speech, which, they acknowledge, can be banned totally because it enjoys no First Amendment protection. See Miller, 413 U. S., at 18. As set forth by the statute, the restriction of "obscene" material enjoys a textual manifestation separate from that for "indecent" material, which we have held unconstitutional. Therefore, we will sever the term "or indecent" from the statute, leaving the rest of §223(a) standing. In no other respect, however, can §223(a) or §223(d) be saved by such a textual surgery.

The Government also draws on an additional, less traditional aspect of the CDA's severability clause, 47 U. S. C., §608, which asks any reviewing court that holds the statute facially unconstitutional not to invalidate the CDA in application to "other persons or circumstances" that might be constitutionally permissible. It further invokes this Court's admonition that, absent "countervailing considerations," a statute should "be declared invalid to the extent it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U. S. 491, 503–504 (1985). There are two flaws in this argument.

First, the statute that grants our jurisdiction for this expedited review, 47 U. S. C. A. §561 (Supp. 1997), limits that jurisdictional grant to actions challenging the CDA "on its face." Consistent with §561, the plaintiffs who brought this suit and the three-judge panel that decided it treated it as a facial challenge. We have no authority, in this particular posture, to convert this litigation into an "as-applied" challenge. Nor, given the vast array of plaintiffs, the range of their expressive activities, and the vagueness of the statute, would it be practicable to limit our holding to a judicially defined set of specific applications.

Second, one of the "countervailing considerations" mentioned in Brockett is present here. In considering a facial challenge, this Court may impose a limiting construction on a statute only if it is "readily susceptible" to such a construction. Virginia v. American Bookseller's Assn., Inc., 484 U. S. 383, 397 (1988). See also Erznoznik v. Jacksonvillle, 422 U. S. 205, 216 (1975) ("readily subject" to narrowing construction). The open-ended character of the CDA provides no guidance what ever for limiting its coverage.

This case is therefore unlike those in which we have construed a statute narrowly because the text or other source of congressional intent identified a clear line that this Court could draw. Cf., e.g., Brockett, 472 U. S., at 504–505 (invalidating obscenity statute only to the extent that word "lust" was actually or effectively excised from statute); United States v. Grace, 461 U. S. 171, 180–183 (1983) (invalidating federal statute banning expressive displays only insofar as it extended to public sidewalks when clear line could be drawn between sidewalks and other grounds that comported with congressional purpose of protecting the building, grounds, and people therein). Rather, our decision in United States v. Treasury Employees, 513 U. S. 454, 479, n. 26 (1995), is applicable. In that case, we declined to "dra[w] one or more lines between categories of speech covered by an overly broad statute, when Congress has sent inconsistent signals as to where the new line or lines should be drawn" because doing so "involves a far more serious invasion of the legislative domain."[49] This Court "will not rewrite a . . . law to conform it to constitutional requirements." American Booksellers, 484 U. S., at 397.[50]

In this Court, though not in the District Court, the Government asserts that—in addition to its interest in protecting children—its "[e]qually significant" interest in fostering the growth of the Internet provides an independent basis for upholding the constitutionality of the CDA. Brief for Appellants 19. The Government apparently assumes that the unregulated availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.

We find this argument singularly unpersuasive. The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.
For the foregoing reasons, the judgment of the district court is affirmed.

It is so ordered.

FOOTNOTES: (opinion)


FN2. The Court made 410 findings, including 356 paragraphs of the parties' stipulation and 54 findings based on evidence received in open court. See 929 F. Supp. at 830, n. 9, 842, n. 15.

FN3. An acronym for the network developed by the Advanced Research Project Agency.

FN4. Id., at 844 (finding 81).

FN5. Id., at 831 (finding 3).

FN6. Id., at 835 (finding 27).

FN7. Id., at 842 (finding 74).

FN8. Id., at 836 (finding 36).

FN9. "Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal 'home pages,' the equivalent of individualized newsletters about the person or organization, which are available to everyone on the Web." Id., at 837 (finding 42).

FN10. Id., at 838 (finding 46).

FN11. Id., at 844 (finding 82).

FN12. Ibid. (finding 86).

FN13. Ibid. (finding 85).


FN15. Id., at 844-845 (finding 88).

FN16. Ibid.

FN17. Id., at 845 (finding 89).

FN18. Id., at 842 (finding 72).

FN19. Ibid. (finding 73).

FN20. Id., at 845 (finding 90): "An e-mail address provides no authoritative information about the addressee, who may use an e-mail 'alias' or an anonymous reailer. There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list."

FN22. *Id.*, at 846 (finding 102).

FN23. *Id.*, at 847 (findings 104–106):

"At least some, if not almost all, non-commercial organizations, such as the ACLU, Stop Prisoner Rape or Critical Path AIDS Project, regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge.

...  

"There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password. Andrew Anker testified that HotWired has received many complaints from its members about HotWired's registration system, which requires only that a member supply a name, e-mail address and self-created password. There is concern by commercial content providers that age verification requirements would decrease advertising and revenue because advertisers depend on a demonstration that the sites are widely available and frequently visited."

FN24. *See* Exon Amendment No. 1268, 141 Cong. Rec. S8120 (June 9, 1995). *See also id.*, at S8087. This amendment, as revised, became §502 of the Communications Act of 1996, 110 Stat. 133, 47 U. S. C. A. §§223(a)–(e) (Supp. 1997). Some Members of the House of Representatives opposed the Exon Amendment because they thought it "possible for our parents now to child-proof the family computer with these products available in the private sector." They also thought the Senate's approach would "involve the Federal Government spending vast sums of money trying to define elusive terms that are going to lead to a flood of legal challenges while our kids are unprotected." These Members offered an amendment intended as a substitute for the Exon Amendment, but instead enacted as an additional section of the Act entitled "Online Family Empowerment." *See* 110 Stat. 137, 47 U. S. C. A. §230 (Supp. 1997); 141 Cong. Rec. H8468–H8472. No hearings were held on the provisions that became law. *See S. Rep. No. 104–23* (1995), p. 9. After the Senate adopted the Exon amendment, however, its Judiciary Committee did conduct a one-day hearing on "Cyberporn and Children." In his opening statement at that hearing, Senator Leahy observed:

"It really struck me in your opening statement when you mentioned, Mr. Chairman, that it is the first ever hearing, and you are absolutely right. And yet we had a major debate on the floor, passed legislation overwhelmingly on a subject involving the Internet, legislation that could dramatically change—some would say even wreak havoc—on the Internet. The Senate went in willy-nilly, passed legislation, and never once had a hearing, never once had a discussion other than an hour or so on the floor." Cyberporn and Children: The Scope of the Problem, The State of the Technology, and the Need for Congressional Action, Hearing on S. 892 before the Senate Committee on the Judiciary, 104th Cong., 1st Sess., 7–8 (1995).

FN25. Although the Government and the dissent break §223(d)(1) into two separate "patently offensive" and "display" provisions, we follow the convention of both parties below, as well the District Court's order and opinion, in describing §223(d)(1) as one provision.

FN26. In full, § 223(e)(5) provides:

"(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) of this section that a person—

"(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such
circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

"(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number."

FN27. American Civil Liberties Union; Human Rights Watch; Electronic Privacy Information Center; Electronic Frontier Foundation; Journalism Education Association; Computer Professionals for Social Responsibility; National Writers Union; Clarinet Communications Corp.; Institute for Global Communications; Stop Prisoner Rape; AIDS Education Global Information System; Bibliobates; Queer Resources Directory; Critical Path AIDS Project, Inc.; Wildcat Press, Inc.; Declan McCullagh dba Justice on Campus; Brock Meeks dba Cyberwire Dispatch; John Troyer dba The Safer Sex Page; Jonathan Wallace dba The Ethical Spectacle; and Planned Parenthood Federation of America, Inc.

FN28. American Library Association; America Online, Inc.; American Booksellers Association, Inc.; American Booksellers Foundation for Free Expression; American Society of Newspaper Editors; Apple Computer, Inc.; Association of American Publishers, Inc.; Association of Publishers, Editors and Writers; Citizens Internet Empowerment Coalition; Commercial Internet Exchange Association; CompuServe Incorporated; Families Against Internet Censorship; Freedom to Read Foundation, Inc.; Health Sciences Libraries Consortium; Hotwired Ventures LLC; Interactive Digital Software Association; Interactive Services Association; Magazine Publishers of America; Microsoft Corporation; The Microsoft Network, L. L. C.; National Press Photographers Association; Netcom On-Line Communication Services, Inc.; Newspaper Association of America; Opnet, Inc.; Prodigy Services Company; Society of Professional Journalists; Wired Ventures, Ltd.


FN30. See also 929 F. Supp., at 877: "Four related characteristics of Internet communication have a transcendent importance to our shared holding that the CDA is unconstitutional on its face. We explain these characteristics in our Findings of fact above, and I only rehearse them briefly here. First, the Internet presents very low barriers to entry. Second, these barriers to entry are identical for both speakers and listeners. Third, as a result of these low barriers, astoundingly diverse content is available on the Internet. Fourth, the Internet provides significant access to all who wish to speak in the medium, and even creates a relative parity among speakers." According to Judge Dalzell, these characteristics and the rest of the District Court's findings "lead to the conclusion that Congress may not regulate indecency on the Internet at all." Ibid. Because appellees do not press this argument before this Court, we do not consider it. Appellees also do not dispute that the Government generally has a compelling interest in protecting minors from "indecent" and "patently offensive" speech.

FN31. 390 U. S., at 639. We quoted from Prince v. Massachusetts, 321 U. S. 158, 166 (1944): "It is cardinal with us that the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder."

FN32. Given the likelihood that many E-mail transmissions from an adult to a minor are conversations between family members, it is therefore incorrect for the dissent to suggest that the provisions of the CDA, even in this narrow area, "are no different from the law we sustained in Ginsberg." Post, at 8.

FN33. Cf. Pacifica Foundation v. FCC, 556 F. 2d 9, 36 (CADC 1977) (Levanthal, J., dissenting), rev'd, FCC v. Pacifica Foundation, 438 U. S. 726 (1978). When Pacifica was decided, given that radio stations were allowed to operate only pursuant to federal license, and that Congress had enacted legislation prohibiting licensees from broadcasting indecent speech, there was a risk that members of the radio audience might infer some sort of official or societal approval of whatever was heard over the radio, see 556 F. 2d, at 37, n. 18. No such risk attends messages received through the Internet, which is not supervised by any federal agency.

FN34. Juris. Statement 3 (citing 929 F. Supp., at 831 (finding 3)).
FN35. "Indecent" does not benefit from any textual embellishment at all. "Patently offensive" is qualified only to the extent that it involves "sexual or excretory activities or organs" taken "in context" and "measured by contemporary community standards."

FN36. See Golan-Peretz v. United States, 498 U. S. 395, 404 (1991) ("Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion and exclusion") (internal quotation marks omitted).


FN38. Even though the word "trunk," standing alone, might refer to luggage, a swimming suit, the base of a tree, or the long nose of an animal, its meaning is clear when it is one prong of a three-part description of a species of gray animals.

FN39. 413 U. S., at 30 (Determinations of "what appeals to the 'prurient interest' or is 'patently offensive'. . . . are essentially questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists"). The CDA, which implements the "contemporary community standards" language of Miller, thus conflicts with the Conferees' own assertion that the CDA was intended "to establish a uniform national standard of content regulation." S. Conf. Rep., at 191.


FN41. The lack of legislative attention to the statute at issue in Sable suggests another parallel with this case. Compare 492 U. S., at 129–130 ("[A]side from conclusory statements during the debates by proponents of the bill, as well as similar assertions in hearings on a substantially identical bill the year before, . . . the congressional record presented to us contains no evidence as to how effective or ineffective the FCC's most recent regulations were or might prove to be. . . . No Congressman or Senator purported to present a considered judgment with respect to how often or to what extent minors could or would circumvent the rules and have access to dial-a-porn messages") with n. 24, supra.

FN42. The Government agrees that these provisions are applicable whenever "a sender transmits a message to more than one recipient, knowing that at least one of the specific persons receiving the message is a minor." Opposition to Motion to Affirm and Reply to Juris. Statement 4–5, n. 1.

FN43. The Government asserts that "[t]here is nothing constitutionally suspect about requiring commercial Web site operators . . . to shoulder the modest burdens associated with their use." Brief for Appellants 35. As a matter of fact, however, there is no evidence that a "modest burden" would be effective.

FN44. Transmitting obscenity and child pornography, whether via the Internet or other means, is already illegal under federal law for both adults and juveniles. See 18 U. S. C. §§1464–1465 (criminalizing obscenity); §2251 (criminalizing child pornography). In fact, when Congress was considering the CDA, the Government expressed its view that the law was unnecessary because existing laws already

FN45. Citing Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U. S. 520 (1993), among other cases, appellees offer an additional reason why, in their view, the CDA fails strict scrutiny. Because so much sexually explicit content originates overseas, they argue, the CDA cannot be "effective." Brief for Appellees American Library Association et al. 33–34. This argument raises difficult issues regarding the intended, as well as the permissible scope of, extraterritorial application of the CDA. We find it unnecessary to address those issues to dispose of this case.

FN46. For the full text of §223(e)(5), see n. 26, supra.

FN47. Thus, ironically, this defense may significantly protect commercial purveyors of obscene postings while providing little (or no) benefit for transmitters of indecent messages that have significant social or artistic value.


FN49. As this Court long ago explained, "It would certainly be dangerous if the Legislature could set a net large enough to catch all possible offenders and leave it to the courts to step inside and say who could be rightfully be detained and who should be set at large. This would, to some extent, substitute the judicial for the legislative department of the government." United States v. Reese, 92 U. S. 214, 221 (1876). In part because of these separation of powers concerns, we have held that a severability clause is "an aid merely; not an inexorable command." Dorcy v. Kansas, 264 U. S. 286, 290 (1924).

FN50. See also Osborne v. Ohio, 495 U. S. 103, 121 (1990) (judicial rewriting of statutes would derogate Congress's "incentive to draft a narrowly tailored law in the first place").

SUPREME COURT OF THE UNITED STATES

No. 96–511

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al.,
APPELLANTS

v.

AMERICAN CIVIL LIBERTIES UNION et al.
APPELLEES

On appeal from the United States District Court for the Eastern District of Pennsylvania

June 26, 1997

Justice O'Connor, with whom The Chief Justice joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes
Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). What the Court classifies as a single "patently offensive display" provision, see ante, at 11, is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specific person" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in any manner available" to minors ("display" provision). §223(d)(1)(B). None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech. Sable Communications of Cal., Inc. v. FCC, 492 U. S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment").

Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. See S. Conf. Rep. No. 104–230, p. 189 (1996) (CDA imposes "access restrictions . . . to protect minors from exposure to indecent material").

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults.[1] States have also denied minors access to speech deemed to be "harmful to minors."[2] The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the Court, however, I would invalidate the provisions only in those circumstances.

I

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no right to obtain—it interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population . . . to reading only what is fit for children." Butler v. Michigan, 352 U. S. 380, 383 (1957). The First Amendment does not tolerate such interference. See id., at 383 (striking down a Michigan criminal law banning sale of books—to minors or adults—that contained words or pictures that "tende[d] to . . . corrupt[t] the morals of youth"); Sable Communications, supra (invalidating federal law that made it a crime to transmit indecent, but nonobscene, commercial telephone messages to minors and adults); Bolger v. Youngs Drug Products Corp., 463 U. S. 60, 74 (1983) (striking down a federal law prohibiting the mailing of unsolicited advertisements for contraceptives). If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In Ginsberg v. New York, 390 U. S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazines to minors in part because adults could still buy those magazines.

The Court in Ginsberg concluded that the New York law created a constitutionally adequate adult zone simply because, on its face, it denied access only to minors. The Court did not question—and therefore necessarily assumed—that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity. See Lessig, Reading the Constitution in Cyberspace, 45 Emory L. J. 869, 886 (1996). A minor can see an adult dance show only if he enters an establishment that provides such entertainment. And should he attempt to do so, the minor will not be able to conceal completely his identity (or, consequently, his age). Thus, the twin characteristics of geography and identity enable the establishment's proprietor to prevent children from entering the establishment, but to let adults inside.

The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities. Cyberspace
undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed "locations" on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, see Lessig, supra, at 901, however, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. Lessig, supra, at 888–889. Id., at 887 (cyberspace "is moving . . . from a relatively unzoned place to a universe that is extraordinarily well zoned"). Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves—perhaps an adult identification number or a credit card number—before they can access certain areas of cyberspace, 929 F. Supp. 824, 845 (E.D Pa. 1996), much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what his children watch on television by installing a lock box. This user-based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites. Id., at 839–842. The Platform for Internet Content Selection (PICS) project is designed to facilitate user-based zoning by encouraging Internet speakers to rate the content of their speech using codes recognized by all screening programs. Id., at 838–839.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, id., at 845; Shea v. Reno, 930 F. Supp. 916, 933–934 (S.D.N.Y. 1996), it is not available to all Web speakers, 929 F. Supp., at 845–846, and is just now becoming technologically feasible for chat rooms and USENET newsgroups, Brief for Federal Parties 37–38. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned—and unzoneable. 929 F. Supp., at 846; Shea, supra, at 934. User-based zoning is also in its infancy. For it to be effective, (i) an agreed-upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available—and widely used—by Internet users. At present, none of these conditions is true. Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." Shea, supra, at 945–946. There is, moreover, no agreed-upon "tag" for those programs to recognize. 929 F. Supp., at 848; Shea, supra, at 945.

Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today. Ante, at 36. Given the present state of cyberspace, I agree with the Court that the "display" provision cannot pass muster. Until gateway technology is available throughout cyberspace, and it is not in 1997, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone." Thus, the only way for a speaker to avoid liability under the CDA is to refrain completely from using indecent speech. But this forced silence impinges on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." Butler, 352 U. S., at 383. As a result, the "display" provision cannot withstand scrutiny. Accord, Sable Communications, 492 U. S., at 126–131; Bolger v. Youngs Drug Products Corp., 463 U. S., at 73–75.

The "indecency transmission" and "specific person" provisions present a closer issue, for they are not unconstitutional in all of their applications. As discussed above, the "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18 years of age. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient of his indecent message is a minor. §223(d)(1)(A). Appellant urges the Court to construe the provision to impose such a knowledge requirement, see Brief for Federal Parties 25–27, and I would do so. See
Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U. S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress").

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors—e.g., when an adult speaker sends an e-mail knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in Ginsberg. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults. He is not prevented from speaking indecently to other adults in a chat room (because there are no other adults participating in the conversation) and he remains free to send indecent e-mails to other adults. The relevant universe contains only one adult, and the adult in that universe has the power to refrain from using indecent speech and consequently to keep all such speech within the room in an "adult" zone.

The analogy to Ginsberg breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group, since they would be transmitting an indecent message to specific persons, one of whom is a minor. Accord, ante, at 30. The CDA is therefore akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store. Even assuming such a law might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store, the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. And as discussed below, I do not find that the provisions are overbroad in the sense that they restrict minors' access to a substantial amount of speech that minors have the right to read and view. Accordingly, the CDA can be applied constitutionally in some situations. Normally, this fact would require the Court to reject a direct facial challenge. United States v. Salerno, 481 U. S. 739, 745 (1987) ("A facial challenge to a legislative Act [succeeds only if] the challenger . . . establish[es] that no set of circumstances exists under which the Act would be valid"). Appellees' claim arises under the First Amendment, however, and they argue that the CDA is facially invalid because it is "substantially overbroad"—that is, it "sweeps too broadly . . . [and] penaliz[es] a substantial amount of speech that is constitutionally protected," Forsyth County v. Nationalist Movement, 505 U. S. 123, 130 (1992). See Brief for Appellees American Library Association et al. 48; Brief for Appellees American Civil Liberties Union et al. 39-41. I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication.

This conclusion does not end the matter, however. Where, as here, "the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish . . . [t]he statute may forthwith be declared invalid to the extent that it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U. S. 491, 504 (1985). There is no question that Congress intended to prohibit certain communications between one adult and one or more minors. See 47 U. S. C. §223(a)(1)(B) (May 1996 Supp.) (punishing "[w]hoever . . . initiates the transmission of [any indecent communication] knowingly that the recipient of the communication is under 18 years of age"); §223(d)(1)(A) (punishing "[w]hoever . . . send[s] to a specific person or persons under 18 years of age [a patently offensive message]"). There is also no question that Congress would have enacted a narrower version of these provisions had it known a broader version would be declared unconstitutional. 47 U. S. C. §608 ("If . . . the application [of any provision of the CDA] to any person or circumstance is held invalid, . . . the application of such provision to other persons or circumstances shall not be affected thereby"). I would therefore sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of Internet communications where the party initiating the communication knows that all of the recipients are minors.
II

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question. In Ginsberg, the New York law we sustained prohibited the sale to minors of magazines that were "harmful to minors." Under that law, a magazine was "harmful to minors" only if it was obscene as to minors. 390 U. S., at 632–633. Noting that obscene speech is not protected by the First Amendment, Roth v. United States, 354 U. S. 476, 485 (1957), and that New York was constitutionally free to adjust the definition of obscenity for minors, 390 U. S., at 638, the Court concluded that the law did not "invalid[e] the area of freedom of expression constitutionally secured to minors." Ia., at 637. New York therefore did not infringe upon the First Amendment rights of minors. Cf. Erznoznik v. Jacksonville, 422 U. S. 205, 213 (1975) (striking down city ordinance that banned nudity that was not "obscene even as to minors").

The Court neither "accept[s] nor reject[s]" the argument that the CDA is facially overbroad because it substantially interferes with the First Amendment rights of minors. Ante, at 32. I would reject it. Ginsberg established that minors may constitutionally be denied access to material that is obscene as to minors. As Ginsberg explained, material is obscene as to minors if it (i) is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable . . . for minors"; (ii) appeals to the prurient interest of minors; and (iii) is "utterly without redeeming social importance for minors." 390 U. S., at 633. Because the CDA denies minors the right to obtain material that is "patently offensive"—even if it has some redeeming value for minors and even if it does not appeal to their prurient interests—Congress' rejection of the Ginsberg "harmful to minors" standard means that the CDA could ban some speech that is "indecent" (i.e., "patently offensive") but that is not obscene as to minors.

I do not deny this possibility, but to prevail in a facial challenge, it is not enough for a plaintiff to show "some" overbreadth. Our cases require a proof of "real" and "substantial" overbreadth, Broadrick v. Oklahoma, 413 U. S. 601, 615 (1973), and appellees have not carried their burden in this case. In my view, the universe of speech constitutionally protected as to minors but banned by the CDA—i.e., the universe of material that is "patently offensive," but which nonetheless has some redeeming value for minors or does not appeal to their prurient interest—is a very small one. Appellees cite no examples of speech falling within this universe and do not attempt to explain why that universe is substantial "in relation to the statute's plainly legitimate sweep." Ibid. That the CDA might deny minors the right to obtain material that has some "value," see ante, at 32–33, is largely beside the point. While discussions about prison rape or nude art, see ibid., may have some redeeming education value for adults, they do not necessarily have any such value for minors, and under Ginsberg, minors only have a First Amendment right to obtain patently offensive material that has "redeeming social importance for minors," 390 U. S., at 633 (emphasis added). There is also no evidence in the record to support the contention that "many [e]-mail transmissions from an adult to a minor are conversations between family members," ante, at 18, n. 32, and no support for the legal proposition that such speech is absolutely immune from regulation. Accordingly, in my view, the CDA does not burden a substantial amount of minors' constitutionally protected speech.

Thus, the constitutionality of the CDA as a zoning law hinges on the extent to which it substantially interferes with the First Amendment rights of adults. Because the rights of adults are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained. The Court reaches a contrary conclusion, and from that holding that I respectfully dissent.

FOOTNOTES: (concurrence)


RECOMMENDED FOR FULL-TEXT PUBLICATION

Pursuant to Sixth Circuit Rule 24

ELECTRONIC CITATION: 1996 FED App. 0032P (6th Cir.)

File Name: 96a0032p.06

Nos. 94-6648/6649

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

____________________________

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ROBERT ALAN THOMAS (94-6648)

and CARLEEN THOMAS (94-6649),

Defendants-Appellants.

>

ON APPEAL from the United States District Court for the Western District of Tennessee

____________________________

Decided and Filed January 29, 1996

____________________________

Before: MARTIN and BATCHELDER, Circuit Judges; EDMUNDS, District Judge.[*

NANCY G. EDMUNDS, District Judge. Defendants Robert and Carleen Thomas appeal their convictions and sentences for violating 18 U.S.C. §§ 1462 and 1465,

federal obscenity laws, in connection with their operation of an electronic bulletin board. For the following reasons, we AFFIRM Robert and Carleen Thomas' convictions and sentences.

I.

Robert Thomas and his wife Carleen Thomas began operating the Amateur Action Computer Bulletin Board System ("AABBS") from their home in Milpitas, California in February 1991. The AABBS was a computer bulletin board system that operated by using telephones, modems, and personal computers. Its features included e-mail, chat lines, public messages, and files that members could access, transfer, and download to their own computers and printers.

Information loaded onto the bulletin board was first converted into binary code, i.e., 0's and 1's, through the use of a scanning device. After purchasing sexually-explicit magazines from public adult book stores in California, Defendant Robert Thomas used an electronic device called a scanner to convert pictures
from the magazines into computer files called Graphic Interchange Format files or "GIF" files. The AABBS contained approximately 14,000 GIF files. Mr. Thomas also purchased, sold, and delivered sexually-explicit videotapes to AABBS members. Customers ordered the tapes by sending Robert Thomas an e-mail message, and Thomas typically delivered them by use of the United Parcel Service ("U.P.S.").

Persons calling the AABBS without a password could view the introductory screens of the system which contained brief, sexually-explicit descriptions of the GIF files and adult videotapes that were offered for sale. Access to the GIF files, however, was limited to members who were given a password after they paid a membership fee and submitted a signed application form that Defendant Robert Thomas reviewed. The application form required the applicant's age, address, and telephone number and required a signature.

Members accessed the GIF files by using a telephone, modem and personal computer. A modem located in the Defendants' home answered the calls. After they established membership by typing in a password, members could then select, retrieve, and instantly transport GIF files to their own computer. A caller could then view the GIF file on his computer screen and print the image out using his printer. The GIF files contained the AABBS name and access telephone number; many also had "Distribute Freely" printed on the image itself.

In July 1993, a United States Postal Inspector, Agent David Dirmeyer ("Dirmeyer"), received a complaint regarding the AABBS from an individual who resided in the Western District of Tennessee. Dirmeyer dialed the AABBS' telephone number. As a non-member, he viewed a screen that read "Welcome to AABBS, the Nastiest Place On Earth," and was able to select various "menus" and read graphic descriptions of the GIF files and videotapes that were offered for sale.

Subsequently, Dirmeyer used an assumed name and sent in $55 along with an executed application form to the AABBS. Defendant Robert Thomas called Dirmeyer at his undercover telephone number in Memphis, Tennessee, acknowledged receipt of his application, and authorized him to log-on with his personal password. Thereafter, Dirmeyer dialed the AABBS's telephone number, logged-on and, using his computer/modem in Memphis, downloaded the GIF files listed in counts 2-7 of the Defendants' indictments. These GIF files depicted images of bestiality, oral sex, incest, sado-masochistic abuse, and sex scenes involving urination. Dirmeyer also ordered six sexually-explicit videotapes from the AABBS and received them via U.P.S. at a Memphis, Tennessee address. Dirmeyer also had several e-mail and chat-mode conversations with Defendant Robert Thomas.

On January 10, 1994, a search warrant was issued by a U.S. Magistrate Judge for the Northern District of California. The AABBS' location was subsequently searched, and the Defendants' computer system was seized.

On January 25, 1994, a federal grand jury for the Western District of Tennessee returned a twelve-count indictment charging Defendants Robert and Carleen Thomas with the following criminal violations: one count under 18 U.S.C. § 371 for conspiracy to violate federal obscenity laws--18 U.S.C. §§ 1462, 1465 (Count 1), six counts under 18 U.S.C. § 1465 for knowingly using and causing to be used a facility and means of interstate commerce--a combined computer/telephone system--for the purpose of transporting obscene, computer-generated materials (the GIF files) in interstate commerce (Counts 2-7), three counts under 18 U.S.C. § 1462 for shipping obscene videotapes via U.P.S. (Counts 8-10), one count of causing the transportation of materials depicting minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(1) as to Mr. Thomas only (Count 11), and one count of forfeiture under 18 U.S.C. § 1467 (Count 12).

Both Defendants were represented by the same retained counsel, Mr. Richard Williams of San Jose, California. They appeared twice in federal district court for the Northern District of California, San Jose division, before being arraigned on March 15, 1994, in federal court in Memphis, Tennessee. They did not retain local counsel for the Tennessee criminal prosecution. Both Defendants were tried by a jury in
July, 1994. Defendant Robert Thomas was found guilty on all counts except count 11 (child pornography). Defendant Carleen Thomas was found guilty on counts 1-10. The jury also found that the Defendants' interest in their computer system should be forfeited to the United States. Robert and Carleen Thomas were sentenced on December 2, 1994 to 37 and 30 months of incarceration, respectively. They filed their notices of appeal on December 9, 1994.

II.

A.

Defendants contend that their conduct, as charged in counts 1-7 of their indictments, does not constitute a violation of 18 U.S.C. § 1465. This presents a question of statutory interpretation, a matter of law, and is reviewed by this court under a de novo standard. United States v. Hans, 921 F.2d 81, 82 (6th Cir. 1990).[1]

Defendants' challenge to their convictions under counts 1-7, rests on two basic premises: 1) Section 1465 does not apply to intangible objects like the computer GIF files at issue here.[2]

Whoever knowingly transports in interstate or foreign commerce for the purpose of sale or distribution, or knowingly travels in interstate commerce, or uses a facility or means of interstate commerce for the purpose of transporting obscene material in interstate or foreign commerce, any obscene, lewd, lascivious, or filthy book, pamphlet, picture, film, paper, letter, writing, print, silhouette, drawing, figure, image, cast, phonograph recording, electrical transcription or other article capable of producing sound or any other matter of indecent or immoral character, shall be fined under this title or imprisoned not more than five years, or both.

The transportation as aforesaid of two or more copies of any publication or two or more of any article of the character described above, or a combined total of five such publications and articles, shall create a presumption that such publications or articles are intended for sale or distribution, but such presumption is rebuttable. 42 U.S.C.A. § 1465 (West 1995 Supp.). and 2) Congress did not intend to regulate computer transmissions such as those involved here because 18 U.S.C. § 1465 does not expressly prohibit such conduct.

In support of their first premise, Defendants cite a Tenth Circuit dial-a-porn decision which holds that 18 U.S.C. §§ 1462 and 1465 prohibit the interstate transportation of tangible objects; not intangible articles like pre-recorded telephone messages. See United States v. Carlin Commun., Inc., 815 F.2d 1367, 1371 (10th Cir. 1987). Defendants claim Carlin is controlling because transmission of the GIF files at issue under counts 1-7 involved an intangible string of 0's and 1's which became viewable images only after they were decoded by an AABBS member's computer. We disagree.

The subject matter in Carlin--telephonic communication of pre-recorded sexually suggestive comments or proposals--is inherently different from the obscene computer-generated materials that were electronically transmitted from California to Tennessee in this case. Defendants erroneously conclude that the GIF files are intangible, and thus outside the scope of § 1465, by focusing solely on the manner and form in which the computer-generated images are transmitted from one destination to another. United States v. Gilboe, 684 F.2d 235 (2nd Cir. 1982), cert. denied, 459 U.S. 1201 (1983), illustrates this point.

In Gilboe, the Second Circuit rejected the argument that the defendant's transmission of electronic impulses could not be prosecuted under a criminal statute prohibiting the transportation of money obtained by fraud. The Gilboe court reasoned that:

electronic signals in this context are the means by which funds are transported. The beginning of the transaction is money in one account and the ending is money in another. The manner in which the funds were moved does not affect the ability to obtain tangible paper dollars or a bank check from the
receiving account.

Id. at 238. The same rationale applies here. Defendants focus on the means by which the GIF files were transferred rather than the fact that the transmissions began with computer-generated images in California and ended with the same computer-generated images in Tennessee. The manner in which the images moved does not affect their ability to be viewed on a computer screen in Tennessee or their ability to be printed out in hard copy in that distant location.

The record does not support Defendants' argument that they had no knowledge, intent or expectation that members of their AABBS would download and print the images contained in their GIF files. They ran a business that advertised and promised its members the availability and transportation of the sexually-explicit GIF files they selected. In light of the overwhelming evidence produced at trial, it is spurious for Defendants to claim now that they did not intend to sell, disseminate, or share the obscene GIF files they advertised on the AABBS with members outside their home and in other states.

We also disagree with Defendants' corollary position, raised at oral argument, that they were prosecuted under the wrong statute and that their conduct, if criminal at all,

falls within the prohibitions under 47 U.S.C. § 223(b)[3]

(1) Whoever knowingly

(A) within the United States, by means of telephone, makes (directly or by recording device) any obscene communication for commercial purposes to any person, regardless of whether the maker of such communication placed the call; or

(B) permits any telephone facility under such person's control to be used for an activity prohibited by subparagraph (A),

shall be fined in accordance with Title 18, or imprisoned not more than two years, or both. rather than 18 U.S.C. § 1465. As recognized by the Supreme Court, Section 223(b) of the Communications Act of 1934, was drafted and enacted by Congress in 1982 "explicitly to address 'dial-a-porn.'" Sable Communications of Cal., Inc. v. F.C.C., 492 U.S. 115, 120-121 (1989). Congress amended Section 223(b) in 1988 to impose a total ban "on dial-a-porn, making it illegal for adults, as well as children, to have access to sexually-explicit messages" that are indecent or obscene. Id. at 122-123.[4] 47 U.S.C. § 223(b) addresses commercial dial-a-porn operations that communicate sexually-explicit telephone messages; not commercial computer bulletin boards that use telephone facilities for the purpose of transmitting obscene, computer-generated images to approved members.

Defendants' second premise, that Congress did not intend to regulate computer transmissions because the statute does not expressly prohibit such conduct, is faulty as well. We have consistently recognized that when construing federal statutes, our duty is to "construe the language so as to give effect to the intent of Congress." United States v. Underhill, 813 F.2d 105, 111 (6th Cir.), cert. denied, 482 U.S. 906 (1987) (quoting United States v. American Trucking Associations, Inc., 310 U.S. 534, 542-44 (1940)). The Supreme Court observed this principle when it rejected an argument similar to one Defendants raise here, i.e., that Congress could not possibly have intended to include conduct not expressly prohibited in the statute. See United States v. Alpers, 338 U.S. 680 (1950).

In United States v. Alpers, the Supreme Court considered the question whether obscene phonograph records--at the time, a novel means of transmitting obscenity--came within the prohibition of 18 U.S.C. § 1462. Initially, the Court acknowledged that criminal statutes are to be strictly construed and that "no offense may be created except by the words of Congress used in their usual and ordinary way." Id. at 681. The Court emphasized, however, that Congress' intent is the most important determination and statutory language is not to be construed in a manner that would defeat that intent.

Applying those principles, the Court held that the rule of ejusdem generis[5] should not be "employed to render general words meaningless" or "be used to defeat the obvious purpose of legislation." Id. at
681-83. It recognized that "[t]he obvious purpose of [Section 1462] was to prevent the channels of interstate commerce from being used to disseminate" any obscene matter. Id. at 683. The Court further recognized that Section 1462 "is a comprehensive statute, which should not be construed by

a mechanical rule of construction." Id. at 684. Accordingly, the Court rejected the defendant's argument that the general words "other matter of indecent character" could not be interpreted to include objects comprehensible by hearing (phonographic recordings) rather than sight; an argument similar to the tangible/intangible one raised here, and held that obscene records fell within the scope of the criminal statute.

In reaching its decision, the Alpers Court found that the legislative history of Section 1462 did not support defendant's sight/sound distinction. It was not persuaded that Congress' amendment of Section 1462 to add motion picture films to the list of prohibited materials "evidenced an intent that obscene matter not specifically added was without the prohibition of the statute." Id. Rather, the Court concluded that the amendment evidenced Congress' preoccupation "with making doubly sure that motion-picture film was within the Act, and was concerned with nothing more or less." Id. We are similarly unpersuaded by Defendants' arguments that the absence of the words "including by computer" in Section 1465, despite Congress' addition of those words in other legislation, is evidence of its intent not to criminalize conduct, such as Defendants' that falls within the plain language and intent of Section 1465.

Furthermore, under similar facts, the U.S. Air Force Court of Criminal Appeals recently considered § 1465's plain language and its intended purpose. In United States v. Maxwell, 42 M.J. 568, 1995 WL 259269 (A.F. Ct. Crim. App. 1995), a defendant was charged with violating Section 1465 because he had transmitted obscene visual images electronically through the use of an on-line computer service. He argued that since the statute is silent concerning computer transmissions, such transmissions were not to be included within the terms "transporting obscene materials in interstate or foreign commerce." The court observed that well-established principles of statutory construction require a court to look first to the statute's plain language. Maxwell, 1995 WL 259269 at *10 (citing

Rubin v. United States, 449 U.S. 424, 430 (1981)). Applying that principle, the Maxwell court concluded that the defendant's conduct fell within the plain language of Section 1465. Specifically, the court held:

[t]he use of the terms "transports," "distribution," "picture," "image" and "electrical transcription" leads us to the inescapable conclusion the statute is fully applicable to the activities engaged in by applicant. . . . It is clear Congress intended to stem the transportation of obscene material in interstate commerce regardless of the means used to effect that end.


Likewise, we conclude that Defendants' conduct here falls within the plain language of Section 1465.[6] Moreover, our interpretation of Section 1465 is consistent with Congress' intent to legislate comprehensively the interstate distribution of obscene materials. Id.

B.

Defendants also challenge venue in the Western District of Tennessee for counts 2-7 of their indictments. They argue that even if venue was proper under count 1 (conspiracy) and counts 8-10 (videotapes sent via U.P.S.), counts 2-7 (GIF files) should have been severed and transferred to California because Defendants did not cause the GIF files to be transmitted to the Western District of Tennessee. Rather, Defendants assert, it was Dirmeyer, a government agent, who, without their knowledge, accessed and downloaded the GIF files and caused them to enter Tennessee. We disagree. To establish a Section 1465 violation, the Government must prove that a defendant

knowingly used a facility or means of interstate commerce for the purpose of distributing obscene materials. Contrary to Defendants' position, Section 1465 does not require the Government to prove that Defendants had specific knowledge of the destination of each transmittal at the time it occurred.
"Venue lies in any district in which the offense was committed," and the Government is required to establish venue by a preponderance of the evidence. United States v. Beddow, 957 F.2d 1330, 1335 (6th Cir. 1992) (quoting United States v. Williams, 788 F.2d 1213, 1215 (6th Cir. 1986)). This court examines the propriety of venue by taking "into account a number of factors—the site of the defendant's acts, the elements and nature of the crime, the locus of the effect of the criminal conduct, and the suitability of each district for accurate fact finding..." Id.

Section 1465 is an obscenity statute, and federal obscenity laws, by virtue of their inherent nexus to interstate and foreign commerce, generally involve acts in more than one jurisdiction or state. Furthermore, it is well-established that "there is no constitutional impediment to the government's power to prosecute pornography dealers in any district into which the material is sent." United States v. Bagnell, 679 F.2d 826, 830 (11th Cir. 1982), cert. denied, 460 U.S. 1047 (1983); United States v. Peraino, 645 F.2d 548, 551 (6th Cir. 1981). Thus, the question of venue has become one of legislative intent. Bagnell, 679 F.2d at 830.

The Bagnell court examined both §§ 1462 and 1465 and found that each statute established a continuing offense within the venue provisions of 18 U.S.C. § 3237(a) "that occur[s] in every judicial district which the material touches." Id. at 830. This court likewise recognized that "venue for federal obscenity prosecutions lies 'in any district from, through, or into which' the allegedly obscene material moves." Peraino, 645 F.2d at 551 (citing 18 U.S.C. § 3237).

Substantial evidence introduced at trial demonstrated that the AABBS was set up so members located in other jurisdictions could access and order GIF files which would then be instantaneously transmitted in interstate commerce. Moreover, AABBS materials were distributed to an approved AABBS member known to reside in the Western District of Tennessee. Specifically, Defendant Robert Thomas knew of, approved, and had conversed with an AABBS member in that judicial district who had his permission to access and copy GIF files that ultimately ended up there. Some of these GIF files were clearly marked "Distribute Freely." In light of the above, the effects of the Defendants' criminal conduct reached the Western District of Tennessee, and that district was suitable for accurate fact-finding. Accordingly, we conclude venue was proper in that judicial district.

C.

Defendants further argue that their convictions under counts 1-7 of their indictments violate their First Amendment rights to freedom of speech. As the Supreme Court noted in Bose, when constitutional facts[7] are at issue, this court has a duty to conduct an independent review of the record "both to be sure that the speech in question actually falls within the unprotected category and to confine the perimeters of any unprotected category within acceptably narrow limits in an effort to ensure that protected expression will not be inhibited." Bose Corp. v. Consumers Union of United States, Inc., 466 U.S. 485, 505 (1984).

1. Defendants' Right to Possess the GIF Files in their Home

 Defendants rely on Stanley v. Georgia, 394 U.S. 557 (1969), and argue they have a constitutionally protected right to possess obscene materials in the privacy of their home. They insist that the GIF files containing sexually-explicit material never left their home. Defendants' reliance on Stanley is misplaced.

The Supreme Court has clarified that Stanley "depended not on any First Amendment Right to purchase or possess obscene materials, but on the right to privacy in the home." United States v. 12 200-Ft. Reels of Super 8mm. Film, 413 U.S. 123, 126 (1973). It has also recognized that the right to possess obscene materials in the privacy of one's home does not create "a correlative right to receive it, transport it, or distribute it" in interstate commerce even if it is for private use only. Nor does it create "some zone of constitutionally protected privacy [that] follows such material when it is moved outside the home area." United States v. Orito, 413 U.S. 139, 141 (1973); see also 12 200-Ft. Reels, 413 U.S. at 128.

Defendants went beyond merely possessing obscene GIF files in their home. They ran a business that advertised and promised its members the availability and transportation of the sexually-explicit GIF files they selected. In light of the overwhelming evidence produced at trial, it is spurious for Defendants to
claim now that they did not intend to sell, disseminate, or share the obscene GIF files they advertised on the AABBS with members outside their home and in other states.

2. The Community Standards to be Applied When Determining Whether the GIF Files Are Obscene

In *Miller v. California*, 413 U.S. 15 (1973), the Supreme Court set out a three-prong test for obscenity. It inquired whether (1) "the average person applying contemporary community standards' would find that the work, taken as a whole appeals to the prurient interest"; (2) it "depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law"; and (3) "the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." *Id.* at 24.

Under the first prong of the *Miller* obscenity test, the jury is to apply "contemporary community standards." Defendants acknowledge the general principle that, in cases involving interstate transportation of obscene material, juries are properly instructed to apply the community standards of the geographic area where the materials are sent. *Miller*, 413 U.S. at 15, 30-34. Nonetheless, Defendants assert that this principle does not apply here for the same reasons they claim venue was improper. As demonstrated above, this argument cannot withstand scrutiny. The computer-generated images described in counts 2-7 were electronically transferred from Defendants' home in California to the Western District of Tennessee. Accordingly, the community standards of that judicial district were properly applied in this case.

Issues regarding which community's standards are to be applied are tied to those involving venue. It is well-established that:

"[v]enue for federal obscenity prosecutions lies 'in any district from, through, or into which' the allegedly obscene material moves, according to 18 U.S.C. § 3237. This may result in prosecutions of persons in a community to which they have sent materials which is obscene under that community's standards though the community from which it is sent would tolerate the same material."

*United States v. Peraino*, 645 F.2d 548, 551 (6th Cir. 1981). Prosecutions may be brought either in the district of dispatch or the district of receipt, *Bagnell*, 679 F.2d at 830-31, and obscenity is determined by the standards of the community where the trial takes place. See *Miller*, 413 U.S. at 15, 30-34; *Hamling v. United States*, 418 U.S. 87, 105-6 (1974); *Sable*, 492 U.S. at 125. Moreover, the federal courts have consistently recognized that it is not unconstitutional to subject interstate distributors of obscenity to varying community standards. *Hamling*, 418 U.S. at 106; *United States v. Sandy*, 605 F.2d 210, 217 (6th Cir.), *cert. denied*, 444 U.S. 984 (1979).

3. The Implications of Computer Technology on the Definition of "Community"

Defendants and *Amicus Curiae* appearing on their behalf argue that the computer technology used here requires a new definition of community, i.e., one that is based on the broad-ranging connections among people in cyberspace rather than the geographic locale of the federal judicial district of the criminal trial. Without a more flexible definition, they argue, there will be an impermissible chill on protected speech because BBS operators cannot select who gets the materials they make available on their bulletin boards. Therefore, they contend, BBS operators like Defendants will be forced to censor their materials so as not to run afoul of the standards of the community with the most restrictive standards.

Defendants' First Amendment issue, however, is not implicated by the facts of this case. This is not a situation where the bulletin board operator had no knowledge or control over the jurisdictions where materials were distributed for downloading or printing. Access to the Defendants' AABBS was limited. Membership was necessary and applications were submitted and screened before passwords were issued and materials were distributed. Thus, Defendants had in place methods to limit user access in
jurisdictions where the risk of a finding of obscenity was greater than that in California. They knew they had a member in Memphis; the member's address and local phone number were provided on his application form. If Defendants did not wish to subject themselves to liability in jurisdictions with less tolerant standards for determining obscenity, they could have refused to give passwords to members in those districts, thus precluding the risk of liability.

This result is supported by the Supreme Court's decision in Sable Communications of Cal., Inc. v. F.C.C. where the Court rejected Sable's argument that it should not be compelled to tailor its dial-a-porn messages to the standards of the least tolerant community. 492 U.S. 115, 125-26 (1989). The Court recognized that distributors of allegedly obscene materials may be subjected to the standards of the varying communities where they transmit their materials, citing Hamling, and further noted that Sable was "free to tailor its messages, on a selective basis, if it so chooses, to the communities it chooses to serve." Id. at 125. The Court also found no constitutional impediment to forcing Sable to incur some costs in developing and implementing a method for screening a customer's location and "providing messages compatible with community standards." Id.

Thus, under the facts of this case, there is no need for this court to adopt a new definition of "community" for use in obscenity prosecutions involving electronic bulletin boards. This court's decision is guided by one of the cardinal rules governing the federal courts, i.e., never reach constitutional questions not squarely presented by the facts of a case. Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 502 (1985).

D.

Defendants next raise a number of challenges to the jury instructions given at their trial. Initially, they claim that, as to counts 2, 3, 6 and 9, the district court should have included an augmented unanimity instruction because those counts involved more than one GIF file or videotape. The district court instructed the jury that "[i]f more than one article is alleged to be obscene in a particular count, the government is required to show only that one of these articles was obscene." There was no request for an augmented unanimity instruction and there was no objection at trial to the instruction given. The issue was raised for the first time at sentencing. Accordingly, this court reviews for plain error. United States v. Mendez-Ortiz, 810 F.2d 76 (6th Cir. 1986), cert. denied, 480 U.S. 922 (1987).

We have recognized that "[t]he plain error doctrine is to be used 'only in exceptional circumstances' and only where the error is so plain that 'the trial judge and the prosecutor were derelict in countenancing it.'" Id. at 78. Moreover, "[w]e consider whether the instructions, when taken as a whole, were so clearly wrong as to produce a grave miscarriage of justice." United States v. Sanderson, 966 F.2d 184, 187 (6th Cir. 1992).

When one count of an indictment charges that a defendant committed an offense by "multiple alternative 'conceptually' distinct acts," the defendant can request that the court give the jury an augmented unanimity instruction, i.e., one that tells them that, with regard to this particular count, they must all agree that the defendant committed one of those distinct acts. United States v. Duncan, 850 F.2d 1104, 1110 (6th Cir. 1988). With regard to specific, or augmented unanimity instructions, this court has recognized that the instruction is not necessary "unless 1) a count is extremely complex, 2) there is variance between the indictment and the proof at trial, or 3) there is a tangible risk of jury confusion." Sanderson, 966 F.2d at 187. Contrary to Defendants' assertions, this court's decision in Duncan does not require a court to sua sponte instruct the jury on specific unanimity when more than one basis for conviction is presented in a single count. Rather, we have consistently recognized that the need arises when it is shown that there is a "genuine risk that the jury is confused or that a conviction may occur as the result of different jurors concluding that a defendant committed different acts." United States v. Sims, 975 F.2d 1225, 1241 (6th Cir. 1992), cert. denied, ___ U.S. ___, 113 S. Ct. 1315 (1993).
In *Duncan*, the court held that an augmented unanimity instruction should have been given because the court had been apprised of the unanimity problem in pretrial motions and by "a mid-deliberation question from the jury raising the genuine possibility that conviction could occur as the result of different jurors using a different false statement as the underlying factual predicate for guilt." *Duncan*, 850 F.2d at 1105. Defendants have not demonstrated that there was a tangible risk of jury confusion here. Thus, this case is easily distinguished from *Duncan*.

Furthermore, counts 2, 3, 6 and 9 were not complex, and there was no variance between the indictment and the proof at trial. Accordingly, none of the circumstances existed that would give rise to the need for a specific unanimity instruction. Consequently, we conclude that the district court did not commit error when it gave general instructions on unanimity. Furthermore, considering the subject matter of each GIF file and videotape listed in counts 2, 3, 6 and 9, we find it unlikely that the jury would have had any trouble reaching unanimity on the fact that one item described in each of those counts was obscene.

E.

We next address the Defendants' argument that the district court erred when it instructed the jury that the government was not required to present expert testimony regarding the prurient appeal of the materials at issue here.[9]

You have heard testimony from an expert witness presented on behalf of the defendants. An expert is allowed to express his opinion on those matters about which he has special knowledge and training. Expert testimony is presented to you on the theory that someone that is experienced in the field can assist you in understanding the evidence or in reaching an independent decision on the facts. There is no requirement, however, that expert testimony be presented in an obscenity case. The government need not produce expert evidence that the materials are obscene, but may rely on the computer generated images and videotapes themselves for its argument that the materials are obscene. Under the first prong of the *Miller* obscenity test, the jury must consider whether the allegedly obscene material "appeals to the prurient interest." *Miller*, 413 U.S. at 24.

The computer-generated images and videotapes involved here portrayed bestiality, incest, rape, and sex scenes involving defecation, urination, and sado-masochistic abuse. Defendants argue that the Government is required to present expert testimony when sexually-explicit material is directed at a deviant group. We disagree. Neither the United States Supreme Court nor this court has adopted any such *per se* rule.

The Supreme Court has consistently recognized that "[e]xpert testimony is not necessary to enable the jury to judge the obscenity of material which . . . has been placed into evidence." *Hamilton v. United States*, 418 U.S. 87, 100 (1974) (citing *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, 56 (1973), *Kaplan v. California*, 413 U.S. 115, 120-21 (1973), *Ginzburg v. United States*, 383 U.S. 463, 465 (1966)). In *Paris Adult Theatre I*, the Court observed that the allegedly obscene materials, "obviously, are the best evidence of what they represent" and have been consistently recognized as "sufficient in themselves for the determination of the question." 413 U.S. at 56 (quoting *Ginzburg*, 383 U.S. at 465). The *Paris I* Court further elaborated that:

[t]his is not a subject that lends itself to the traditional use of expert testimony. Such testimony is usually admitted for the purpose of explaining to lay jurors what they otherwise could not understand. No such assistance is needed by jurors in obscenity cases; indeed the "expert witness" practices employed in these cases have often made a mockery out of the otherwise sound concept of expert testimony.

*Id.* at 56, n.6 (citations omitted).
The Court has explicitly reserved judgment on the issue whether expert testimony is required in the "extreme case" where "contested materials are directed at such a bizarre deviant group that the experience of the trier of fact would be plainly inadequate to judge whether the material appeals to the prurient interest." *Id.* In *Pinkus v. United States*, 436 U.S. 293 (1978), the Court once again reserved judgment on this question, finding that it was not presented with the "extreme case" referenced in *Paris I* because there was expert testimony in evidence which, when "combined with the exhibits themselves, sufficiently guided the jury." *Pinkus*, 436 U.S. at 303.

Expert testimony on prurient appeal to deviant groups was also presented in this case. Defendants' expert, Dr. Victor Pascale, a licensed clinical psychologist, testified at trial about how certain groups of individuals can become sexually aroused by objects or conduct not normally thought of as sexual in nature, i.e., the use of whips, cross-dressing, urination, defecation, infliction of pain (sado-masochism), and voyeurism. Thus, as in *Pinkus*, we find that the expert testimony, when combined with the allegedly obscene materials themselves, was sufficient to guide the jury with regard to prurient appeal.

Defendants rely heavily on decisions from the Second Circuit. *See United States v. Klaw*, 350 F.2d 155 (2nd Cir. 1965); *United States v. Petrov*, 747 F.2d 824 (2nd Cir. 1984), *cert. denied*, 471 U.S. 1025 (1985). In *Petrov*, however, the court concluded that *Klaw* is "properly understood to require expert testimony that material appeals to the prurient interest of a deviant group only when the material portrays conduct not generally understood to be sexual." *Id.* at 836. Furthermore, the *Petrov* court concluded that expert testimony is "not required to establish the prurient appeal of photographs depicting bestiality." *Id.* at 837. The court further clarified that although *Klaw* required expert testimony on depictions of sado-masochistic activity, the requirement was met where the defendant's expert testified on cross-examination that such materials would appeal to the sexual interest of a small minority of individuals even though they would not appeal to the average person. *Id.* at 830-31. Thus, *Petrov* does not compel a different result, and this court concludes that the challenged jury instruction was not erroneous.

**F.**

A required element of § 1465 is that the defendant knowingly "used a facility or means of interstate commerce" for the purpose of transporting or transmitting obscene material. Defendants argue that the district court's instruction, that "facility or means of interstate commerce" includes "any method of communication between different states," improperly expanded the meaning of this criminal statute. Defendants failed to object to the instruction, therefore, it is examined for plain error. We conclude that there is no plain error here.

Contrary to Defendants' argument, the instruction finds support in 2 Devitt, Blackmar and O'Malley, *Federal Jury Practice and Instruction, Criminal*, (4th Ed. 1990), § 46.06 at 664, which provides:

The term "uses any facility in interstate . . . commerce" means employing or utilizing any method of communication or transportation between one state and another. The term "uses any facility in interstate . . . commerce", for example, includes the use of the telephone and mails.

**G.**

Defendants claim they were denied due process of law and a fair trial by the admission of uncharged GIF files and descriptions of uncharged materials at their trial. We will not disturb the district court's admission of this evidence and its determinations of relevancy absent a clear abuse of discretion. *United States v. Seago*, 930 F.2d 482, 494 (6th Cir. 1991). We also apply an abuse of discretion standard to the district court's decision in balancing the potentially unfair prejudicial impact of evidence against its probative value. *United States v. Feinman*, 930 F.2d 495, 499 (6th Cir. 1991). In reviewing how such a balance is weighed, "the appellate court must view the evidence in the light most favorable to its proponent, giving "the evidence its maximum reasonable probative force and its minimum reasonable prejudicial value."

Defendants complain that the district court erred when it allowed the Government to introduce 31 uncharged GIF files, portions of 2 uncharged videos, and the AABBS' descriptions of uncharged GIF files and videotapes at trial. They assert that the material had no probative value, and its introduction served only to unfairly prejudice the jury. Based on our review of the record, we find no abuse of discretion.

With regard to the videotapes, the record reveals that the district court considered whether the probative value of two minutes of one of the three "child nudist" videotapes sent by Defendant Robert Thomas to Dirmeyer was substantially outweighed by the danger of unfair prejudice. F.R.E. 401, 403. Despite an objection from Defendants' counsel, the district court ruled that the material was probative to the issue of Mr. Thomas' predisposition in light of his entrapment defense to count 11, charging him with knowing receipt of child pornography. We find no error in the admission of the videotapes since they were properly introduced in response to the entrapment defense.

Defendants' claim that the district court erred when it permitted the jury to see 31 uncharged GIF files is likewise without merit. Each of the GIF file images was made from the charged videotapes by stopping the tapes at a certain point, making a still frame or photograph, and then scanning it onto the AABBS and making it available for distribution as a separate item. Because the entire videotape was properly admitted and viewed by the jury, we reject Defendants' claim of unfair prejudice.

Defendants also complain that the district court erred by allowing the jury to hear sexually-explicit descriptions of other uncharged GIF files and videotapes. Contrary to Defendants' contention, this material did have probative value, i.e., it was relevant to establishing scienter and pandering. Defendants posted these graphic descriptions in the public areas of the AABBS, and this was one way they advertised for members. See Mishkin v. New York, 383 U.S. 502 (1966); Pinkus, 436 U.S. at 303. Accordingly, we reject Defendants' argument that the above evidence was clearly more prejudicial than probative under F.R.E. 403, and find no abuse of discretion in its admission under F.R.E. 401.

H.

Defendants next contend that they were denied effective assistance of counsel at their trial because their retained counsel failed to: (1) move for dismissal based on Carlin; (2) object to the admission of evidence at trial; (3) move for judgment of acquittal based on the government's requirement to provide expert testimony regarding "prurient appeal" to deviant groups; (4) recognize the conflict of interest inherent in his dual representation of both Defendants; (5) sever the child pornography count; (6) file a suppression motion; (7) request discovery; (8) challenge the indictment as duplicative; (9) move for a mistrial; (10) submit a theory-of-the-case instruction; (11) introduce comparable sexually-explicit videotapes available in Memphis; and (12) with regard to Carleen Thomas, failed to move for a judgment of acquittal at the close of the government's case for lack of evidence of scienter and then called her to the stand when her testimony could only incriminate her.

As a general rule, this court "will not review claims of ineffective counsel that are raised for the first time on appeal." United States v. Seymour, 38 F.3d 261, 263 (6th Cir. 1994). These claims are "'best brought by a defendant in a post-conviction proceeding under 28 U.S.C. § 2255 so that the parties can develop an adequate record on the issue.'" Id. (quoting United States v. Daniel, 956 F.2d 540, 543 (6th Cir. 1992)). We consider such claims on direct appeal only where the record has been sufficiently developed so as to allow us to evaluate counsel's performance. Seymour, 38 F.3d at 263. We find that the record here is not adequately developed for us to consider the ineffective assistance of counsel claims asserted above.

We will, however, consider Defendant Carleen Thomas' argument that she was denied effective assistance of counsel because the district court refused her request for separate counsel without adequate inquiry as to her reasons. Unlike the above claims, we find the record below is sufficiently developed to
address this issue.

Carleen Thomas first raised her request for separate counsel on the day of trial. The Government informed the district court that Defendants had previously been informed of their right to separate counsel but they had waived that right. While considering Carleen Thomas' late request, the district court made additional inquiries and reviewed the record to determine whether she had indeed been informed of, and had waived, that right. The inquiry revealed both events had occurred. The district court refused to delay the trial that was set to begin immediately but did offer to arrange for separate standby counsel for Carleen Thomas. The court also informed Carleen Thomas that, because she was not indigent, she would have to reimburse this counsel at the rate charged by court-appointed attorneys. After considering the court's offer, Carleen Thomas stated on the record that she wished to continue with Mr. Williams as her retained counsel. In light of the above, we reject Carleen Thomas' claim.

I.

Defendants' final argument challenges the district court's denial of a two-level reduction in their sentences for acceptance of responsibility. They claim they are entitled to the reduction because they fully acknowledged their conduct in running the AABBS. The sentencing court's finding regarding acceptance of responsibility is entitled to great deference and is reversed only if found to be clearly erroneous. See United States v. Ivery, 999 F.2d 1043, 1045 (6th Cir. 1993); see also U.S.S.G. § 3E1.1(a), comment, n.5.

U.S.S.G. § 3E1.1(a) provides for a two-level reduction for a defendant who "clearly demonstrates acceptance of responsibility." To qualify for this reduction, Defendants were required to show by a preponderance of the evidence that they had accepted responsibility for the crime committed. United States v. Williams, 940 F.2d 176 (6th Cir.), cert. denied, 502 U.S. 1016 (1991). U.S.S.G. 3E1.1(a), comment, n.2 clarifies that the reduction is "not intended for a defendant who puts the government to its burden of proof at trial by denying the essential factual elements of guilt, is convicted, and only then admits guilt and expresses remorse." This comment further clarifies that only in "rare situations" will the adjustment apply after a trial and verdict of guilt, e.g., where the defendant makes a challenge to the applicability of a statute to his conduct. Defendants assert that they fit the "rare situation" and should not have been denied the reduction.

The sentencing judge, however, stated more than one ground for denying the two-level reduction. She noted that neither Defendant acknowledged the character of the materials found to be obscene. In addition, she found no indication that either of them had put aside making their living through the same means. U.S.S.G. § 3E1.1(a), comment n.1(b) lists voluntary termination or withdrawal from criminal conduct as a factor to be considered by the court. This court has recognized that the two-level adjustment is properly denied under circumstances where the defendant continues conduct that is the same type as the underlying offense. See United States v. Reed, 951 F.2d 97, 99-100 (6th Cir. 1991), cert. denied, 503 U.S. 996 (1992); United States v. Snyder, 913 F.2d 300, 305 (6th Cir. 1990), cert. denied, 498 U.S. 1039 (1991). Accordingly, we hold that the sentencing court's denial of the two-level reduction was not clearly erroneous.

III.

For the foregoing reasons, this court AFFIRMS Robert and Carleen Thomas' convictions and sentences.

Case in RTF Format
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

INTERMATIC INCORPORATED, Plaintiff,

v.

DENNIS TOEPPEN, Defendant.

No. 96 C 1982

Dated: Oct. 3, 1996

Judge Ann C. Williams
Magistrate Judge Morton Denlow

TO: THE HONORABLE ANN C. WILLIAMS
UNITED STATES DISTRICT JUDGE

REPORT AND RECOMMENDATION

Welcome to cyberspace! This case presents the Court with the increasingly important issue of whether and how federal and state trademark laws apply to govern names selected by users for their Internet website. As the Internet grows in prominence as a venue for business, the courts will be called upon to apply traditional legal principles to new avenues of commerce. This is such a case.

Plaintiff Intermatic Incorporated ("Intermatic"), brings this action in seven counts against defendant Dennis Toeppen ("Toeppen"). Intermatic alleges that Toeppen's use of the Internet domain name "Intermatic.com" violates sections 32(1) (Federal Trademark Infringement) (count I), 43(a) (Federal Unfair Competition) (count II), and 43(c) (Federal Trademark Dilution Act of 1995) of the Lanham Act (count III). 15 U.S.C. Section 1114(1); 15 U.S.C. Section 1125(a); and 15 U.S.C. Section 1125(e) respectively. Intermatic also alleges that Toeppen's conduct violates the Illinois Anti-Dilution Act, 765 ILCS 1035/1 et. seq. (count IV); the common law of unfair competition (count V); the Uniform Deceptive Trade Practices Act, 815 ILCS 510/1 et. seq. (count VI); and the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2. (count VII). Toeppen denies that his conduct is unlawful.

Intermatic and Toeppen have filed cross-motions for summary judgment on all seven counts. The Court held extensive oral argument on August 29, 1996 and has reviewed the briefs, stipulations, affidavits and exhibits submitted by the parties. For the reasons set forth below, the Court recommends that Intermatic's motion for summary judgment be granted as to counts III and IV (the "Dilution counts") and be denied as to the remaining counts. The Court recommends that Toeppen's motion be denied as to all counts.

I. BACKGROUND FACTS
A. The Parties.

Intermatic is a Delaware corporation having a place of business in Spring Grove, Illinois. Intermatic has been doing business under the name INTERMATIC since 1941. Intermatic has 37 offices throughout the United States and has been in business in Illinois since 1892. Intermatic is a manufacturer and distributor of a wide variety of electrical and electronic products, including computerized and programmable timers and other devices which are sold under the name and trademark INTERMATIC.

Intermatic's sales and advertising of INTERMATIC labeled products have been continuous since the 1940's. (SF para. 6). In the last 8 years, its sales in the U.S. have exceeded $850 million. Id.

Intermatic's products prominently bear the INTERMATIC name and trademark, and well over 100 million units have been installed in homes and businesses throughout the United States. (SF paras. 6, 9).

Advertising and promotional expenditures for products bearing the INTERMATIC mark for the last 8 years have exceeded $16 million. (SF para. 7). Intermatic's co-op advertising consists of approximately 700 print ads per year, with each displaying the INTERMATIC mark. Intermatic also advertises and promotes its INTERMATIC products, mark and name by way of trade shows throughout the United States, magazines, point-of-purchase displays, brochures, radio, and television. (12 M paras. 12, 31, 32).

Defendant Toeppen resides in Champaign, Illinois, where he operates an Internet service provider business known as Net66. Toeppen has registered approximately 240 Internet domain names without seeking the permission from any entity that has previously used the names he registered, because he contends that no permission was or is necessary. Among the domain names which he has registered are the following well known business names:

- deltaairlines.com
- greatamerica.com
- britishairways.com
- neiman-marcus.com
- crateandbarrel.com
- northwestairlines.com
- ramadainn.com
- ussteel.com
- eddiebauer.com
- unionpacific.com

One of Toeppen's business objectives is to profit by the resale or licensing of these domain names, presumably to the entities who conduct business under these names.

B. Intermatic's Trademarks.

Intermatic owns five incontestable trademark registrations issued by the U.S. Patent and Trademark Office for its INTERMATIC mark. (SF para. 4, Ex. 2).

Intermatic is the exclusive owner of the INTERMATIC trademark and trade name, and there are no known third party uses of INTERMATIC in the U.S. (SF paras. 4, 11, Ex. 2). Prior to registering the intermatic.com domain name, Toeppen had never used the term intmatic for any purpose.

C. The Internet.

1. Domain Names.

The Internet is a vast and expanding network of computers and other devices linked together by various telecommunications media, enabling all the computers and other devices on the Internet to exchange and share data.
The Internet provides information about a myriad of corporations and products, as well as educational, research and entertainment information and services. An estimated 30 million people worldwide use the Internet with 100 million predicted to be on the "net" in a matter of years.[2]

A computer or device that is attached to the Internet is often referred to as a "host." In order to facilitate communications between hosts, each host has a numerical IP (Internet protocol) address.[3] The IP address is comprised of four groups of numbers separated by decimals. For example, the IP address of one of Toeppen's host computers is 206.139.80.66. Each host also has a unique "fully qualified domain name." The "fully qualified domain name" may not be repeated in the Internet. In the case of 206.139.80.66, the "fully qualified domain name" is "winslow.net66.com".

In its most generic form, a fully qualified domain name consists of three elements. Taking "winslow.net66.com" as an example, the three elements are the hostname ("winslow"), a domain name ("net66") and a top level domain ("com"). A given host looks up the IP addresses of other hosts on the Internet through a system known as domain name service.

Domain name service is accomplished as follows: The Internet is divided into several "top level" domains. For example, "edu" is a domain reserved for educational institutions, "gov" is a domain reserved for government entities and "net" is reserved to networks. Although "com" is short for "commercial," it is a catchall domain and the only one generally available to Internet users that have no special attributes i.e., they are not a school or a government office or a network. Each domain name active in a given top-level domain is registered with the top level server which contains certain hostname and IP address information.

In order to access the Internet, most users rely on programs called "web browsers." Commercially available web browsers include such well-known programs as Netscape and Mosaic. If an Internet user desires to establish a connection with a web page hosted at winslow.net66.com, the Internet user might enter into a web browser program the URL "http://www.net66.com." (URL stands for uniform resource locator.) The first element of the URL is a transfer protocol (most commonly, "http" standing for hypertext transfer protocol). The remaining elements of this URL (in this case, "www" standing for World Wide Web and "net66.com") are an alias for the fully qualified domain name of the host winslow.net66.com. Once a URL is entered into the browser, the corresponding IP address is looked up in a process facilitated by a "top-level server." In other words, all queries for addresses are routed to certain computers, the so-called "top level servers". The top level server matches the domain name to an IP address of a domain name server capable of directing the inquiry to the computer hosting the web page. Thus, domain name service ultimately matches an alphanumeric name such as www.net66.com with its numeric IP address 206.139.80.66.

2. Registration of Domain Names.

Domain names using the suffix ".com" are established by registration with an organization called Network Solutions, Inc. ("NSI"). Registration of the other available top-level domain names, "edu," "gov" and "net", is handled by other organizations. With some limitations, NSI will register any combination of up to 24 alphanumeric characters as a domain name on a first-come, first-served basis to anyone who has access to at least two domain name servers. A domain
name server is a host computer with software capable of responding to domain name inquiries and accessible on a full-time basis to other computers on the Internet. Registering a domain name is the step that allows the top-level servers within the Internet to know where the domain name servers or hosts associated with those domain names are located in the Internet. The cost for a domain name registration is currently $100. Domain name service can be operated by the domain name holder or obtained from any entity with the proper computer equipment, including hundreds of Internet service providers.

3. Web Pages.

One way to establish a presence on the Internet is by placing a web page, which is, ultimately, a computer data file on a host operating a web server within a given domain name. When the web server receives an inquiry from the Internet, it returns the web page data in the file to the computer making the inquiry. The web page may comprise a single line or multiple pages of information and may include any message, name, word, sound or picture, or combination of such elements. Most web browsers will show somewhere on the screen the domain name of the web page being shown and will automatically include the domain name in any printout of the web page. There is no technical connection or relationship between a domain name and the contents of the corresponding web page.

There are a number of ways for an Internet user to find a web page. Web browsers feature access to various indexes, commonly referred to as search engines. Well-known indexes include InfoSeek Guide, Lycos, Magellan, ExCite and Yahoo. These indexes will allow the user to enter a name or a word or a combination of words, much like a Lexis or WestLaw search, and will return the results of the search as a list of "hyperlinks" to webpages that have information within or associated with the document comprising the page responding to the search.

4. Hyperlinks.

A hyperlink is a link from one site on the Internet to a second site on the Internet. "Clicking" on a designated space on the initial page which references the subsequent site by a picture, by some highlighted text or by some other indication will take a person viewing the initial web page to a second page. In addition to their use in indexes, hyperlinks are commonly placed on existing web pages, thus allowing Internet users to move from web page to web page at the click of a button, without having to type in URLs.

Hyperlinks can be and commonly are established without reference to the domain name of the second site. A hyperlink for the Champaign-Urbana map page might be a picture of a map or a statement such as "a map of Champaign-Urbana" or, more simply, "Champaign-Urbana." A hyperlink is not technically related to a domain name and therefore it can be identical to an existing domain name without conflicting with that domain name. For example, were Intermatic to establish an Intermatic home page at http://www.xyz.com, any number of indexes could be employed and hyperlinks could be established to bring up the page through use of the word INTERMATIC.

D. The Dispute.

In December of 1995, Toeppen applied for registration of the domain name http://www.intermatic.com ("intermatic.com") and NSI registered the domain
name to Toeppen's domain name servers. A given domain name, the exact alphanumeric combination in the same network and using the same suffix, can only be registered to one entity. Intermatic subsequently attempted to register the same domain name and was prevented from registering "intermatic.com" as its domain name because of Toeppen's prior registration of that domain name.

Intermatic also became aware that Toeppen was using the mark "Intermatic" in connection with the sale of a computer software program. Upon discovery of Toeppen's prior registration and use of the Intermatic mark, Intermatic made a written demand on Toeppen that he relinquish or assign the "intermatic.com" domain name registration and discontinue use of the Intermatic mark. Toeppen agreed to discontinue using the Intermatic mark for his software product but refused to give up the "intermatic.com" domain name registration. In response to a formal request by Intermatic, NSI put Toeppen's registration on hold in April of 1996.

As long as Mr. Toeppen is allowed to retain the "intermatic.com" registration, Intermatic will be unable to acquire "intermatic.com" as an Internet domain name or use "intermatic.com" as an e-mail address on the Internet. However, Intermatic is technically capable of establishing its web page at another domain name, including, for example, "intermatic-inc.com" and it is technically capable of establishing at any available domain name a web page featuring the INTERMATIC mark and any other Internet-related marketing or business information. To date, Intermatic has not chosen to reserve any other domain name or to take any other action to establish a presence on the Internet. However, some of its distributors have placed Intermatic information on the Internet.

Until NSI placed the intermatic.com domain name on hold, Toeppen maintained intermatic.com as an active domain name on the Internet. Although he initially set up a web page regarding a software program he was developing and intended to call "Intermatic," Toeppen removed that page (which was available for less than a week) and dropped the proposed name for his software in response to demand from Intermatic. No software programs were ever sold. He then instituted as a web page a map of Champaign-Urbana, the community where Toeppen resides.

When Toeppen became aware of Intermatic's efforts to have the intermatic.com domain name placed on hold, he changed the web page associated with intermatic.com to bear the caption "Champaign-Urbana Map Page/has Moved To www.c-u.com." Toeppen moved the map and put the forwarding address on the intermatic.com page so that Internet users could update relevant hyperlinks before the NSI freeze simply locked them out of the page, as is now the case. Presently, entering intermatic.com will return a message that there is no functional domain name server at that domain name.

At no time did Toeppen use intermatic.com in connection with the sale of any available goods or services. At no time has Toeppen advertised the intermatic.com domain name in association with any goods or services. Presently, the intermatic.com domain name is not available for use by any party. Toeppen did not seek permission from Intermatic to use the intermatic.com domain name because he believes that no permission was or is necessary. Intermatic disagrees. This litigation ensued.

II. SUMMARY JUDGMENT STANDARD

Summary judgment "shall be rendered forthwith if the pleadings,
answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56(c).


When reviewing the record on summary judgment, the court must draw all reasonable inferences in the light most favorable to the nonmovant. Hill v. Burrell Communications Group, Inc., 67 F.3d 665, 667 (7th Cir. 1995). To avert summary judgment, however, plaintiff "must do more than simply show that there is some metaphysical doubt as to the material facts." Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp., 475 U.S. 574, 586, 106 S.Ct. 1348, 1356, (1986). A dispute about a material fact is genuine only if the evidence presented is such that a reasonable jury could return a verdict for the nonmovant. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248, 106 S.Ct. 2505, 2510 (1986). A summary judgment proceeding is not a vehicle for the resolution of factual disputes; it is designed to determine whether there is any material dispute of fact that requires a trial. Id. If no reasonable jury could find for the party opposing the motion, it must be granted. Hedberg v. Indiana Bell Tel. Co., 47 F.3d 928, 931 (7th Cir. 1995). The fact that the parties have filed cross-motions for summary judgment does not necessarily mean that summary judgment must be entered for one side. Lac Courte Oreilles Band of Lake Superior Chippewa Indians v. Voigt, 700 F.2d 341, 349 (7th Cir. 1983) (" ... filing of cross-motions does not automatically empower district court to dispense with assessment of whether material fact questions exist.").

III. LEGAL DISCUSSION

This case involves a dispute over the ownership of a highly prized Internet address. The issue is whether the owner of the Intermatic trademark may preclude the use of the trademark as an Internet domain name by defendant Toeppen, who had made no prior use of the Intermatic name prior to registering it as an Internet domain name. This case does not involve competing claims to the same name by parties who have actively used the same name in their business, such as the use of the term "United" by United Airlines, United Van Lines, United Mine Workers Union and the United Way.

Toeppen is what is commonly referred to as a cyber-squatter. Miller, Cyber Squatters Give Carl's Jr., Others Net Loss, Los Angeles Times, 1996 WL11004750. These individuals attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark. While many may find patenty offensive the practice of reserving the name or mark of a federally registered trademark as a domain name and then attempting to sell the name back to the holder of the trademark, others may view it as a service. Regardless of one's views as to the morality of such conduct, the legal issue is whether such conduct is illegal. Cyber-squatters such as Toeppen contend that because they were the first to register the domain name through NSI it is theirs. Intermatic argues that it is entitled to protect its valuable trademark by preventing Toeppen from using "intermatic.com" as a domain name.

The practical effect of Toeppen's conduct is to enjoin Intermatic from using its trademark as its domain name on the Internet. Unlike the typical trademark dispute, where both parties are using the name simultaneously and arguing whether confusion exists, the current configuration of the Internet allows only one party to use the "intermatic.com" domain name. Because the Internet assigns the top-level domain name .com to commercial and non-commercial
users, there does not currently appear to be a way in which both Intermatic and Toeppen can both use the internatic.com name.

Congress and the states have been slow to respond to the activities of the cyber-squatters. Some commentators take an extremely dim view of their activities. As one commentator has noted: "There is no doubt that some of these pirates, if not most, anticipated a lottery-like bonanza, selling the domain registration to the trademark owner or canceling it in return for a huge amount of money." 1 Gilson, Trademark Protection and Practice, Section 5.11[4], p. 5-237 (1996). "Dozens of companies, including Taco Bell, MTV, Kentucky Fried Chicken and others have had to cajole, pay thousands of dollars or even sue to gain the rights to domain names that match trademarks they have spent millions of dollars cultivating and protecting," Miller, Cyber Squatters Give Carl's Jr., Others Net Loss. Los Angeles Times, 1996 WL 11004750. However, becoming rich does not make one's activity necessarily illegal. Speculation and arbitrage have a long history in this country.

For the reasons set forth below, the Court recommends that Intermatic's motion for summary judgment be granted in part as to the Dilution counts III and IV and denied as to the remaining counts and Toeppen's motion be denied as to all counts. We will begin our analysis with a discussion of Intermatic's trademark and unfair competition claims (section IV) and we will then turn to its trademark dilution claims (section V).

IV. INTERMATIC'S TRADEMARK INFRINGEMENT AND UNFAIR COMPETITION CLAIMS -- LIKELIHOOD OF CONFUSION.

Our discussion begins with an analysis of Intermatic's trademark and unfair competition claims. Intermatic asserts that it is entitled to summary judgment on all counts by showing the likelihood of confusion resulting from Toeppen's use of Intermatic's trademark as a domain name. In order to prevail under the federal trademark infringement claim, the federal unfair competition claim, and the state deceptive trade practices and unfair competition claims, (Counts I, II, V, VI, and VII), Intermatic need only prove that: 1) it owns prior rights in the INTERMATIC mark; and 2) Toeppen's use of "internatic.com" is likely to cause consumer confusion, deception or mistake. Dorr-Oliver, Inc. v. Fluid-Quip, Inc., 94 F.3d 376 (7th Cir. 1996).[4]

Intermatic's name and prior rights over Toeppen to use the INTERMATIC name are clear. Intermatic's first use of the INTERMATIC name and mark predates Toeppen's first use of "internatic.com" by more than fifty years. Also, it is undisputed that Intermatic holds a valid registration for the trademark INTERMATIC.

The Seventh Circuit has held that the following seven factors should be weighed to determine if there is a likelihood of confusion: 1) the degree of similarity between the marks in appearance and suggestion; 2) the similarity of products or services for which the name is used; 3) the area and manner of concurrent use; 4) the degree of care likely to be exercised by consumers; 5) the strength of the complainant's mark; 6) actual confusion; and 7) an intent on the part of the alleged infringer to palm off his products as those of another. Forum Corp. of North Am. v. Forum Ltd., 903 F.2d 434, 439 (7th Cir. 1990). The test is not whether the public would confuse the marks, but whether the viewer of an accused mark would be likely to associate the product or service with which it is connected with the source of products or services with which an earlier
mark is connected. *Nike, Inc. v. "Just Did It" Enterprises*, 6 F.3d 1225, 1228-29 (7th Cir. 1993). Where factual issues exist on these criteria, the Seventh Circuit has clearly stated that summary judgment is inappropriate. *McGraw-Edison Company v. Walt Disney Products*, 787 F.2d 1163, 1173 (7th Cir. 1987) ("the district court erred in concluding as a matter of law that no likelihood of confusion exist and in granting summary judgment in favor of defendants on count I"); *Nike, Incorporated v. "Just Did It" Enterprises*, 6 F.3d 1225 (7th Cir. 1993) (reversing district court grant of summary judgment and holding that genuine issue of material fact existed as to whether parody of "Nike," "Just Do It" and swoosh symbol trademarks was likely to confuse consumers).

1. **Similarity of Marks**

In this case, Toeppen's use of "intermatic.com" is similar to the federally registered name and mark of INTERMATIC because it contains the term "intermatic." Each of the five registered INTERMATIC trademarks contain the Intermatic name. (SF para. 4 and Ex. 2 thereto).

2. **Similarity of Products or Services**

There is no similarity between the products and services that Toeppen and Intermatic provide. Toeppen's web page contained a map of the city of Urbana, whereas Intermatic's web page would presumably contain product information or catalogs of the various Intermatic products. At the present time, Intermatic has chosen to await the outcome of this litigation before initiating its own Internet web page. More importantly though, Toeppen is willing to be enjoined from using the website for the sale of any product or service thereby guaranteeing that his use would be entirely dissimilar from Intermatic's use.

3. **The Area and Manner of Use**

This factor requires the Court to "consider whether there is a relationship in use, promotion, distribution, or sales between the goods or services of the parties." *Forum Corp. of North Am. v. Forum, Ltd.*, 903 F.2d 434, 442 (7th Cir. 1990). Also, a trademark protects the owner against not only its use upon the articles to which he has applied it but also upon such other articles as might naturally be supposed to come from him. *Nike, Inc. v. "Just Did It" Enterprises*, 6 F.3d 1225, 1228-29 (7th Cir. 1993). Toeppen will not be selling any goods or services through the intermatic.com domain.

Both parties are attempting to establish a presence on the Internet through the creation of a web page. The distribution channel in this case is cyberspace. As consumers "surf the net" they seek out information on a plethora of subjects or companies. Companies around the globe are scrambling to establish their presence on the Internet. It is axiomatic that companies seek to register their trademarks as domain names so that consumers can easily find information about them or their products and services. However, at the present time, there is no area and manner of concurrent use. There is no bar to Intermatic setting up a web page under a name other than intermatic.com. Because Intermatic has not set up its own web page, it is unable to demonstrate any relationship in use, promotion, distribution or sales between the goods or services of the parties.

4. **Degree of Care Likely To Be Exercised By Consumers**

The record contains no information regarding consumer behavior on the Internet. The Court finds that the degree of care to be exercised by consumers
raises a question of fact. The consumers in this case are individuals that log onto the Internet to seek information, products, or services. There has been no evidence presented as to the degree of care that could be expected among the average Internet user. The Court cannot simply infer what degree of care would be used by consumers. Because this matter is before the Court on summary judgment, the Court infers that a fact question exists as to whether a web surfer who logged onto the intmatic.com web page and found a map of Urbana, Illinois would associate that page with Intmatic. Nike, Inc. v. "Just Did It" Enterprises, 6 F.3d 1225, 1230-1 (7th Cir. 1993). Thus, the Court finds that a fact question exists on this issue.

5. Strength of Intmatic's Mark

Toeppen does not contest the fact that Intmatic's mark is strong. The Court finds that the mark is strong and entitled to broad protection as a matter of law. As the Seventh Circuit noted in Polaroid Corp. v. Polaraid Inc., 319 F.2d 830, 831 (7th Cir. 1963), a trademark or trade name that is a coined or invented word which has never been used as a trade name or trademark by any other entity acquires the status of a famous-brand trademark. The following language from Polaroid is applicable to the case at bar: "in the instant case plaintiff's trademark and trade name was original -- it was coined and invented -- and was a strong name exclusively appropriated by plaintiff. It was a name which through much effort and the expenditure of large amounts of money had acquired a widespread reputation and much good will, which plaintiff should not be required to share with defendant." Id at 837.

6. Actual Confusion

There has been no evidence presented of actual confusion. Intmatic states that the use of the "intmatic.com" domain name in and of itself would cause confusion. However, this is a question of fact to be determined. Nike, Inc. v. "Just Did It" Enterprises, 6 F.3d 1225, 1231 (7th Cir. 1993).

7. Toeppen's Intent

Intmatic argues that Toeppen's registration of more than 200 domain names is indicia of willful intent. However, Toeppen argues that he was motivated in part to test the legality of arbitraging domain names. This is a relatively new area of law and Toeppen is free to test the waters. There has been no evidence that Toeppen intended to pass off any of his products or services as Intmatic's. Neither the software nor the map of Urbana are in anyway similar to Intmatic's products. He immediately ceased to market the software under the Intmatic name when contacted by Intmatic's counsel. Whether Toeppen's registration of several domain names is sufficient to rise to the level of willful intent is also a question of fact. Id. at 1231-32.

Therefore the Court recommends that since there are questions of fact as to a likelihood of confusion, the parties' cross motions for summary judgment as to counts I, II, V, VI, and VII should be denied.

V. INTERMATIC'S DILUTION CLAIMS

The parties also move for summary judgment on the Dilution claims. The issue squarely presented is whether the Federal Trademark Dilution Act of 1995 and the Illinois Anti-Dilution Act protect Intmatic from having its federally registered trademarks used as a domain name by Toeppen. For the reasons set
forth below the Court holds that Toeppen's action in registering and using "intermatic.com" as a domain name violates section 43(c) of the Lanham Act and the Illinois Anti-Dilution Act because it lessens the capacity of a famous mark, Intermatic, to identify and distinguish goods or services as a matter of law.

A. History of Dilution Statutes.

The concept of trademark dilution dates back[5] to an article written by Frank I. Schechter and published in the Harvard Law Review in 1927. *The Rational Basis of Trademark Protection*, 40 Harv. L. Rev. 813 (1927). Schechter explained that the true function of a trademark is "to identify a product as satisfactory and thereby to stimulate further purchases by the consuming public." Id. at 818. Schechter rejected the theory that the exclusive role of a trademark was to serve as a source identifier. He argued that the true function of a mark is to identify a product as satisfactory and thereby stimulate further purchases by the consuming public. He argued that injury occurs to a trademark owner whenever a trademark is used by another, even when used on non-competing goods. He explained that an injury to the trademark owner occurs when there is "a gradual whittling away or dispersion of the identity and hold upon the public mind of the mark or name by its use upon non-competing goods. The more distinctive or unique the mark, the deeper is its impress upon the public consciousness, and the greater is its need for protection against vitiation or dissociation from the particular product in connection with which it has been used." *Id.* at 825. This argument that the trademark laws should protect owners in connection with non-competing goods was novel. Attempts to enact a federal dilution statute in 1932 were unsuccessful. See, *Gilson*, at p. 3.

Massachusetts became the first state to adopt a trademark dilution law in 1947. Since then, over twenty other states have followed suit. In addition, at least three states, Michigan, New Jersey and Ohio recognize dilution as a common law cause of action. Section 12 of the Model State Trademark Act contains the following dilution provision:

Likelihood of injury to business reputation or of dilution of the distinctive quality of a mark registered under this Act, or a mark valid at common law, shall be a ground for injunctive relief notwithstanding the absence of competition between the parties or the absence of confusion as to the source of goods or services.

Model State Trademark Bill, Section 12 (USTA 1964). A trademark dilution provision is also contained in Section 25 of the Restatement (Third) of Unfair Competition.

B. The Trademark Dilution Act of 1995.[6]

The serious push for a federal-trademark dilution law began in 1987 with the publication of "The United States Trademark Association Review Commission Report and Recommendations to USTA President and Board of Directors." In that report, the Commission proposed the adoption of a new federal trademark dilution law. Trademark dilution provisions were included in S. 1883, the proposed Trademark Law Revision Act of 1987. However, while most of the bill's provisions eventually became law, concerns -- raised by the broadcast industry and rallied by Rep. Robert Kastenmeier (D. Wis.) -- that dilution protection would impinge on the First Amendment resulted in the deletion of the dilution provisions from the final legislation.

On March 22, 1995, the Federal Trademark Dilution Act of 1995 was introduced in the House of Representatives as H.R. 1295. With changes largely designed to make the bill applicable to the owners of both federally registered and common law trademarks, the bill was signed into law on January 16, 1996 as Public Law 10498, creating a new Section 43(c) to the Lanham Act.

C. Analysis of the Act.

Section 43(c) of the Lanham Act, also known as the Federal Trademark Dilution Act of 1995 ("ACT") became effective on January 16, 1996. A copy of the Act is attached as Appendix A. The new law benefits only "famous" trademarks. The "federal dilution statute is necessary because famous marks ordinarily are used on a nationwide basis and dilution protection is currently only available on a patch-quilt system of protection, in that only approximately 25 states have laws that prohibit trademark dilution." H.R. Rep. No. 374, 104th Cong., 1st Sess. 1995, 1195 WL 709280, pg. 4 (Leg. Hist.) The Federal Trademark Dilution Act provides that:

the owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark,... 15 U.S.C. 1125(c).[7]

In order to state a cause of action under the Act a party must show that the mark is famous and that the complainant's use is commercial and in commerce which is likely to cause dilution. The statute defines the term "dilution" to mean "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake, or deception." 15 U.S.C. Section 1127. "The definition is designed to encompass all forms of dilution recognized by the courts, including dilution by blurring, by tarnishment and disparagement, and by diminishment. In an effort to clarify the law on the subject, the definition also recognizes that a cause of action for dilution may exist whether or not the parties market the same or related goods or whether or not a likelihood of confusion exists. Thus, a mark protected against dilution can have acquired its fame in connection with one type of good or service and, as a result, be so famous as to be entitled to protection against dilution when used on or in connection with an unrelated good or service." H.R. Rep. No. 374, 104th Cong., 1st Sess. 1995, 1995 WL 709280, pg. 3 (Leg. Hist.).

Under the Act, the owner of a famous mark is only entitled to injunctive relief unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. The Act does not preempt state dilution claims. The Act specifically provides that noncommercial use of the mark is not actionable. 15 U.S.C. Section 1125(c)(4)(B).

The legislative history of the Act indicates that it was intended to address
Internet domain name issues. Senator Patrick J. Leahy (D-Vt.), in discussing the Act stated:

... it is my hope that this anti-dilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others.


D. Existing Case Law.

Very few courts have addressed the issue of registering trademarks as domain names under the Federal Trademark Dilution Act. This court in Actmedia, Inc. v. Active Media Intl Inc., 1996 WL 399707 (N.D.III. 1996) held that defendant's reservation of the domain name "actmedia.com" without the authorization of the plaintiff, who had done business under Actmedia since 1972 and had registered the mark in 1986, violated the Lanham Act and the Illinois Anti-Dilution Act. The court held that the reservation of the domain name without authorization violated 15 U.S.C. Section 1125 and Illinois common law because the action "(a) constitutes unauthorized use and misappropriation of Plaintiff's mark; (b) constitutes false designation of origin; (c) is likely to cause confusion in the marketplace that Plaintiff and Defendant are affiliated; and (d) is likely to cause confusion that Plaintiff sponsors or approves Defendant's commercial activities." Id. at 2. The court further held that defendant's actions violate the Illinois Anti-Dilution Act, Ill. Rev. Stat. ch. 140 Section 22, because "it creates a likelihood of dilution of the distinctive quality of the Mark." Id. The court entered a permanent injunction requiring Defendant to transfer the domain name to plaintiff.

In Hasbro, Inc. v. Internet Entertainment Group, Ltd., 1996 WL 84853 (W.D. Wash.), the court preliminarily enjoined defendant's use of the domain name "candyland.com" to identify a sexually explicit Internet site. The court held that "Hasbro has demonstrated a likelihood of prevailing on its claims that defendant's conduct violates the federal trademark anti-dilution statute, 15 U.S.C. Section 1125(c) and the Washington State trademark anti-dilution statute, RCW 19.77. 160." Id at 1.

E. The Dilution Statutes Have Been Violated by Toeppen.

1. Intermatic Is a Famous Mark.

As a matter of law the Court finds that the Intermatic mark is famous within the meaning of 15 U.S.C. Section 1125(c). Toeppen does not dispute that the Intermatic mark is famous and no evidence has been presented to contradict Intermatic's long history and use of its mark. The Intermatic mark is a strong fanciful federally registered mark, which has been exclusively used by Intermatic for over 50 years. Therefore since Intermatic has established that its mark is famous, it need only show that Toeppen's use is a commercial use in commerce and that by his use dilution will likely occur.

2. Toeppen Is Engaged In a Commercial Use of the Intermatic Trademark.

Toeppen argues that there has been no violation of the Federal Trademark
Dilution Act because his use of the Internatic mark is not a commercial use. Internatic asserts that Toeppen's use is commercial because the Internet designation "*.com" is short for commercial and Toeppen used "intermatic.com" in connection with the sale of a computer software program.

The use of the first level domain designation "*.com" does not in and of itself constitute a commercial use. The Internet is constantly changing and evolving. Currently the "*.com" designation is the only one available for both commercial and private use. In the future perhaps other first level domain designations will be available solely for private or commercial uses. However, the Court is not here to set policy guidelines for the Internet but rather the Court must apply the law to the Internet as it exists today. Therefore, the Court holds that the "*.com" designation alone does not establish commercial use.

Internatic also argues that Toeppen's use of the "intermatic.com" domain name in connection with the proposed sale of a computer software program constitutes a commercial use. Toeppen's use ended before the effective date of the Federal Trademark Dilution Act. Toeppen's use of "intermatic.com" in connection with the software program does not constitute a commercial use because this particular commercial use terminated prior to the passage of the Act.

Toeppen's intention to arbitrage the "intermatic.com" domain name constitutes a commercial use. At oral argument Toeppen's counsel candidly conceded that one of Toeppen's intended uses for registering the Internatic mark was to eventually sell it back to Internatic or to some other party. Toeppen's desire to resell the domain name is sufficient to meet the "commercial use" requirement of the Lanham Act.

3. Toeppen's Use of the Internet Constitutes Commerce.

Toeppen's use of the Internet satisfies the "in commerce" requirement of Section 43(c). Toeppen also argues that he has not violated the Act because his use of the "intermatic.com" domain name was not in commerce. This argument misses the mark. "Because Internet communications transmit instantaneously on a worldwide basis there is little question that the "in commerce' requirement would be met in a typical Internet message, be it trademark infringement or false advertising." 1 Gilson, Trademark Protection and Practice, Section 5.11[2], p. 5-234 (1996). The Supreme Court has held that the in commerce requirement should be construed liberally because the Lanham Act "confers broad jurisdictional powers upon the courts of the United States." Steele v. Bulova Watch Co., 344 U.S. 280, 293, 73 S.Ct. 252 (1952). Therefore the Court finds that use of the Internet is sufficient to meet the "in commerce" requirement of the Act.

4. Toeppen Is Causing Dilution of the Distinctive Quality of the Mark.

Toeppen's use of "intermatic.com" is likely to cause dilution of its mark. For purposes of the Act, the "term "dilution' means the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception." 15 U.S.C. Section 1127. Toeppen's conduct has caused dilution in at least two respects. First, Toeppen's registration of the intermatic.com domain name lessens the capacity of Internatic to identify and distinguish its goods and
services by means of the Internet. Intermatic is not currently free to use its mark as its domain name. This is not a situation where there were competing users of the same name by competing parties and a race to the Internet between them. This case involves one party, Intermatic, with a long history of trademark use, and a second, Toeppen, who has effectively enjoined Intermatic from using its trademark by the payment of $100 to register the "intermatic.com" domain name. This activity clearly violates the Congressional intent of encouraging the registration and development of trademarks to assist the public in differentiating products. Park 'N Fly, Inc. v. Dollar Park and Fly, Inc., 469 U.S. 189, 198, 105 S.Ct. 658, 663 (1985). It would seriously undermine the trademark policy to prevent a company from exercising its mark by reason of Toeppen's conduct. Such conduct lessens the capacity of Intermatic to identify its goods to potential consumers who would expect to locate Intermatic on the Internet through the "intermatic.com" domain name.

Second, Toeppen's conduct dilutes the Intermatic mark by using the Intermatic name on its web page. As the Seventh Circuit explained in Polaroid Corp. v. Polaroid Inc., 319 F.2d 830, 836 (7th Cir. 1963),

The gravamen of a dilution complaint is that the continuous use of a mark similar to plaintiff's works an inexorably adverse effect upon the distinctiveness of the plaintiff's mark, and that, if he is powerless to prevent such use, his mark will lose its distinctiveness entirely ... dilution is an infection which, if allowed to spread, will inevitably destroy the advertising value of the mark.

"The harm caused by dilution is, for example, that the distinctiveness of the name [Intermatic] and the favorable association that accrued to it by virtue of [Intermatic's] commercial success would be undermined by the use of similar names in connection with other non-competing and non-confusing products." Ringling Bros.-Barnum & Bailey Combined Shows, Inc., v. Celozzi-Ettelson Chevrolet, Inc., 855 F.2d 480, 485 (7th Cir. 1988). If Toeppen were allowed to use "intermatic.com", Intermatic's name and reputation would be at Toeppen's mercy and could be associated with an unimaginable amount of messages on Toeppen's web page. "It is the same dissonance that would be produced by selling cat food under the name 'Romanoff,' or baby carriages under the name 'Aston Martin'" Exxon Corp. v. Exxene Corp., 696 F.2d 544, 550 (7th Cir. 1983).

Dilution of Intermatic's mark is likely to occur because the domain name appears on the web page and is included on every page that is printed from the web page. At oral argument counsel agreed that almost all web pages will include the domain name on the computer screen as well as printing the name on any and all pages that are printed. The all inclusive nature of the domain name all but guarantees that "intermatic.com" will appear on the web page and any printouts. Attaching Intermatic's name to a myriad of possible messages, even something as innocuous as a map of Urbana, Illinois, is something that the Act does not permit. "[T]he most corrosive and irreparable harm attributable to trademark infringement is the inability of the victim to control the nature and quality of the defendant's goods." Ideal Industries, Inc. v. Gardner Bender, Inc., 612 F.2d 1018, 1026 (7th Cir. 1979).

The fact that "intermatic.com" will be displayed on every aspect of the web page is sufficient to show that Intermatic's mark will likely be diluted.

The Illinois Anti-Dilution Act permits the owner of a mark to obtain an injunction enjoining the use by another of a similar mark "if there exists a likelihood ... of dilution of the distinctive quality of the mark, ... notwithstanding the absence of competition between the parties or of confusion as to the source of goods or services." 765 ILCS 1035/1 et. seq. Under the Illinois Act, "an injunction must be granted if the prior user can show that the mark is distinctive and that the subsequent user's use dilutes that distinctiveness." Hyatt Corp. v. Hyatt Legal Services, 736 F.2d 1153, 1157 (7th Cir. 1984), cert. denied, 469 U.S. 1019, 105 S.Ct. 434.

VI. RELIEF

Both the Lanham Act and the Illinois Anti-Dilution Act provide for injunctive relief upon a finding that a mark will likely be diluted. However, as mentioned earlier the federal trademark dilution act provides for additional relief upon a finding of willfulness. Such a finding cannot be made on this record in the context of summary judgment because a fact question exists. See e.g., HardRock Cafe Licensing Corp. v. Concession Services, Inc., 955 F.2d 1143 (7th Cir. 1992) (reversing and vacating the denial of attorney's fees in Lanham Act case for factual determination of whether "exceptional circumstances" or "extenuating circumstances" exist). Therefore it appears that the only relief plaintiff is entitled to at this time is injunctive relief. The appropriate relief in this case is to restrain Toeppen from preventing Intermatic from obtaining "intermatic.com" domain name designation and to require Toeppen to discontinue any and all use of the Intermatic mark.

VII. CONCLUSION

For the foregoing reasons, the court recommends that Intermatic's motion for summary judgment should be GRANTED in part and denied in part as to counts III and IV, Intermatic's motion for summary judgment should be DENIED as to counts I, II, V, VI, and VII, and Toeppen's motion for summary judgment should be DENIED as to all counts.

Intermatic should be granted the following relief:

1) Pursuant to 15 U.S.C. Section 1125(c) and the Illinois Anti-Dilution Act, Toeppen, and his officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with them who receive actual notice of this final judgment and permanent injunction are hereby permanently enjoined from using or infringing in any matter Intermatic's registered trademark, "INTERMATIC";
2) Pursuant to 15 U.S.C. Section 1125(c) and the Illinois Anti-Dilution Act Toeppen, and his officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with them who receive actual notice of this final judgment and permanent injunction are hereby permanently enjoined from taking any action to prevent Intermatic from obtaining the Internet domain name, "intermatic.com", and are permanently enjoined from asserting any further interest in "intermatic.com" domain name; and
3) The Court reserves jurisdiction to enforce the terms of this Injunction.

Respectfully submitted,
Appendix A


Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Section 1. Short Title.

This act may be cited as the "Federal Trademark Dilution Act of 1995".

Section 2. Reference to the Trademark Act of 1946.

For the purpose of this Act, the Act entitled "An Act to provide for the registration and protection of trade-marks used in commerce, to carry out the provisions of certain international conventions, and for other purposes", approved July 5, 1946 (15 U.S.C. 1051 and following), shall be referred to as the "Trademark Act of 1946".

Section 3. Remedies for Dilution of Famous Marks.

(a) Remedies. -- Section 43 of the Trade-mark Act of 1946 [15 U.S.C. 1125] is amended by adding at the end the following new subsection:

   (c)(1) The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection. In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to --
   (A) the degree of inherent or acquired distinctiveness of the mark;
   (B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;
   (C) the duration and extent of advertising and publicity of the mark;
   (D) the geographical extent of the trading area in which the mark is used;
   (E) the channels of trade for the goods and services with which the mark is used;
   (F) the degree of recognition of the mark in the trading "areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;
   (G) the nature and extent of use of the same or similar marks by third parties; and
   (H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principle register.
(2) In an action brought under this subsection, the owner of the famous mark shall be entitled only to injunctive relief unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. If such willful intent is proven, the owner of the famous mark shall also be entitled to the remedies set forth in sections 35(a) and 36, subject to the discretion of the court and the principles of equity.

(3) The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principle register shall be a complete bar to an action against that person, with respect to that mark, that is brought by another person under the common law or a statute of a State and that seeks to prevent dilution of the distinctiveness of a mark, label, or form of advertisement.

(4) The following shall not be actionable under this section:
(A) Fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark.
(B) Noncommercial use of a mark.
(C) All forms of news reporting and news commentary.

(b) CONFORMING AMENDMENT. -- The heading for title VIII of the Trademark Act of 1946 is amended by striking "AND FALSE DESCRIPTIONS" and inserting "FALSE DESCRIPTIONS, AND DILUTION".

Section 4. Definition.

Section 45 of the Trademark Act of 1946 (15 U.S.C. 1127) is amended by inserting after the paragraph defining when a mark "shall be deemed to be "abandoned" the following:

"The term "dilution" means the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of
(1) competition between the owner of the famous mark and other parties, or
(2) likelihood of confusion, mistake, or deception."

Section 5. Effective Date.

This Act and the amendments made by this Act shall take effect on the date of the enactment of this Act.

Any objections to this Report and Recommendation must be filed with the Clerk of the Court within ten (10) days of receipt of this notice. Failure to file objections within the specified time waives the right to appeal the Magistrate Judge's Report and Recommendation. See Fed.R.Civ.P. 72 (b); 28 U.S.C. 636 (b)(1)(B); Lorentzen v. Anderson Pest Control, 64 F.3d 327, 329 (7th Cir. 1995); The Provident Bank v. Manor Stell Corp., 882 F.2d 258 (7th Cir. 1989).

NOTES

1. SF refers to the Stipulation of Facts filed by the parties.

2. The Internet is described in detail in MTV Networks v. Curry, 867 F.Supp.


4. One of the difficulties with the procedural posture of this case, is that the parties have persisted in proceeding on the basis of cross motions for summary judgment rather than on an agreed record for purposes of final resolution as permitted by Fed.R. Civ. P. 52(a). Under the summary judgment standard, the Court may not resolve factual disputes, but rather examines the record to determine whether a material dispute of fact exists.

5. See, Gilson, Trademark Dilution Now a Federal Wrong: An Analysis of the Federal Trademark Dilution Act of 1995 (1996), pgs. 3-5 for a brief overview of the history of dilution statutes from which much of the Court's discussion of the history is taken.

6. See, Robert V. Petershack, 1995 Federal Trademark Dilution Act, 69 JUL Wis. Law 18, for discussion of evolution of the Act from which this section is taken.

7. Factors considered in determining the distinctiveness and fame of the mark are:

   a) degree of inherent or acquired distinctiveness of the mark;
   b) duration and extent of use of the mark;
   c) duration and extent of advertising and publicity of the mark;
   d) geographical extent of the trading area in which the mark is used;
   e) channels of trade for the goods or services;
   f) degree of recognition of the mark in the trading area;
   g) use of the same or similar marks by third parties; and
   h) whether the mark was federally registered.


© 1997 The Bureau of National Affairs Inc., All Rights Reserved
UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

PANAVISION INTERNATIONAL, L.P., a Delaware Limited Partnership,
 Plaintiff,

v.

DENNIS TOEPPEN, an individual, NETWORK
SOLUTIONS, INC., District of Columbia Corporation,
and DOES 1-50, Defendants.

Case No. 96-3284 DDP (JRx)

Nov. 27, 1996

Defendant Network Solutions, Inc.'s motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) or, in the alternative, for summary judgment came before the Court on November 18, 1996. After reviewing and considering the materials submitted by the parties and hearing oral argument, the Court grants Network Solutions, Inc.'s motion for summary judgment.

I. BACKGROUND

Plaintiff Panavision International, L.P. ("Panavision") is a Delaware limited partnership with its principal place of business in Los Angeles, California. Panavision owns several federally registered trademarks, including "Panavision" and "Panaflex" (the "Panavision marks"), which it uses in connection with its theatrical motion picture and television camera and photographic equipment business.

Defendant Dennis Toeppen ("Toeppen") is an individual residing in Illinois. Toeppen owns several websites, including the two at issue in this case, "panavision.com" and "panaflex.com."

Defendant Network Solutions, Inc. ("NSI") is a District of Columbia corporation with its principal place of business in Herndon, Virginia. NSI registers Internet domain names.

Defendant Toeppen registered the Panavision marks as domain names and then attempted to sell the domain names to Panavision. Panavision brought suit against both Toeppen and NSI alleging various federal and state causes of action. On November 5, 1996, the Court granted in part and denied in part Panavision's motion for summary judgment against Toeppen, holding, inter alia, that Toeppen had violated Panavision's rights under the Lanham Act by diluting its marks. See Panavision v. Toeppen, 1996 WL 653726 (C.D. Cal. Nov. 5, 1996).

NSI now moves to dismiss Panavision's claim for negligent interference with prospective economic advantage or, in the alternative, for summary judgment on that claim. The negligent interference claim is the only claim pending against NSI.
II. DISCUSSION

A. NSI's Motion to Dismiss Pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(6).

Dismissal under Rule 12(b)(6) is appropriate when it is clear that no relief could be granted under any set of facts that could be proven consistent with the allegations. *Newman v. Universal Pictures*, 813 F.2d 1519, 1521-22 (9th Cir. 1987), *cert. denied*, 486 U.S. 1059 (1988). The court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-movant. *North Star Int'l v. Arizona Corp. Comm'n*, 720 F.2d 578, 581 (9th Cir. 1983). Generally, the court is limited to considering the pleadings; however, the court may also consider documents whose contents are alleged in the complaint, are "central" to the plaintiff's claim, and whose authenticity is not disputed, but which are not physically attached to the complaint. *Branch v. Tunnell*, 14 F.3d 449, 453-54 (9th Cir.), *cert. denied*, 114 S. Ct. 2704 (1994).

As a prerequisite to maintaining an action for negligent interference with prospective economic advantage, the plaintiff must establish a "special relationship" between the plaintiff and the defendant giving rise to a duty of care. See *J'Aire Corp. v. Gregory*, 24 Cal.3d 799, 803-804 (1979); *Ott v. Alfa-Laval Agrei, Inc.*, 31 Cal.App.4th 1439, 1448 (1995).

California courts use a six factor test (the first four of which are the most important) to determine whether the requisite special relationship exist: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of the harm; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm.

Panavision's complaint asserts:

Defendant NSI knew or should have known that by allowing Defendant Toeppen to register the domain name "PANAVISION.COM," Defendant Toeppen would deceive, confuse, and misguide the public and the entertainment industry to believe that Defendant Toeppen's sham services are authorized by or associated with Panavision. Defendant's therefore owed a duty of care to Panavision to ensure that Panavision's intellectual property was not damaged and that Defendant Toeppen's actions did not cause economic injury. It was reasonably foreseeable to Defendant NSI that allowing Defendant Toeppen to register the domain name "PANAVISION.COM" would injure Panavision and damage Panavision's goodwill, reputation and profits. In failing to conform its conduct with this duty, Defendant NSI failed to exercise ordinary and reasonable care and acted negligently.

(Complaint at para. 68).

NSI makes two arguments in support of its motion to dismiss.

First, NSI argues that as a matter of law NSI did not and does not owe any duty of care to Panavision to avoid harming Panavision's trademark rights. NSI asserts that "[t]he law simply does not impose an affirmative duty upon a third party to police millions of trademarks for trademark owners," citing *MDT Corp. v. New York Stock Exchange, Inc.*, 858 F.Supp. 1028 (1994), as support for this proposition. This argument is appealing in the abstract, but it fails when analyzed more fully.

In *MDT*, the court held that the New York Stock Exchange ("NYSE") had not infringed the plaintiff's trademark by permitting a third party to use the plaintiff's mark as the third party's trading symbol. Id. at 1033-1034. The plaintiff did not argue that NYSE or the third party infringed the mark; rather, it argued that other individuals had infringed the plaintiff's trademark because of the way in which the other individuals utilized the trading symbol.

To be liable for contributory infringement, however, the defendant must have "intentionally induce[d]
another to infringe a trademark, or ... continue[d] to supply its product to one who it knows or has reason to know is engaged in trademark infringement." Id. at 1033 (citation omitted). Therefore, because the defendant had not in any way encourage others to use the trading symbol in a manner that infringed the plaintiff's mark, it could not be liable for contributory infringement. The court stated that it appeared as though the plaintiff were arguing that the law "impose[d] an affirmative duty on innocent third party users of a mark to police the mark for its owner ... [however,] [n]o such duty exists." Id. at 1033-34.

NSI asserts that MDT stands for the proposition that, as a matter of law, it does not have a duty to Panavision or any other trademark owner in connection with registering domain names. However, there are important distinctions between MDT and the case at bar.

In MDT, court addressed the claim on a motion for summary judgment, not on a motion to dismiss. Moreover, a critical factor in the court's analysis was that the plaintiff had not asserted that NYSE was guilty of any wrongdoing. The court's holding was therefore narrow: an innocent party has no duty to prevent other parties from infringing a plaintiff's trademark.

Here, however, Panavision's complaint asserts that NSI knew that Toeppen was registering Panavision's marks with the intent to injure Panavision. For purposes of this motion, the Court must assume the truth of Panavision's allegation. Accordingly, NSI does not stand on the same footing as NYSE, which was an admittedly innocent party acting in good faith.

NSI's second argument is that there is no set of facts that Panavision could prove consistent with the allegations of the complaint that would pass muster under the six factor special relationship test established by the California courts. This argument likewise fails.

With regard to the first factor, intent to affect the plaintiff, NSI argues that its domain name dispute policy (properly considered in this motion to dismiss because Panavision referenced the policy in its complaint) specifically states that a breach of any of the warranties, representations, or obligations of an applicant "shall not provide any third party a right to require or demand removal of a domain name or an applicant from the Network Solutions registry." However, this statement does not establish that the NSI-Toeppen contract was not intended to affect Panavision, it merely shows that the contract was not intended to benefit Panavision.

Another defect of NSI's motion to dismiss is its assertion that the harm to Panavision was not foreseeable because, as asserted in Panavision's complaint, NSI "makes no independent determination of an applicant's right to use the requested domain name prior to allowing a name to be reserved." The problem with this argument is that foreseeability also encompasses harm that the defendant "should have foreseen."

NSI's motion to dismiss is not proper if the Court has to resort to considering the six factor test. The Court must accept Panavision's allegations as true, as well as any inferences reasonably drawn from those facts. Indeed, even improbable facts must be accepted as true for the purposes of a Rule 12(b)(6) motion. See Neitzke v. Williams, 490 U.S. 319 (1989). Any questions regarding Panavision's ability to prove its allegations are of no concern. See Allison v. California Adult Authority, 419 F.2d 822, 823 (9th Cir. 1969). Therefore, because the six factors all present factual issues supported by the assertions in the complaint, the Court denies NSI's motion to dismiss.

B. NSI's Motion for Summary Judgment.

Summary judgment is appropriate when there "is no genuine issue of material fact and ... the moving party is entitled to a judgment as a matter of law." Fed.R.Civ.P. 56(c); see Celotex Corp. v. Catrett, 477 U.S. 317 (1986).

In order to defeat a motion for summary judgment, there must be facts in dispute that are both genuine and material, i.e., there must be facts upon which a fact finder could "reasonably find" for the non-moving party. See Anderson v. Liberty Lobby, 477 U.S. 242, 252 (1986). The court does not weigh the evidence or make credibility determinations; rather, the court only determines whether there
are any disputed issues and, if so, whether those issues are both genuine and material. Id.

The initial burden of establishing that there is no genuine issue of material fact lies with the moving party. Fed.R.Civ.P 56(c); Celotex, 477 U.S. at 323; British Airways Board v. Boeing Co., 585 F.2d 946, 951 (9th Cir. 1978), cert. denied, 440 U.S. 981 (1979). Once the movant has met this burden by producing evidence that would entitle the moving party to a directed verdict at trial if left uncontroverted, the burden shifts to the non-movant to present specific facts showing that there is a genuine issue of material fact. See Fed.R.Civ.P. 56(e); Celotex, 477 U.S. at 324; Lake Nacimiento Ranch Co. v. San Luis Obispo, 841 F.2d 872, 876 (9th Cir. 1987), cert. denied, 488 U.S. 827 (1988). If a party has had adequate time for discovery but "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial," summary judgment is appropriate. Celotex, 477 U.S. at 321.

NSI's motion for summary judgment is appropriate because there is no genuine issue of material fact and NSI is entitled to judgment as a matter of law. Panavision has not presented any evidence beyond its pleadings that could establish the necessary "special relationship" between NSI and Panavision.[1]

With regard to the first factor, intent to affect the plaintiff, Panavision has argued only that (1) "[i]t is obvious that registrations of the domain name [] PANAVISION.COM ... affects the rights of Panavision;" (2) "[i]t is obvious that [NSI] knows that registrations like the ones at issue can affect trademark owners;" and (3) NSI's Domain Name Dispute Policy "evidences a clear awareness of the impact of domain name registration, by requiring an applicant for a domain name to warrant that the domain name does not violate any trademark laws." Nowhere, however, does Panavision present any evidence that NSI actually knew or should have known that Toeppen was registering the domain name with an intent to harm Panavision. One could speculate about such a possibility, but "[t]he mere submission of a scintilla of evidence in support of the non-moving party's position is not sufficient" to survive a motion for summary judgment. Anderson, 477 U.S. at 252. With regard to the second factor, foreseeability of harm, there is evidence that NSI knows that a given registrant could utilize a domain name in a manner that would violate an intellectual property owner's trademark rights. However, NSI registers 50,000 domain names per month, and Panavision has produced no evidence suggesting that NSI knew or should have known that co-defendant Dennis Toeppen's registration of "panavision.com" would harm Panavision.

With regard to the fourth factor, the closeness of the connection between NSI's conduct and the injury suffered by Panavision, Panavision premises its argument on the fact that NSI does not take any action to investigate the rights of third parties prior to registering a domain name. NSI, however, requires a registrant to sign a statement warranting that it has the right to register the name and that the registration does not interfere with or infringe the rights of third parties. More importantly, NSI is under no general duty to investigate whether a given registration is improper, see MDT, 858 F.Supp. at 1033-34, and Panavision has failed to present any evidence that there were any facts necessitating such an investigation in this case.

With regard to the fifth factor, the moral blame attached to NSI's conduct, Panavision merely asserts that NSI should analyze registrations for potential trademark violations. In response to NSI's position that it does not have the resources to investigate, arbitrate, or adjudicate domain name disputes, Panavision asserts that "there is no evidence that [NSI] does not have 'the financial resources ... to [investigate]' ...." However, it is Panavision's burden to establish that there is a genuine issue of fact on this issue requiring trial -- a burden not satisfied by the sentence quoted above.

Moreover, NSI has submitted a declaration from its Internet Business Manager stating, under penalty of perjury, that NSI does not have the "financial resources, personnel, expertise or authority to arbitrate or adjudicate conflicting claims .... " This statement rings true particularly in this case, where the trademark issues are issues of first impression. In December of 1995, when Toeppen registered the "panavision.com" domain name, NSI could not have known whether Toeppen's registration would eventually be held to violate the Lanham Act.

III. CONCLUSION
Based on the foregoing, the Court grants NSI's motion as a motion for summary judgment.

IT IS SO ORDERED.

DATED: November 27, 1996

DEAN D. PREGERSON

United States District Judge

END NOTES

1. [Return to Text] Again, the six factors, the first four of which are the most important, are: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of the harm; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm.

© 1996 The Bureau of National Affairs, Inc., All Rights Reserved
UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

LOCKHEED MARTIN CORPORATION,
Plaintiff,

v.
NETWORK SOLUTIONS, INC., and DOES 1-20,
Defendants.

Case No. CV 96-7438 DDP (ANx)

Order Granting Defendant's Motion for Summary Judgment

The motion by defendant Network Solutions, Inc. ("NSI") for summary judgment came before the Court on October 6, 1997. After reviewing and considering the materials submitted by the parties and hearing oral argument, the Court grants the motion in its entirety.

I. Background

The issue presented by this litigation is whether NSI violated federal trademark law by accepting registrations of Internet domain names that are identical or similar to Lockheed Martin Corporation's ("Lockheed") SKUNK WORKS service mark. Lockheed asserts that NSI directly infringed and diluted its mark by accepting the registrations. Lockheed also asserts that NSI is liable as a contributory infringer because NSI did not comply with Lockheed's demands to cancel the registrations.

As to direct infringement, the Court concludes that NSI has not used Lockheed's service mark in connection with the sale, offering for sale, distribution or advertising of goods or service, and therefore cannot be liable for infringement under 15 U.S.C. §1114(1)(a) or for unfair competition under 15 U.S.C. §1125(a).

As to dilution, the Court finds that NSI has not made a commercial use of domain names as trademarks, and therefore cannot satisfy the commercial use element of dilution under 15 U.S.C. §1125(c).

As to contributory infringement, there are two potential bases for liability. First, a defendant is liable if it intentionally induced others to infringe a mark. Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 853-54, 102 S.Ct. 2182, 2188 (1982); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996). Second, a defendant is liable if it continued to supply a product to others when the defendant knew or had reason to know that the party receiving the product used it to infringe a mark. Inwood, 456 U.S. at 853-54, 102 S.Ct. at 2488; Fonovisa, 76 F.3d at 264.

Lockheed has not presented evidence that NSI induced others to infringe Lockheed's service mark. Therefore, NSI is not liable under the first basis.
As to the knowledge basis, the Court concludes that NSI's limited role as a registrar of domain names coupled with the inherent uncertainty in defining the scope of intellectual property rights in a trademark militates against finding that NSI knew or had reason to know of potentially infringing uses by others. Furthermore, contributory infringement doctrine does not impose upon NSI an affirmative duty to seek out potentially infringing uses of domain names by registrants.

A. The Parties

For over 50 years, plaintiff Lockheed and its predecessors have operated "Skunk Works," an aerospace development and production facility. Lockheed owns the federally registered "SKUNK WORKS" service mark.

Defendant NSI is a publicly traded corporation with its principal place of business in Herndon, Virginia. Under a contract with the National Science Foundation, NSI is the exclusive registrar of most Internet domain names.

B. The Internet

The Internet is an international "super-network" connecting millions of individual computer networks and computers. The Internet is not a single entity. It is a highly diffuse and complex system over which no entity has authority or control. See generally American Civil Liberties Union of Georgia v. Reno, 929 F.Supp. 224, 930-45 (E.D. Pa. 1995), aff'd, 117 S.Ct. 2325 (1997). Although the Internet is now widely known for one of its ways of presenting information -- the World Wide Web ("Web") -- the Internet supports many other forms of communication. The Internet allows one-to-one communication via electronic mail ("e-mail"). In addition, one person can reach many other users through bulletin board services, newsgroups and numerous other Internet based means of communication. Id. at 834. All of these forms of Internet communication depend on the use of domain names to locate specific computers and networks on the Internet.

For commercial users, the Web is the most important part of the Internet. Unlike previous Internet-based communications formats, the Web is easy to use for people inexperienced with computers. Information on the Web can be presented on "pages" of graphics and text that contain "links" to other pages either within the same set of data files ("Web site") or within data files located on other computer networks. Users access information on the Web using "browser" programs. Browser programs process information from Web sites and display the information using graphics, text, sound and animation. Because of these capabilities, the Web has become a popular medium for advertising and for direct consumer access to goods and services. At the same time, the Web, like the rest of the Internet, is an important medium of non-commercial communications. The Web has made it easier for individuals and small organizations to publish information to the general public. Publication on the Web simply requires placing a formatted file on a host computer.

Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.

Id. at 837. Much of the Web's usefulness derives from its use of links. A link is an image or a short section of text referring to another document on the Web. A user interested in accessing the referenced document selects the link, causing the document to be displayed automatically, along with a new set of links that the user may follow. Id. at 836.

While the linked structure of the Web is well-suited to allow users to browse among many sites, following whatever links happen to draw their interest, it is poorly suited for users who want to find a single Web site directly. Users searching for a specific Web site have two options. First, if users know or
can deduce the address of a Web site, they can type the address into a browser and connect directly to the Web site as if dialing a telephone number. Panavision Int'l, L.P. v. Toeppen, 945 F.Supp. 1296, 1299 (C.D. Cal. 1996). More often, users do not know the exact address and must rely on "search engines" available on the Web to search for key words and phrases associated with the desired Web site. Because of the quantity of information on the Web, searches often yield thousands of possible Web sites. Such a cumbersome process is rarely satisfactory to businesses seeking to use the Web as a marketing tool. Instead, businesses would prefer that customers simply be able to find a Web site directly using a corporate name, trademark or servicemark. Panavision, 945 F.Supp. at 1299.

1. The Domain Name System

Web sites, like other information resources on the Internet, are currently addressed using the Internet "domain name system." A numbering system called the "Internet Protocol" gives each individual computer or network a unique numerical address on the Internet. The "Internet Protocol number," also known as an "IP number," consists of four groups of digits separated by periods, such as "192.215.247.50." For the convenience of users, individual resources on the Internet are also given names. Specialized computers known as "domain name servers" maintain tables linking domain names to IP numbers.

Domain names are arranged so that reading from right to left, each part of the name points to a more localized area of the Internet. For example, in the domain name "cadc.uscourts.gov," "gov" is the top-level domain, reserved for all networks associated with the federal government. The "uscourts" part specifies a second-level domain, a set of the networks used by the federal courts. The "cadc" part specifies a sub-network or computer used by the United States District Court for the Central District of California.

If a user knows or can deduce the domain name associated with a Web site, the user can directly access the Web site by typing the domain name into a Web browser, without having to conduct a time-consuming search. Because most businesses with a presence on the Internet use the ".com" top-level domain name, as in "acme.com." Second-level domain names, the name just to the left of ".com," must be exclusive. Therefore, although two companies can have non-exclusive trademark rights in a name, only one company can have a second-level domain name that corresponds to its trademark. [1] For example, Juno Lighting, a maker of lamps, sought to establish a Web site with the address "juno.com," a domain name already in use by Juno Online Services, which uses the domain name as part of e-mail addresses for hundreds of thousands of e-mail customers. See Juno Online Servs., L.P. v. Juno Lighting, Inc., ___ F.Supp. ___, 1997 WL 613021 (N.D. Ill. Sept. 29, 1997). In short, the exclusive quality of second-level domain names has set trademark owners against each other in the struggle to establish a commercial presence on the Internet, and has set businesses against domain name holders who seek to continue the traditional use of the Internet as a non-commercial medium of communication.

2. NSI's Role in the Domain Naming System

Under a contract with the National Science Foundation, NSI manages domain name registrations for the ".com," ".net," ".org," ".edu," and ".gov" top-level domains. The contract authorizes NSI to charge $100 for an initial two-year registration and $50 annually starting the third year. NSI registers approximately 100,000 Internet domain names per month. (Graves Decl. ¶ 5.) Registration applications are made via e-mail and in more than 90% of registrations no human intervention takes place. (Graves Depo. at 54.) On average, a new registration occurs approximately once every 20 seconds. (Id. at 47-48.)

NSI performs two functions in the domain name system. First, it screens domain name applications against its registry to prevent repeated registrations of the same name. Second, it maintains a directory linking domain names with the IP numbers of domain name servers. The domain name servers, which are outside of NSI's control, connect domain names with Internet resources such as Web sites and e-mail systems.

NSI does not make an independent determination of an applicant's right to use a domain name. Nor does
NSI assign domain names; users may choose any available second-level domain name. In 1995, NSI responded to the problem of conflicting claims to domain names by instituting a domain name dispute policy. Under the current policy, in effect since September 9, 1996, NSI requires applicants to represent and warrant that their use of a particular domain name does not interfere with the intellectual property rights of third parties. (Graves Decl. Ex. 1.) Under the policy, if a trademark holder presents NSI with a United States Patent and Trademark Office registration of a trademark identical to a currently registered domain name, NSI will require the domain name holder to prove that it has a pre-existing right to use the name. If the domain name holder fails to do so, NSI will cancel the registration. (Id.) NSI's policy has been criticized as favoring trademark owners over domain name holders, and favoring owners of federally registered marks over owners of non-registered marks, because owners of federally registered marks can invoke NSI's policy to effectively enjoin the use of identical domain names without having to make any showing of infringement or dilution. Jerome Gilson & Jeffrey M. Samuels, *Trademark Protection and Practice*, §§8.11[4][B], at 5-239, 5.11[5], at 5-243 (1997) (noting that NSI's policy is tilted in favor of trademark owners, who can deprive registrants of domain names without meeting the likelihood of confusion test for infringement or showing that the domain name dilutes the mark); Gayle Weiswasser, *Domain Names, the Internet, and Trademarks Infringement in Cyberspace*, 13 Santa Clara Computer & High Tech. L. J. 137, 172-73 (1997). If a trademark holder and domain name registrant take their dispute to court, NSI will deposit the domain name in the registry of the court. This process maintains the status quo; the domain name remains active while in the registry of the court. [2]

C. Factual Background

Most of the underlying facts of this case are not in dispute. The dispute at summary judgment is over the interpretation of the law and the application of the law to the facts. The court finds that there is no genuine issue as to the following facts:

1. Lockheed owns the federally registered SKUNK WORKS service mark for "engineering, technical consulting, and advisory services with respect to designing, building, equipping, and testing commercial and military aircraft and related equipment." (Land Decl. Exs. A & B (Certificate of Registration Nos. 968,861 & 1,161,482).)

2. In August 1994, Seng-Poh Lee registered the domain name "skunkwrks.com" with NSI. Lee did not associate the domain name with a web site. In March 1996, Lockheed demanded that Lee cancel his registration. In May 1996, Lee complied. However, Lockheed did not apply to NSI for registration of the name. It became generally available and was registered by Grant Smith, a resident of the United Kingdom, in December 1996. (Graves Decl. ¶ 14; Quinto Decl. Ex. H.)

3. In September 1995, Kathy Huber, a resident of New York, registered "skunkworks.com" with NSI for the use of her employer Skunkworks Marketing Lab, Inc ("SML"). SML used the domain name for e-mail only; it did not associate a web site with the domain name. (Jones Decl. Ex. 4.) On March 21, 1996, Lockheed sent a cease-and-desist-letter to SML. (Meeg Decl. Ex. C.) SML filed a petition in the United States Patent and Trademark Office seeking to cancel registration of the SKUNK WORKS mark on the grounds that "skunk works" was generic. SML has since moved to withdraw its petition. (Quinto Decl. ¶¶ 9-11.)

4. In January 1996, Ken Hoang, a resident of California, registered the domain name "skunkwrks.com" with NSI for use by his company Skunk Works Multimedia, Inc. Lockheed sued Hoang's company for trademark infringement in May 1996. *Lockheed Martin Corp. v. Clayton Jacobs*, CV 96-3422 (C.D. Ca. filed May 13, 1996). On July 23, 1996, that action resulted in a consent judgment under which the parties agreed that the domain name would be assigned to Lockheed. (Jones Decl. Ex. 7.) Lockheed claims that it provided NSI with a file-stamped copy of the consent judgment and requested that NSI transfer the infringing domain name registrations to Lockheed, but NSI took no action. (Quinto Decl. ¶¶ 6, 7.) NSI, however, asserts that Lockheed has failed to complete the necessary form to effect the transfer despite offers of assistance by NSI's counsel. (Heeg Decl. ¶ 2, Ex. A.).

5. In January 1996, Roger Barski, an Illinois resident, registered the domain name "skunkwerks.com" with NSI. Barski used the domain name in association with a Web site offering his services as a Web
site designer. (Jones Decl. Ex. 5.) After receiving a cease-and-desist letter from Lockheed, Barski canceled his "skunkwerks.com" account with his Internet service provider, essentially deactivating the domain name. He did not, however, request to have the name removed from NSI's registry.

6. On May 7, 1996 Lockheed sent NSI a letter advising NSI that Lockheed owned the SKUNK WORKS mark and requesting that NSI cease registering domain names that referred to or included the names "skunk works" or "skunkworks" or otherwise infringed Lockheed's mark. (Quinto Decl. Ex. A.) Lockheed also requested that NSI provide Lockheed with a list of registered domain names that contain the words "skunk works" or any variation thereof. Lockheed's letter did not include a certified copy of its trademark registration. (Id.; Graves Decl. ¶ 11.)

7. On June 18, 1996, Lockheed sent a second letter, informing NSI that the registrant of "skunkworks.com" had agreed to stop using the domain name, and that the registrant of "skunkworks.net" was being sued in federal district court. (Quinto Decl. Ex. C.) The letter did not refer to the lawsuit by docket number or caption, nor did it include a copy of the complaint or other pleading. (Id.)

8. In September 1996, James McBride, a Missouri resident, acting as the administrative contact for Skunkworx Industries, Ltd, registered the domain name "skunkworx.com" with NSI. (Quinto Decl. Ex. K.) The parties have not presented evidence of use of this domain name in connection with Web sites or other forms of communication.

9. On September 18, 1996, NSI's Internet business manager, David Graves, wrote to Lockheed's counsel in response to the May 7 and June 18 letters. NSI informed Lockheed that NSI could not provide a list of all domain names that included "skunkworks" or any variation thereof, but that Lockheed could use the public "Whois" database of domain name registrations to find this information. NSI further informed Lockheed that upon receipt of a file-stamped copy of the complaint in the "skunkworks .net" case, NSI would immediately deposit the domain name in the registry of the court, maintaining the status quo until the court ordered otherwise. (Graves Decl. Ex. 5.)

10. In December 1996, Terry Robinson, a Texas resident, registered the domain name "the-skunkwerks .com" with NSI. (Quinto Dec. Ex. L.) The parties have not presented evidence of use of this domain name in connection with Web sites or other forms of communication.

11. On January 3, 1997, Peter Pasho, a resident of Canada, registered the domain name "theskunkworks.com" with NSI. (Quinto Decl. Ex. M.) Pasho has associated the domain name with a Web site offering his services as a Web site designer. (Quito Decl. Ex. N.) As of April 9, 1997, this Web site included a page depicting a Lockheed-designed aircraft and briefly discussing its design at the Lockheed Skunk Works. (Id.)

**D. Procedural Background**

Lockheed filed this action on October 22, 1996, alleging infringement, unfair competition, dilution and contributory infringement under the Lanham Act, and seeking injunctive and declaratory relief. NSI answered the complaint and counterclaimed for declaratory relief.


On September 29, 1997, this Court denied Lockheed's motion to file a first amended complaint adding a cause of action for "contributory dilution." The Court denied the motion on the bases of futility, undue delay and prejudice.

NSI's present motion seeks summary judgment on all of Lockheed's claims.

**II. Discussion**
This Court has subject matter jurisdiction over Lanham Act claims pursuant to 28 U.S.C. §§1331 and 1338(a). NSI has consented to personal jurisdiction by appearing in this action. Fed.R.Civ.P. 12(h)(1).

A. Standard for Summary Judgment

Summary judgment is appropriate when there is no genuine issue of material fact and the moving party is entitled to a judgment as a matter of law. Fed.R.Civ.P. 56(c), see Celotex Corp. v. Catrett, 477 U.S. 317, 106 S.Ct. 2548 (1986).

In order to defeat a motion for summary judgment, there must be facts in dispute that are both genuine and material, i.e., there must be facts upon which a fact finder could reasonably find for the non-moving party. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 252 106 S.Ct. 2505, 2515 (1986). The Court does not weigh the evidence or make credibility determinations; rather, the court only determines whether there are any disputed issues and, if so, whether those issues are both genuine and material. Id.

The initial burden of establishing that there is no genuine issue of material fact lies with the moving party. Fed.R.Civ.P. 56(c); Celotex, 477 U.S. at 323, 106 S.Ct. at 2552-53; British Airways Board v. Boeing Co., 585 F.2d 946, 951 (9th Cir. 1978). Once the movant has met this burden by procuring evidence that, if left uncontroverted, would entitle the moving party to a direct verdict at trial, the burden shifts to the non-movant to present specific facts showing that there is a genuine issue of material fact. See Fed.R.Civ.P. 56(e); Celotex 477 U.S. at 324, 106 S.Ct. at 2553; Lake Nacimiento Ranch Co. v. San Luis Obispo, 841 F.2d 872, 876 (9th Cir. 1997).

Summary judgment is disfavored in trademark cases because of the inherently factual nature of most trademark disputes. See Levi Strauss & Co. v. Blue Bell, Inc., 778 F.2d 1352, 1355 (9th Cir. 1985). Nonetheless, summary judgment is appropriate "where the party opposing the motion fails to demonstrate the existence of any material issues of fact for trial." Sykes Laboratory, Inc. v. Kalvin, 610 F.Supp. 849, 860 (C.D. Cal. 1985).


Section 32 of the Lanham Act prohibits a person from using another's mark without permission "in connection with the sale, offering for sale, distribution or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive ...." 15 U.S.C. §1114(1). To be liable under section 32, a person must use the mark on competing or related goods in a way that creates a likelihood of confusion. AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348 (9th Cir. 1979). Before considering the likelihood of confusion, however, the Court must determine whether NSI, by accepting registrations, has used the SKUNK WORKS mark in connection with the sale, distribution or advertising of goods or services. See Planned Parenthood Fed'n of America, Inc. v. Bucci, 42 U.S.P.Q.2d 1430, 1434 (S.D.N.Y. 1997).

Domain names present a special problem under the Lanham Act because they are used for both a non-trademark technical purpose, to designate a set of computers on the Internet, and for trademark purposes, to identify an Internet user who offers goods or services on the Internet. See 2 Gilson, supra, §5.11(3), at S-235, 5.11(5), at S-243-44 (distinguishing the technical use of domain names from the trademark use to identify goods or services). When a domain name is used only to indicate an address on the Internet, the domain name is not functioning as a trademark. [3] See Walt-West Enters., Inc. v. Gannett Co., Inc., 695 F.2d 1050, 1059-60 (7th Cir. 1982) (radio station frequency used in "utilitarian sense of calling the listener's attention to a location on the FM dial" is not protectable under trademark law). Like trade names, domain names can function as trademarks, and therefore can be used to infringe trademark rights. See Accuride Int'l, Inc. v. Accuride Corp., 671 F.2d 1531 (9th Cir. 1989). Domain names like trade names, do not act as trademarks when they are used merely to identify a business entity; in order to infringe they must be used to identify the source of goods or services. Cf. In re Unclaimed Salvage & Freight Co., 192 U.S.P.Q. 165, 168 (T.T.A.B. 1976) (affirming refusal of registration of trade name as trademark where specimen demonstrated use only to identify applicant as a business); U.S. Dept. of Commerce, Patent and Trademark Office, Trademark Manual of Examining
Procedure §1202.02, at 1202-3 (2d ed. May 1993) (directing examiners to refuse registration of material that functions only to identify a business.)

NSI's acceptance of domain name registrations is connected only with the name's technical function on the Internet to designate a set of computers. By accepting registrations of domain names containing the words "skunk works," NSI is not using the SKUNK WORKS mark in connection with the sale, distribution or advertising of good and services. NSI merely uses domain names to designate host computers on the Internet. This is the type of purely "nominative" function that is not prohibited by trademark law. See New Kids on the Block v. New America Pub., Inc., 971 F.2d 302, 307 (9th Cir. 1992) (noting that laws against infringement do not apply to "non-trademark use of a mark") Lucasfilm, Ltd. v. High Frontier, 622 F.Supp. 931, 933 (D.D.C. 1985) (holding that property rights in a trademark do not extend to the use of the trademark to express ideas unconnected with the sale or offer for sale of goods or services).

This is not to say that a domain name can never be used to infringe a trademark. However, something more than the registration of the name is required before the use of a domain name is infringing. In Planned Parenthood Fed'n of America, Inc. v. Bucci, for example, the defendant registered the domain name "plannedparenthood.com" and used it as the address of a Web site promoting his book on abortion. 42 U.S.P.Q.2d 1430, 1432 (S.D.N.Y. 1997). The defendant admitted that he used the domain name hoping that people looking for the Planned Parenthood site would find this site. Id. at 1433. The defendant argued that registration without more is not a commercial use of a mark. Id. at 1436. The court, however, found that the defendant did "more than merely register a domain name; he has created a home page that uses plaintiff's mark as its address, conveying the impression to Internet users that plaintiff is the sponsor of defendant's web site." Id. at 1437. The infringing use in Planned Parenthood was not registration of the plaintiff's mark with NSI, but rather the use of the plaintiff's trademark "as a domain name to identify his web site" in a manner that confused Internet users as to the source or sponsorship of the product offered there. Id. at 1440; cf. TeleTech Customer Care Management (California), Inc. v. TeleTech Co., 42 U.S.P.Q.2d 1913, 1919 (C.D. Cal. 1997) (finding that the plaintiff was not likely to prevail on the merits of an infringement claim because the plaintiff demonstrated only that customers were likely to be confused as to location of Web site, not as to source of goods or services).

The cases dealing with vanity telephone numbers are consistent with the conclusion that registration of a domain name, without more, does not constitute use of the name as a trademark. A toll-free telephone number with an easy-to-remember letter equivalent is a valuable business asset. As with domain names, courts have held that the promotion of a confusingly similar telephone number may be enjoined as trademark infringement and unfair competition. Dial-a-Mattress Franchise Corp. v. Page, 880 F.2d 675, 678 (2d Cir. 1989); American Airlines, Inc. v. A 1-800-A-M-E-R-I-C-A-N Corp., 622 F. Supp. 673 (N.D. Ill. 1985). The infringing act, however, is not the mere possession and use of the telephone number. If it were, trademark holders would be able to eliminate every toll-free number whose letter equivalent happen to correspond to a trademark. In Holiday Inns, Inc. v. 800 Reservation, Inc., 86 F.3d 619 (6th Cir. 1996), the district court held that the defendant's use of 1-800 H[zero]LIDAY infringed the plaintiff's trademark in the telephone number 1-800-HOLIDAY. Id. at 620. The court of appeals reversed, holding that Holiday Inn's trademark rights in its vanity telephone number did not allow it to control use by others of confusingly similar telephone numbers. Although the defendant's toll-free number was often misdialed by customers seeking 1-800-HOLIDAY, the defendant never promoted the number in connection with the HOLIDAY trademark; but only prompted it as 1-800-405-4329. Id. at 623. Because the defendant had used the number only as a telephone number, and not as a trademark the court of appeals held that the defendant had not infringed the plaintiff's trademark. Id. at 625-26.

Domain names and vanity telephone numbers both have dual functions. Domain names, like telephone numbers, allow one machine to connect to another machine. Domain names, like telephone numbers, are also valuable to trademark holders when they make it easier for customers to find the trademark holder. Where the holder of a vanity telephone number promotes it in a way that causes a likelihood of confusion, the holder has engaged in an infringing use. American Airlines, 622 F. Supp. at 682 (mere use of telephone number is not infringing, but misleading use of trademarked term in yellow pages
advertisement is infringing). But, where, as with NSI, the pure machine-linking function is the only use at issue, there is no trademark use and there can be no infringement.

In the ordinary trademark infringement case, where there is no question that the defendant used the mark, the analysis proceeds directly to the issue of whether there is a likelihood of confusion. Here, however, because NSI has not used Lockheed's service mark in connection with goods or services, the Court need not apply the test for likelihood of confusion. NSI, therefore, is entitled to judgment as a matter of law on the section 32 claim.

1. Printer and Publisher Liability Under 15 U.S.C. §1114(2)(A), (B)

Lockheed asserts that NSI has infringed its service mark as a "printer" of the mark under 15 U.S.C. §1114(2)(A). This assertion misapprehends NSI's function as a domain name registrar. To the extent that registrants of SKUNK WORKS-type domain names infringed the mark, they did so by using it on Web sites or other Internet resources in a way that created a likelihood of confusion as to source or sponsorship. NSI is not an Internet service provider. It does not provide host computers for Web sites on other Internet resources. NSI's role is restricted to publishing a list of domain names, their holders, and the IP numbers of the domain name servers that perform the directory function associated with the domain names. (Graves Decl. ¶ 10.)

NSI's role is fundamentally dissimilar from that of telephone directory publishers whose conduct has been found enjoinal under §1114(2)(A). See Century 21 Real Estate Corp. of Northern Illinois v. R.M. Post Inc., 8 U.S.P.Q.2d 1614, 1617 (N.D. Ill. 1988) (denying motion to dismiss where yellow pages publishers were alleged to have printed infringing trademark in listing of former licensee who no longer had right to use trademark). There, the telephone directory printers supplied the material that directly caused the likelihood of confusion. In the domain name context, the domain name registration itself does not infringe the trademark. Infringement occurs when the domain name is used in certain ways. For example, a domain name may infringe trademark rights when it is used in connection with a Web site that advertises services in competition with those of the trademark owner. See, e.g., Cardservice International, Inc. v. McGee, 950 F.Supp. 737, 738 (E.D. Va. 1997); Comp Examiner Agency, Inc. v. Juris, Inc., 1996 WL 376600 (C.D. Cal. 1996). Where domain names are used to infringe, the infringement does not result from NSI's publication of the domain name list, but from the registrant's use of the name of a Web site or other Internet form of communication in connection with goods or services. NSI is not a "printer or publisher" of Web sites, or any other form of Internet "publication." As discussed below in the section on contributory infringement, NSI's involvement with the use of domain names does not extent beyond registration. NSI's liability cannot be premised on an argument that it prints or publishers the list of domain names, because the list is not the instrument or forum for infringement. NSI's liability, if it exists at all, would stem from registrants' use of domain names in connection with other services not provided by NSI. This type of liability is properly analyzed under contributory liability doctrine, not as printer and publisher liability under §1114(2)(A).

C. Unfair Competition Under Lanham Act Section 43(a), 15 U.S.C. §1125(a)

Lockheed has followed the common practice of alleging unfair competition under section 43(a) of the Lanham Act along with trademark infringement under section 32. Both causes of action depend on a demonstration of a likelihood of confusion. 1 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition §2:8 (1997). Federal unfair competition requires use of the mark in connection with goods or services, 15 U.S.C. § 1125(a)(1). As discussed above, NSI's acceptance of registrations for domain names resembling SKUNK WORKS is not a use of the mark in connection with goods or services.

A recent district court decision illustrates the application of federal unfair competition law to the domain name context. Juno Online Servs., L.P. v. Juno Lighting, Inc., ___ F.Supp. ___, 1997 WL 613021 (N.D. Ill. Sept. 29, 1997). During a dispute over the domain name "juno.com," Juno Lighting registered the domain name "juno-online.com" in the hopes of persuading Juno Online Services to switch its e-mail service to that domain name. Juno Online sued Juno Lighting for federal unfair competition. The district court dismissed the unfair competition claim because Juno Online alleged only that Juno Lighting
registered the name with NSI, and did not allege further use of the name to create a Web site or to advertise its services. Id. at *8-*9. The court held that registration of a trademark as a domain name does not constitute use of the trademark on the Internet in connection with goods or services, and therefore was not prohibited by action 43(a). Id. This reasoning applies more strongly to NSI which has not registered domain names resembling SKUNK WORKS for its own use, but has merely accepted domain name registrations from others.


Trademark dilution laws protect "famous" marks from certain unauthorized uses regardless of a showing of competition, relatedness or likelihood of confusion. The federal dilution statute entitles the owner of a famous mark to enjoin "another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark ..." 15 U.S.C. §1125(c)(1). Dilution is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of -- (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake or deception." 15 U.S.C. §1127. The Federal Trademark Dilution Act specifically excludes non-commercial use of a mark from its coverage. 15 U.S.C. §1125(c)(4)(B).

NSI's acceptance of domain name registrations is not a "commercial use" within the meaning of the Federal Trademark Dilution Act. Lockheed argues that NSI engages in commercial use because the registration of SKUNK WORKS-type domain names inhibits Lockheed's ability to use its service mark as a domain name. (Opp'n at 29.) Lockheed contends that NSI's conduct is similar to that of the defendant in Panavision Int'l L.P. v. Toeppen, 945 F.Supp. 1296, 1299 (C.D. Cal. 1996). In Panavision the defendant, Toeppen, was a "cybersquatter," an entrepreneur who made a business of registering trademarks as domain names for the purpose of selling them later to the trademarks' owners. Panavision, 945 F.Supp. at 1303. The court held that Toeppen "traded on the value of the marks as marks by attempting to sell the domain names to Panavision." Id. The court found that "[t]his conduct injured Panavision by preventing Panavision from exploiting its marks and it injured customers because it would have been difficult to locate Panavision's web site if Panavision had established a web site under a name other than its own." Id.; see also Internic Inc. v. Toeppen, 947 F.Supp. 1227, 1239 (N.D. Ill. 1995) (holding that defendant's use of the mark was diluting because it prevented plaintiff from using it). Lockheed's argument implies that any conduct that makes it more difficult for Lockheed to establish a presence on the Internet is diluting conduct. This argument is flawed. In Panavision and Internic, the fact that the defendant's conduct impeded plaintiff's use of its trademark as a domain name was not the determining factor in finding that the defendant's use was diluting. If impeding use of the trademark as a domain name were the only factor, the court in Panavision would not have asserted that registration of a trademark "as a domain name, without more, is not a commercial use of the trademark and therefore not within the prohibitions of the Act." Panavision, 945 F.Supp. at 1303. All prior domain name registrations corresponding to words in a trademark impede the trademark owner's use of the same words for use as a domain name. The Internet, however, is not exclusively a medium of commerce. The non-commercial use of a domain name that impedes a trademark owner's use of that domain name does not constitute dilution. [4] In Internic and Panavision, the defendant's use was commercial because the defendant sought to "arbitrage" the trademarks for their value as domain names. Internic, 947 F.Supp. at 1239; Panavision, 945 F.Supp. at 1303. Lockheed argues that NSI is engaged in commercial use of its service mark because NSI seeks to maximize the number of domain names registered in order to maximize its revenue and profits. (Opp'n at 27.) Lockheed cites statements in NSI's Initial Public Offering registration statement ("IPO") [5] to the effect that part of NSI's strategy for growth is to stimulate demand for domain names in targeted customer segments, including among trademark owners. (Id.; see Rierson Decl. Ex. B.) Lockheed contends that like Toeppen, NSI trades on the value of domain names by "selling" registrations to as many people as possible. (Id.) NSI, however, does not trade on the value of domain names as trademarks. NSI's use of domain names is connected to the names' technical function on the Internet to designate computer addresses, not to the names' trademark function to distinguish goods and services. The fact that NSI makes a profit from the technical
function of domain names does not convert NSI's activity to trademark use. See New Kids, 971 F.2d at 309. The Court does not question that a domain name which is easily deducible from a trademark is a valuable asset to the trademark owner. Such a domain name makes it easier for the trademark owner's customers to find the trademark owner's Internet resources such as Web sites. But a domain name's correspondence to a trademark does not make the domain name any more valuable to NSI, whose only interest in a domain name is as a pointer to an IP number. NSI, unlike the defendant in Intermatic and Panavision, does not make a commercial use of domain names by trading on their value as trademarks.

Because the Court finds as a matter of law that NSI does not make commercial use of domain names as trademarks, Lockheed cannot prevail on its dilution claim. The Court therefore does not address the other dilution elements.

E. Contributory Infringement

Lockheed asserts that NSI is liable for contributory infringement of the SKUNK WORKS mark because NSI accepted registrations of domain names similar to the mark and refused to cancel the registrations in response to Lockheed's demands. Contributory infringement doctrine extends liability to reach manufacturers and distributors who do not themselves use the mark in connection with the sale of goods, but who induce such use by supplying goods to direct infringers. Liability for contributory infringement requires that the defendant either "(1) intentionally induces another to infringe on a trademark or (2) continues to supply a product knowing that the recipient is using the product to engage in trademark infringement." Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) (citing the test set forth in Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844, 853-54, 102 S. Ct. 2182, 2188 (1982)). Lockheed does not contend that NSI induced infringement. No evidence has been presented to indicate inducement. The issue, therefore, is whether Lockheed has created a genuine issue as to the knowledge prong of the Inwood test.

Following Inwood, courts have extended liability for trademark infringement beyond direct infringers, but only under certain circumstances. Mini Maid Servs. Co. v. Maid Brigade Sys., Inc., 967 F.2d 1516, 1521 (11th Cir. 1992). The clearest circumstances for extending liability are those presented by Inwood itself. There, a pharmaceutical manufacturer supplied generic drugs that some pharmacists mislabeled as brand-name drugs. Each extension of contributory liability doctrine beyond defendants who manufacture or distribute a mislabeled product has required careful examination of the circumstances to determine whether knowledge of infringement should be imputed to the alleged contributory infringer. See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148 (7th Cir. 1992) (holding that the landlord/tenant relationship between a flea market operator and vendors provides a basis for extending contributory trademark infringement doctrine in circumstances indicating willful blindness of the flea market operator toward the vendors' blatantly infringing acts); Fonovisa, 76 F.3d at 265 (same) Mini Maid, 967 F.2d at 1522 (extending contributory liability doctrine to a franchisor/franchisee relationship but holding that the district court erred in finding contributory liability based on the franchisor's failure to supervise the franchisee with reasonable diligence). Lockheed now asks that the Court extend contributory liability to the relationship between a domain name registrar and domain name registrants who are alleged to have directly infringed Lockheed's mark.

NSI is involved only in the registration of domain names, not in the use of domain names in connection with goods and services on the Internet. (Graves Decl. ¶ 10); cf, Intermatic, 947 F.Supp. at 1231-32 (noting that there is no technical connection between domain name service and contents of Web sites or other Internet resources). NSI does not provide the other services needed to use the domain name in association with a Web site or other means of communication on the Internet. The services necessary to maintain a Web site, such as an IP address, communications, computer processing and storage are performed by Internet service providers ("ISP") who provide the host computers and connections necessary for communications on the Internet. It is not necessary to secure a second-level domain name registration in order to establish a presence on the Internet. Users may simply use the second-level domain name of the ISP. Where domain name registration is necessary, the ISP usually acts as an agent to secure and maintain the registration. See Domain Name System, Hearings Before the Subcomm. on Basic Research of the House Science Comm., 105th Cong., 1997 WL 14151463 (September 30, 1997) (testimony of Barbara A. Dooley, Executive Director, Commercial Internet Exchange

Association) (noting that most users rely on ISPs to act as agents to secure and maintain registrations, and that ISPs are the primary providers with a close relationship to end users).

The registration of a domain name, without more, does not amount to infringement of a mark similar to the name. Panavision, 945 F. Supp. at 1303. Infringing acts occur when a domain name is used in a Web site or other Internet form of communication in connection with goods or services. Planned Parenthood Fed’n of America v. Bucci, 42 U.S.P.Q.2d 1430, 1437 (S.D.N.Y. 1997). After a domain name is registered, NSI’s involvement is over. NSI is not part of the process of linking domain names with potentially infringing resources such as Web sites. NSI does not require holders to use domain names for Web sites or any other form of Internet communication. [6] Nor do domain name holders need NSI’s permission to do so.

Because NSI’s involvement with the Internet is remote from domain name uses that are capable of infringement, Lockheed’s reliance on the flea market cases, Fonovisa and Hard Rock, is misplaced. In Hard Rock, the Seventh Circuit noted that the common law of landlord/tenant relations imposes vicarious liability on a landlord who knows or has reason to know of the tortious activity of those whom the landlord permits on the landlord’s premises. Hard Rock, 955 F.2d at 1149. Because the landlord/tenant standard is similar to the Inwood standard for contributory infringement by manufacturers, the court held that the Inwood standard should apply to flea market operators who lease space to vendors. Id. This holding was further supported by the district court’s finding that the flea market operator not only rented space, but also advertised and promoted the activity on its premises, sold tickets and directly supervised the premises. Id. at 1148. In Fonovisa, the Ninth Circuit adopted Hard Rock's analogy between landlord/tenant vicarious liability and trademark law contributory liability in order to extend the Inwood standard to the flea market context. Fonovisa, 76 F.3d at 265. There, too, the court found that the flea market operator provided more than space, and was directly and substantially involved in the businesses of the infringing vendors. Id. at 264.

The flea market operators directly controlled and monitored the premises. NSI neither controls nor monitors the Internet. A domain name, once registered, can be used in connection with thousands of pages of constantly changing information. While the landlord of a flea market might reasonably be expected to monitor the merchandise sold on his premises, NSI cannot reasonably be expected to monitor the Internet. See American Civil Liberties Union of Georgia v. Reno, 929 F. Supp. 824, 832 (E.D. Pa. 1996), aff’d, 117 S.Ct. 2329 (1997) (“There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.”). NSI’s role in the Internet is distinguishable from that of an Internet service provider whose computers provide the actual storage and communications for infringing material, and who therefore might be more accurately compared to the flea market vendors in Fonovisa and Hard Rock. [7] See Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1373 (N.D. Cal. 1995).

Because NSI’s involvement with potentially infringing uses of domain names is remote, the Court finds that it is inappropriate to extend contributory liability to NSI absent a showing that NSI had unequivocal knowledge that a domain name was being used to infringe a trademark.

1. NSI’s Knowledge

The mere assertion by a trademark owner that a domain name infringes its mark is not sufficient to impute knowledge of infringement to NSI. The use of an identical or similar mark does not necessarily constitute infringement. In order to be infringing, such use must be in connection with goods or services that are competitive with, or at least related to, the goods or services for which the trademark has been registered or used in commerce. AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348 (9th Cir. 1979). The use must also cause a likelihood of confusion as to origin or sponsorship. Id. Whether a use is likely to cause confusion depends on numerous variables including the strength of the mark, the proximity of the goods, the similarity of the marks, evidence of actual confusion, marketing channels used, the type of goods and degree of care used by purchasers, the defendant’s intent in selecting the mark, and the likelihood of expansion of product lines. Eclipse Associates Ltd. v. Data General Corp., 894 F.2d 1114, 1117 (9th Cir. 1990).
NSI's registration form requires the applicant to state the purpose of the domain name registration. Lockheed contends that NSI receives sufficient information on the form to know whether a domain name registration will be used to infringe a mark, and that the use of the form satisfies the knowledge element of contributory infringement doctrine. The form instructs the applicant to "[b]riefly describe the domain name Registrant and the purpose for which this domain name is being applied." (Quinto Decl. in Opp'n to Ex Parte Application for Order Finding Civil Contempt, Ex. C.) Infringement depends on likelihood of confusion. The likelihood of confusion test examines the totality of circumstances under which a mark is used. See Eclipse, 894 F.2d at 1118. The outcome of the test cannot be predicted from an examination of the mark and the domain name in connection with a brief statement of the purpose for which the mark is being used. A reasonable person in NSI's position could not presume infringement even where the domain name is identical to a mark and registered for use in connection with a similar or identical purpose. See Taj Mahal Enterprises, Ltd. v. Trump, 745 F.Supp. 240 (D.N.J. 1990) (finding insufficient likelihood of confusion between TAJ MAHAL mark as used by restaurant and TAJ MAHAL mark as used by casino and hotel complex which included several restaurants); Church of the Larger Fellowship, Unitarian Universalist v. Conservation Law Foundation of New England, Inc., 221 U.S.P.Q. 869 (D. Mass 1983) (finding insufficient likelihood of confusion between plaintiff's use of CLF mark for direct mail charitable solicitation and defendant's use of CLF mark for same purpose in same city); Pump, Inc. v. Collins Management, Inc., 746 F.Supp. 1150 (D. Mass. 1990) (granting defendant's motion for summary judgment, finding insufficient likelihood of confusion between plaintiff's use of PUMP for purpose of promoting rock band and defendant's use of PUMP for same purpose). The receipt of a brief statement of purpose from domain name applicants does not give NSI sufficient information for the Court to impute knowledge of future infringing uses to NSI.

An owner's rights in a trademark do not remain stable over time. The scope of the owner's rights is subject to contraction if the trademark is abandoned or becomes generic for all or part of the goods or services identified. This dynamic nature of trademark rights increases their inherent uncertainty. Lockheed concedes that the Lanham Act recognizes that a mark may become generic for a portion of the goods or services for which it is registered, causing the owner to lose trademark protection against use of the mark in connection with such goods. (Lockheed's Separate Statement of Genuine Issues at 11); 15 U.S.C. §1064 (providing for cancellation of trademark registration with respect to goods and services for which mark has become generic). NSI submits evidence of numerous third-party uses of the term "skunk works" to describe a type of corporate management style. (Jones Decl. Exs. 14-44.) (newspaper, magazine and trade journal articles describing "skunk works" at companies including IBM, Chrysler, General Motors, Buick, Compaq, Patagonia and Bell Atlantic). "Skunk works" is defined in the 1996 American Heritage Dictionary as "[a] small loosely structured corporate research and development unit or subsidiary formed to foster innovation."(Jones Decl. Ex. 9.) Parallel generic meanings do not remove trademark protection over uses of the trademarked term to distinguish the source of goods. 2 McCarthy §12:3. The trademark owner, however, does not have protection against purely generic or nominative uses of the term that do not serve to distinguish goods or services. [8] 15 U.S.C. §1064; New Kids on the Block v. New America Pub. Inc., 971 F.2d 302 (9th Cir. 1992); Lucasfilm Ltd. v. High Frontier, 622 F.Supp. 931 (D.D.C. 1985). The existence of numerous legitimate, non-infringing uses of the term "skunk works" further illustrates the uncertainty inherent in the question of whether NSI knew or had reason to know of infringing uses of domain name registrations. [9]

Additionally, trademark law permits multiple parties to use and register the same mark for different classes of goods and services. NSI points to United States Trademark Registration 1,941,484 for SKUNKWORKS PUBLISHING for use on printed publications relating to business (Jones Decl. Ex. 45.) The applicant was required to disclaim any rights to PUBLISHING apart from the mark as shown. (Id. Ex. 46.) Where a party disclaims portions of the mark, the un-disclaimed portions are considered "dominant" for purposes of customer confusion. In re Dixie Restaurants, Inc., 105 F.3d 1405, 1407 (Fed. Cir. 1997) (holding that there was a likelihood of confusion between THE DELTA CAFE and DELTA where the owner of the former trademark disclaimed CAFE). Therefore, for purposes of determining possible infringement by the domain name "skunkworks.com," SKUNK WORKS and SKUNKWORKS PUBLISHING are the same mark. If NSI had received letters from both Lockheed and the registered owner of SKUNKWORKS PUBLISHING, it would have no basis for deciding which party's rights placed NSI at greater risk of liability for contributory infringement. The proper course of
action in such a situation would be for NSI to initiate an interpleader action, placing the domain name in the registry of the court and allowing the claimants to adjudicate the question of whether one claimant's trademark rights allowed exclusive use of the mark as an Internet domain name. (See Grave Decl. Ex. 1 (domain name dispute policy).)

In holding that the degree of uncertainty over infringing uses of domain names makes it inappropriate to impose contributory liability on NSI, the Court is not making new trademark rules for the Internet. Contributory infringement doctrine has always treated uncertainty of infringement as relevant to the question of an alleged contributory infringer's knowledge. See Mini Maid, 967 F.2d at 1521 (instructing district court to consider extent and nature of alleged infringement in determining whether to impute knowledge to alleged contributory infringer); Restatement (Third) of Unfair competition §26 cmt. a (993) (noting that a person's liability for contributory infringement "depends upon the nature of the business relationship between the person and the direct infringer and the knowledge attributable to the person on the basis of that relationship"). A trademark owner's demand letter is insufficient to resolve this inherent uncertainty. Coca-Cola Co., v. Snow Crest Beverages, 64 F.Supp. 980 (D. Mass. 1946), aff'd, 162 F.2d 280 (1st. Cir. 1947), a seminal contributory infringement case, addressed the contention offered here by Lockheed that an attorney's demand letter should be sufficient to impute knowledge of infringement. There, Coca-Cola asserted that Snow Crest had contributiorily infringed its mark by selling "Polar Cola" to bartenders who sometimes mixed the soda into customers' "rum and Coke" drinks. Coca-Cola, 64 F.Supp. at 989. Coca Cola asserted that Snow Crest should have known about the infringement because Coca-Cola's counsel had told Snow Crest's president of the bartending practice. The court found that such "lawyer's argumentative talk" was insufficient to establish that a reasonable business person in Snow Crest's position should have concluded that its products were being used to infringe. Id. at 990. The court reasoned that if it imputed knowledge to the defendant based on Coca-Cola's blanket demand, the court would be expanding Coca-Cola's property right in its trademark, allowing Coca-Cola to secure a monopoly over the entire mixed drink trade Id. The same reasoning applies here. Lockheed's argument would require the Court to impute knowledge of infringement to NSI in circumstances where the use of the term "skunk works" in a domain name may or may not be infringing. Such an expansion of contributory liability would give Lockheed a right in gross to control all uses of "skunk works" in domain names.

Lockheed relies on a copyright contributory infringement case, Religious Technology Center v. Netcom On-Line Communication Servs., Inc., 907 F.Supp. 1361 (N.D. Cal. 1995), for the proposition that only a low level of certainty as to infringement should be required to impute knowledge to NSI. There, the court rejected an Internet service provider's argument that its knowledge of infringement must be unequivocal in order for it to face contributory liability. Id. at 1374. At the same time the court noted that a "mere unsupported allegation of infringement by a copyright owner" is not enough to impute knowledge to an Internet service provider. Id. The court noted that where infringement is uncertain for a variety of reasons such as lack of copyright notice or a colorable fair use defense, the Internet service provider's "lack of knowledge will be found reasonable and there will be no liability for contributory infringement ... ." Id. Because the property right protected by trademark law is narrower than that protected by copyright law, liability for contributory infringement of a trademark is narrower than liability for contributory infringement of a copyright. Sony Corp. v. Universal City Studios, Inc. 464 U.S. 417, 439 n.19, 104 S.Ct. 774, 787 n. 19, (1984). Unlike trademark law, copyright law gives owners a generalized right to prohibit all copying, provided that the owner's rights are valid and the material copied is original. Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 340 111 S.Ct. 1282, 1296 (1991). Trademark law, on the other hand, tolerates a broad range of non-infringing uses of words that are identical or similar to trademarks.

2. Knowledge as to Specific Registrants

Lockheed's complaint alleges contributory infringement in connection with four specific registrations of SKUNK WORKS-type domain names. In addition, Lockheed has submitted evidence in opposition to summary judgment of four subsequent registrations of domain names similar to SKUNK WORKS. (Quinto Decl. Ex. E, H, L, M.) As to all of the domain name registrations, the Court finds that the alleged infringing activity did not give NSI knowledge or reason to know that its domain name registration service was being used to infringe Lockheed's service mark.
Two of the four original registrants never used their domain name in connection with a Web site or other form of Internet communication that would create a likelihood of confusion. [10] The other two registrants used their domain names, one in association with Web site, [11] and one as an e-mail address. [12] As discussed above, however, NSI is not involved with uses of domain names in connection with Internet resources such as Web sites and e-mail. Therefore, the Court cannot impute knowledge of potential infringement merely from the fact that such uses occurred. NSI, as a domain name registrar, has no affirmative duty to police the Internet in search of potentially infringing uses of domain names. Hard Rock, 955 F.2d at 1149 (flea market operator had no affirmative duty to take precautions against infringement by vendors); MDT Corp. v. New York Stock Exchange, Inc., 858 F.Supp. 1028, 1034 (C.D. Cal. 1994). Lockheed's May 7, 1996 and June 18, 1996 demand letters do not notify NSI of any post-registration uses such as Web sites or e-mail, but merely assert that the domain names have been registered and demand their cancellation. (Quinto Decl. Exs. A & C.) Considering the uncertainty inherent in any determination that use of a domain name is infringing, the Court finds that Lockheed has failed to raise a triable issue as to NSI's knowledge of infringing uses of its services.

The parties have presented no evidence regarding use on the Internet of three of the four domain names registered since Lockheed filed its complaint. The remaining registration, that of Peter Pasho, was used in connection with a Web site. Lockheed has presented a print-out of a Web page associated with the domain name "theskunkworks.com," registered to Pasho. (Quinto Decl. Ex. N.) The Web site includes a depiction of Lockheed's SR-71 spy plane and a definition of the term "skunk works" that refers to the Lockheed facility. (Id.) Lockheed argues that the use of the domain name "theskunkworks.com" in connection with this Web site raises the possibility of confusion over possible sponsorship by Lockheed. This argument is tenuous given the fact that the services promoted on the page are Web site design, not aerospace design. But Lockheed makes a colorable claim that where a strong mark is concerned, the use of a trademark on different products can be infringing if customers would be led to infer sponsorship. HMH Publishing Co. v. Brincat, 504 F.2d 713, 717 (9th Cir. 1974).

Lockheed, however, has not demonstrated that NSI was involved with or had reason to know about this Web site. NSI's management of the domain name registration process does not include a content review of Web sites and other Internet resources associated with a domain name. Although the use of the domain name "theskunkworks.com" might contribute to a likelihood of confusion as to sponsorship, NSI did not supply the domain name to Pasho. Registrants choose their own domain names. NSI, therefore, cannot be compared to a manufacturer who chooses to make generic pills that can be easily substituted for pills with protected trade dress; Inwood, 456 U.S. at 848-50, 102 S.Ct. at 2185-86, or a mattress manufacturer who chooses to cover box springs with fabric pattern identical to that retailed by another company. Sealy, Inc. v. Easy Living, Inc., 743 F.2d 1378, 1382 (9th Cir. 1984). Nor can NSI be compared to the flea market operators who provide space, parking, food service and advertising to vendors selling infringing merchandise. If Pasho's use of the domain name "theskunkwork.com" creates a likelihood of confusion, it does so only in combination with the content of the Web page. The Web page exists on Pasho's computer or on an Internet service provider's computer. NSI does not provide computer storage, processing or communications for Web sites. NSI's role in Pasho's possible infringement is therefore not similar to the role of the flea market vendors, who provided a substantial portion of the services needed for the vendor's infringing activities, and on whose premises the infringing activities occurred. Fonovisa, 76 F.3d 259, 256; Hard Rock, 955 F.2d at 1149.

3. Conclusion as to Contributory Infringement

Lockheed bears the burden of proving that NSI induced infringement, or continued to supply a product when it knew or should have known that its customers were using the product to infringe Lockheed's mark. See Inwood, 456 U.S. at 853-54, 102 S.Ct. at 2188. Lockheed asserts in its Separate Statement of Genuine Issues that NSI is not entitled to summary judgment because NSI "has not adduced any evidence" regarding infringement by its registrants. (Plaintiff's Separate Statement ¶ 23.) It is not NSI's burden on summary judgment to negate the elements of Lockheed's case. The moving party on summary judgment need not produce evidence showing the absence of a genuine issue of material fact with respect to issues on which the non-moving party bears the burden of proof at trial. Celotex Corp. v. Catrett, 477 U.S. 317, 325, 106 S.Ct. 2540, 2554 (1986). The moving party need only point out to the
district court that there is an absence of evidence to support the non-moving party's case. Id.

NSI has met this burden. Lockheed's evidence would only establish liability for contributory infringement if NSI had an affirmative duty to police the Internet for infringing uses of Lockheed's service mark. No such duty exists. Lockheed's evidence does not show that NSI was involved in infringing activity or that it knew or had reason to know that its services were being used to infringe Lockheed's service mark. The Court finds that knowledge of infringement cannot be imputed to NSI because of the inherent uncertainty of trademark protection in domain names. Even after receiving Lockheed's demand letters NSI would not have reason to know that the holders of SKUNK WORKS-type domain names were infringing. Trademark law does not give Lockheed the right to interfere with all uses of the term "skunk works" by current domain name holders. Because of the inherent uncertainty of a trademark owner's right to stop others from using words corresponding to the owner's trademark in a domain name, the Court finds that an extension of contributory liability here would improperly broaden Lockheed's property rights in its service mark.

III. Conclusion

The Court finds that NSI's use of domain names is connected with their technical function to designate computers on the Internet, not with their trademark function to identify the source of goods and services. Because Lockheed cannot establish that NSI has used its service mark in connection with goods or services or with the sale, offer for sale, distribution or advertising of goods and services, the Court grants summary judgment for NSI on the direct infringement and unfair competition claims under 15 U.S.C. §§1114(1), 1125(a).

Because the Court finds that NSI's acceptance of domain name registrations is not a commercial use within the meaning of the Federal Trademark Dilution Act, 15 U.S.C. §1125(c), the Court grants summary judgment for NSI on the dilution claim.

Because NSI has demonstrated that Lockheed cannot establish that NSI knew or had reason to know that its domain name registration service was used to infringe Lockheed's mark, the Court grants summary judgment for NSI on the contributory infringement claim.

Because summary judgment on the above claims is based on Lockheed's lack of a legal right to control the domain name registration process, there is no case or controversy between these parties. Therefore, the Court grants NSI's motion for summary judgment as to Lockheed's declaratory judgment cause of action.

If the Internet were a technically ideal system for commercial exploitation, then every trademark owner would be able to have a domain name identical to its trademark. But the parts of the Internet that perform the critical addressing functions still operate on the 1960s and 1970s technologies that were adequate when the Internet's function was to facilitate academic and military research. Commerce has entered the Internet only recently. In response, the Internet's existing addressing systems will have to evolve to accommodate conflicts among holders of intellectual property rights, and conflicts between commercial and non-commercial users of the Internet. "In the long run, the most appropriate technology to access Web sites and e-mail will be directories that point to the desired Internet address. Directory technology of the necessary scale and complexity is not yet available, but when it is developed it will relieve much of the pressure on domain names." Domain Name System, Hearing Before the Subcommittee on Basic Research of the House Science Committee, 105th Cong., 1997 WL 14151463 (September 30, 1997) (testimony of Barbara A. Dooley, Executive Director, Commercial Internet Exchange Association). No doubt trademark owners would like to make the Internet safe for their intellectual property rights by reordering the allocation of existing domain names so that each trademark owner automatically owned the domain name corresponding to the owner's mark. Creating an exact match between Internet addresses and trademark will require overcoming the problem of concurrent uses of the same trademark in different classes of goods and geographical areas. Various solutions to this problem are being discussed, such as a graphically-based Internet directory that would allow the presentation of trademark in conjunction with distinguishing logos, new top-level domains for each class of goods, or a new top-level domain for trademarks only. The solution to the current
difficulties faced by trademark owners on the Internet lies in this sort of technical innovation, not in attempts to assert trademark rights over legitimate non-trademark uses of this important new means of communication.

DATED: November 17, 1997

DEAN D. PREGERSON

United States District Judge

FOOTNOTES

1. [Return to Text] One solution to this problem is for businesses to stake their claims on higher level domain names. For example, a business could use an Internet service providers's second-level domain and place its trademark in the third-level domain. Thus, if Acme Plumbing uses the Microsoft Network, its web site could be at America Online with the address "acme.aol.com." The drawback of this solution is that it requires customers to guess as to the second-level domain.

2. [Return to Text] Although NSI's policy does not refer explicitly to interpleader actions, NSI has attempted to deposit domain names in the registry of the court by bringing interpleader actions. None of the actions have been successful. (Graves Depo. at 104-05.) In the one reported case arising from this interpleader policy, the district court dismissed NSI's interpleader action. Network Solutions Inc. v. Clue Computing Inc., 946 F.Supp 858 (D. Colo 1996). Clue Computing had sued NSI in state court to prevent cancellation of its domain name registration, "clue.com," at the behest of Hasbro, Inc., which sought to use the domain name for a Web site based on the board game "Clue." Hasbro had presented NSI with the federal registration of Hasbro's CLUE trademark, and demanded that NSI cancel Clue Computing's domain name registration. NSI attempted to extricate itself from between the two claimants by filing an interpleader action. However, the district court found that NSI was not a disinterested stakeholder because Clue Computing had accused it of breaching the domain name registration contract. 946. F.Supp. at 861.

3. [Return to Text] The Court takes judicial notice of a draft document prepared by the staff in the Office of the Assistant Commissioner for Trademarks of the United States Patent and Trademark Office entitled "Observations Concerning the Examination of Applications for Registration of Domain Names in the Trademark Office." This document directs trademark examiners to determine whether a domain name submitted for trademark registration functions only as a locator of a business on the Internet, in which case registration should be refused because the domain name is not serving a trademark function. While the Court's conclusion does not depend on this document or any Patent and Trademark Office policy that it might reflect, the Court notes that trademark examiner practice is consistent with the view that the registration or a domain name with NSI for use on the Internet, without more, is not a commercial use of the name as a trademark under the Lanham Act. See also, 2 Gilson, supra, § 5.11 [5], at 5-243-44 (noting Patent and Trademark Office practice regarding use-based registration of domain names as trademarks).

4. [Return to Text] It is important to note that impending access to a domain name is not the same thing as impending access to the Internet. Even if the trademark owner cannot establish a "vanity" domain name, the owner remains free to promote the trademark on the Internet by using the trademark in the content of a web site. A web site's content is not connected to or restricted by the domain name under which it is accessed. See David J. Loundy, A Primer on Trademark Law and Internet Addresses, 15 J. Marshall J. Computer & Info. L. 465, 480 n. 86 (1997). In addition, the trademark owner may use the trademarked words as a third-level domain name, or as a second-level domain name in combination with letters that distinguish it from previously registered second-level domains. A domain name dispute between Acme Plumbing and Acme Pizza, for example, can be resolved by adding more information to the second-level domain names, as in "acmeplumbing.com" and "acmepizza.com."

5. [Return to Text] NSI objects to the IPO as inadmissible hearsay. The IPO is admissible as an admission of a party opponent. Fed.R.Evid 801 (d)(2).
6. [Return to Text] Lockheed asserts that NSI's domain name dispute policy requires registrants to use their domain names. (Quinto Decl. in Opp'n to Ex Parte Application for Civil Contempt ¶ 8.) Lockheed points to the section of the policy that requires registrants "to have operational name service from at least two operational domain name servers ... ." (Id., Ex. E.) This language is quoted from a section of the policy under the heading "Connectivity." This section does not require the registrant to connect the domain name with any content on the Internet, such as a web site. It merely requires the registrant to secure the use of two domain name servers to list the domain name in connection with an IP number. Requiring registrants to link their domain names with IP numbers is not the same thing as requiring registrants to use their domain names on the Internet.

7. [Return to Text] The Court notes, however, that the tort law analogy used in Fonovisa and Hard Rock probably would not apply to Internet service providers and better than it applies to NSI. Even though Internet service providers directly provide the storage and communications facilities for Internet communication, they cannot be held liable merely for failing to monitor the information posted on their computers for tortious content. See Zeran v. America Online, Inc., ___ F.3d ___, 1997 WL 701309, at *3 (4th Cir. Nov. 12, 1997) (noting that Congress created a tort immunity for Internet service providers in the Communications Decency Act of 1996, 47 U.S.C. § 230, because "[i]t would be impossible for service providers to screen each of their millions of postings for possible problems"); but see 47 U.S.C. § 230(d)(2) (providing that the tort immunity does not limit or expand any law pertaining to intellectual property).

8. [Return to Text] The uncertainty of Lockheed's rights over potentially generic uses of words similar to its mark is made greater in this case by the breadth of the preemptive rights asserted by Lockheed. NSI propounded an interrogatory asking Lockheed to identify all alphaneumeric strings whose inclusion in a domain name would infringe Lockheed's service mark. Lockheed objected to the interrogatory as unduly burdensome, and answered with 24 phrases that would infringe, including the word "skunk" (Jones Decl. Ex. 1.)

9. [Return to Text] Internet users may also have a free speech interest in non-infringing uses of domain names that are similar or identical to trademarks. See American Civil Liberties Union of Georgia v. Miller, ___ F.Supp ___, 1997 WL 552487, at *4 (N.D. GA. June 23, 1997) (invalidating as overbroad statute that criminalized certain uses of trademarks on the internet by persons other than trademark owner because statute would have prohibited "use of trade names or logos in non-commercial educational speech, news, and commentary -- a prohibition with well-recognized First Amendment problems").

10. [Return to Text] Seng-Poh Lee's "skunkworks.com" name was used to established an e-mail forwarder. Mr. Lee never received or sent e-mail using the domain name. (Jones Decl. Ex. 3.) After receiving a cease-and-desist letter from Lockheed, Mr. Lee canceled his domain name registration. The domain name became generally available and was registered to a new user, Grant Smith, in 1996.

Ken Hoang's "skunkworks.net" was not used in association with a web site or any other Internet form of communication. (Jones Decl. Ex. 6.)

11. [Return to Text] Roger Barski's "skunkworks.com" domain name was associated with a web site offering Mr. Barski's services as a web site designer. (Jones Decl. Ex. 5.) After receiving Lockheed's cease-and-desist letter, Mr. Barski canceled the Internet service provider account that had supplied domain name service for "skunkworks.com." Without domain name service, the domain name is effectively removed from the Internet, because users who attempt to access Internet resources associated with the domain name receive only an error message. (Id.).

12. [Return to Text] Kathy Huber's "skunkwrks.com" was not associated with a Web site, but was associated with an e-mail address for Ms. Huber's former company, Skunkworks Marketing Labs. (Jones Decl. Ex. 4.)
I. INTRODUCTION

Influential futurist Ithiel de Sola Pool wrote:

For copyright, the implications [of electronic publishing] are fundamental. Established notions about copyright become obsolete, rooted as they are in the technology of print. The recognition of a copyright and the practice of paying royalties emerged with the printing press. With the arrival of electronic reproduction, these practices become unworkable. Electronic publishing is analogous not so much to the print shop of the eighteenth century as to word-of-mouth communication, to which copyright was never
applied.\(^{(1)}\)

The emergence of electronic networks has undeniably placed significant pressure on our existing intellectual property system. As with each new technological advance, copyright law must adjust to fit the new circumstances presented by the Internet. Until law and technology reach an equilibrium, many predict that intellectual property creators will be reluctant to create works for the Internet environment since creators will be unable to protect their copyright interests.\(^{(2)}\) Others have argued that only minor adjustments are necessary to fit copyright law to electronic networks such as the Internet.\(^{(3)}\) Still others—a distinct minority—believe that copyright law has become less important in the age of electronic networks, and that productio of intellectual property will continue unabated even without powerful copyright rights.\(^{(4)}\)

Unlike Professor Pool, we have the benefit of a few years of empirical evidence to draw upon analyzing the effects of electronic networks on intellectual property. This article analyzes some of the lessons we have learned in the commercial Internet's toddler years to glean some insights into the implications for copyright law and Internet-based commerce. After analyzing recent economic, business, sociological and technological developments, this article concludes that, while copyright law has a role to play on the Internet, other developments overshadow copyright law as a tool for conforming behavior such that copyright law may be unimportant to the Internet. The public policy implications are clear: the business models, sociology and technology of the Internet are evolving so rapidly that efforts to conform copyright law to this environment would be detrimental.

Part II summarizes a few basic points of U.S. copyright law. Part III describes specific threats that the Internet poses to the enforcement of rights under copyright law. Part IV analyzes the economics of electronic networks to identify why intellectual property might be created even in a putatively anarchistic, piracy-infested environment such as the Internet. Part V discusses sociological attitudes towards intellectual property on the Internet, identifying why it will be difficult to conform behavior on the Internet to the strict letter of existing copyright laws. Part V discusses technologies that copyright holders can use in the battle over works subject to copyright. Finally, part VII concludes with thoughts about how we can live in a world where copyright laws are not the primary influence on our behavior towards intellectual property.

II. UNITED STATES COPYRIGHT LAW BASICS\(^{(5)}\)

Many excellent summaries of U.S. copyright law exist,\(^{(6)}\) and this section will not attempt to duplicate those efforts. However, mapping out the basic contours of the existing U.S. copyright law scheme is helpful in understanding the import of the conclusions of this article.

The Constitution authorizes Congress to establish a legislative scheme "to promote Science and the useful Arts, by securing for limited Times to Authors... the exclusive right to their... writings..."\(^{(7)}\) In response, Congress enacted the Copyright Act of 1909, which it later replace with the Copyright Act of 1976 (the "Copyright Act").\(^{(6)}\)

The Copyright Act governs original works of authorship that are fixed in a tangible medium of expression. While the standard for originality is low, facts and ideas may not be copyrighted.\(^{(8)}\) For copyrightable works, the owner has the following exclusive rights:

1. to reproduce the copyrighted work in copies or phonorecords;
2. to prepare derivative works based upon the copyrighted work;
3. to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
4. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
5. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
6. in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.\(^{(9)}\)
These exclusive rights are subject to numerous restrictions. First, in the case of works created after January 1, 1978, these rights cease 50 years after the death of the author, or, in the case of works made for hire, the earlier of 75 years from the date of first publication or 100 years from the date of creation. (11)

Second, these exclusive rights are subject to the doctrine of fair use, which may permit the infringement of an exclusive right of a copyright owner if its conditions are met. The Copyright Act enumerates four factors that are to be considered to determine whether or not a use is fair:

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
(2) the nature of the copyrighted work;
(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
(4) the effect of the use upon the potential market for or value of the copyrighted work. (12)

In evaluating a claim of fair use, the court is to consider all four factors. However, taking 100 percent of a copyrighted work ordinarily militates against a finding of fair use, (13) and the fourth factor is generally considered the most important. (14)

There are numerous other statutory exceptions and limitations to copyright owners' rights, generally set out in Sections 108 to 120 of the Copyright Act.

Other intellectual property rights in U.S. law often also apply to works for which copyright protection is sought, including trade secret rights, trademark rights, patent rights, rights of publicity, and rights of privacy. While these other forms of intellectual property are not addressed in this paper, collectively they form an important additional basket of rights available to creators of intellectual property.

III. THREATS TO ENFORCING COPYRIGHT RIGHTS ON THE INTERNET

This section describes some of the unique ways that the Internet poses a threat to copyright owners' ability to enforce their copyrights.

A. No Loss of Quality in Reproduction

Unlike copies of intellectual property made using analog copiers (such as photocopy machine video and music tape recorders, facsimile machines and others), digital copies of intellectual property produce perfect copies without any loss of quality. The first generation and the 1000th generation copy of digital material are indistinguishable. Since each copy is a perfect copy, quality-related limits inhibit pirates from making as many copies as they please, and recipient of these copies have no incentive to return to authorized sources to get another copy equal in quality to the original version.

B. No Meaningful Marginal Costs of Reproduction or Distribution

Unlike the business of selling and distributing physical copies of books, magazines, music cassettes or CDs, video cassettes or software, the costs of making one extra copy of intellectual property on-line are insignificant, as are the distribution costs associated with moving that copy to the end user over the Internet. Assuming no per-byte or other volume cost is imposed on the site owner (which is the current state of the market), infringement can occur at virtually no marginal cost.

C. Ability to Act Anonymously

Using anonymous remailers and other existing technologies, pirates are able to act anonymously on-line, leaving no traceable trail of activity. Anonymity poses a significant threat on the Internet, because it theoretically allows pirates to cause harm without bearing any risk of loss, thus undermining the general presumption that those causing harm can be forced to internalize the costs of their actions. As a result, more infringement is likely to occur than if costs were properly internalized.

However, anonymous activity is not a copyright-specific problem; it applies to all crimes and torts that can be committed on-line. Therefore, it may be more appropriate to address the har
caused by anonymity generally, rather than drafting a specific resolution applicable only to losses suffered by copyright owners. Furthermore, there is a built-in limitation to the scope an size of anonymous actions, particularly if any element of the activity is commercial; at a certain point the activity should become large enough to leave at least shreds of evidence, both in physical space and cyberspace, sufficient to allow attribution. (15)

D. Uneducated Users

Many users do not understand the existing copyright legal framework (16) While the lack of us education applies in both physical space and cyberspace, the Internet permits these users to widely disseminate works with relative ease. Often times, this publication can inadvertently cause harm, such as the forwarding of works subject to copyright to third parties. The result may be a number of relatively small infringements that, in the aggregate, can lead to signif- icant losses for copyright holders.

E. Conclusion

The foregoing threats indicate that copyright holders face substantial risks on-line. Nevertheless, we already have ample evidence that intellectual property is still being created for distribution on the Internet. Indeed, a staggering—almost unmanageable—quantity of intellectual property continues to be produced and made available on-line despite these threats. (17) Therefore, despite the assertions of those who believe that the threats posed on-line to copyrighted works would result in disincentives to create and distribute works, it appears other forces are at work on the Internet.

IV. ECONOMICS AND THE INTERNET

This section applies economic theory and surveys existing business models to suggest why, without increased copyright protection, intellectual property is still likely to be produced even if is given away on the Internet.

A. Price-Setting Behavior in a Nearly Efficient Marketplace When Marginal Costs Are Meaningfully Zero

The Internet is not a perfectly efficient market, but it does represent a close approximation. Among the requirements for an efficient market are perfect information and zero transaction costs. First, while the Internet does not offer perfect information, some industries provide enough information on the Internet to give buyers an opportunity to compare prices based on nearly perfect information. (18) On the Internet, it is likely that many additional industries will experience this phenomenon. Second, while transaction costs are not zero, the Internet has significantly reduced transaction costs. In particular, buyers may experience no marginal transaction costs attributable to using the Internet for finding purchasing opportunities or consummating a transaction. (19)

In an efficient marketplace, a firm's profit-maximizing price is the price where marginal revenue from each sale of the product equals the marginal costs of the product. (20) If marginal costs a zero, what is the profit maximizing price?

1. Marginal Costs on the Internet

For many intellectual property creators, the marginal cost of each additional "sale" of the intellectual property is likely to be effectively zero. While many costs are associated with producing intellectual property, including the time of the creator and the Internet infrastructure (such as the hardware, software and Internet connection), these costs become fixed costs on the intellectual property is produced. (21) At that point, if the intellectual property is uploaded to the Internet, the remaining costs are trivial—further reproduction or distribution on the Internet imposes no meaningful marginal costs.

2. Optimal Pricing

Economic theory predicts that if the marginal costs to "selling" intellectual property is zero, th some producers will accept zero marginal revenues. In other words, the profit-maximizing pri for these producers will be zero. Since this is a seemingly anomalous result, how can this be explained? There are at least four different possible explanations:

(I) A zero-revenue pricing strategy may persist only in the short run; but, ultimately, because profits are being made, all producers will exit this business. This is fundamentally the assertio
of those who believe that intellectual property owners must be paid directly for their creative efforts, or else they will not produce.\(^{(22)}\)

(ii) The only sustainable pricing strategy may be a scheme involving price discrimination, where prices are set in accordance with users' willingness to pay. In this situation, intellectual property will be offered at varying prices, including possibly free, depending on the user.\(^{(23)}\)

(iii) Traditional economic theory may break down on the Internet so that intellectual property not be offered for free despite the absence of marginal variable costs. If this were true, the profit-maximizing price may not be where marginal revenue equals marginal cost. This would be a rather profound result, implicating large chunks of existing economic theory.

(iv) Finally, the profit-maximizing price on the Internet may be where marginal revenue equals marginal cost because intellectual property will be cross-subsidized by other products in a manner sufficient to cover the fixed costs associated with intellectual property creation and distribution. If this is true, a market price of zero for intellectual property can still create long-term economic profits attributable to intellectual property creation.

Of the four possible explanations, as explained in the remainder of this part IV, the author believes that the last proposition best explains why the production and distribution of intellectual property will continue even in the absence of marginal revenues directly attributable to users the intellectual property.

The remainder of this part IV will discuss why the last theory is at least supportable when it comes to many categories of intellectual property on the Internet.

B. Cross-subsidization of Intellectual Property Creation

There is nothing new about the proposition that vendors may give away X to sell Y. In the classic formulation of its strategy, Gillette is credited with conceiving the business model of giving away razors to sell its blades.\(^{(24)}\) However, the deployment of this strategy is inherently limited because a razor is a tangible "thing" that will always have marginal costs to produce. The Internet, where the marginal costs of reproduction and distribution of intellectual property are effectively zero, cross-subsidization becomes viable for a significantly greater number of products.

An intellectual property owner can use a myriad of alternative business models to extract value from the free distribution of intellectual property. If successful, these business models will permit the cross-subsidization of intellectual property creation. Internet entrepreneurs will be induced to create intellectual property if they are able to use it to make a profit from alternative revenue sources.\(^{(25)}\)

The remainder of part IV.B provides a survey of Internet-based cross-subsidization models that may support the production of intellectual property designed to be given away freely.

1. Advertising

Advertising is one of the highest-profile business models on the Internet. Under the advertising model, a company gives away intellectual property to attract visitors to its site and then sells advertising space on its site to others. A broad range of companies are launching advertising-based attempts to freely give away intellectual property and substantive services, including email accounts,\(^{(26)}\) interactive news agents,\(^{(27)}\) editorial periodicals\(^{(28)}\) and search engines and indexes.\(^{(29)}\)

However, the slow increase in Internet advertising dollars suggests that, in the short run, advertising revenue may be insufficient to support the level of free distribution of intellectual property that exists today. \(^{(30)}\) Because the supply of advertisement placement opportunities exceeds the demand of advertisers, advertisers are becoming more demanding.\(^{(31)}\) Moreover, Internet users have grown weary of the often annoying banner advertisements. Nevertheless, the results obtainable from on-line advertising can be so compelling that certain advertisers have strong incentives to choose Internet advertising over other media.\(^{(32)}\)

Furthermore, other media industries indicate that multi-billion dollar industries can be built primarily on advertising. For example, the multi-billion dollar broadcast TV industry effectively gives away its intellectual property to viewers, supporting itself almost exclusively on advertising. The television broadcasting model is consistent with the contention that Internet users will not be required to pay for intellectual property, and that the production of intellectual
property can be entirely supported by advertising.

In reality, many intellectual property owners will combine the advertising model with other for of ancillary revenues. Nevertheless, advertising remains a critically important component Internet cross-subsidization business models.

2. Sponsorships

A variant on the advertising model, sponsorship is the "co-branding" of intellectual property wi the sponsor's trademarks. In the old days of television, sponsorship was common; company would purchase all of the advertising for a show and be acknowledged as the sponsor. On-line, sponsorship can take many forms, but the fundamental premise is that the sponsor be more integrated with the content than just sticking its banner ad at the top of the page. For example, Riddler <http://www.riddler.com/home/html> promotes a contest which gives reward to participants who can answer riddles that require the participants to visit sponsors' sites.

Sponsorship is emerging as a strong alternative to banner advertising, at least partly due to advertisers' dissatisfaction with the results from banner advertising. However, sponsored content also raises difficult issues about editorial integrity as the line between advertisement and editorial information becomes blurred.

3. "Try Before You Buy"

In the "try before you buy" model, companies provide consumers with a free copy of a work which is limited in some way (such as duration or functionality) in the hopes that the consume will purchase a full copy. For example, a vendor may give away software in the hopes that recipients will return to purchase a copy. Moreover, in many instances consumers may unilaterally pirate works and then later decide to purchase legitimate copies, even though the vendor never intended to provide "try before you buy" copies. On the Internet, the "try before you buy" model has become extremely popular, in part because no meaningful marginal cost are associated with manufacturing or distributing trial copies. Thus, software, content are routinely given away on a "try before you buy" basis.

4. Sales of Upgrades

Under the sale of upgrades model, consumers are freely given intellectual property with the expectation that some of them will purchase a superior version. In some ways a variant of the "try before you buy" model, this model capitalizes on the fact that version 1.0 of a product can be the best device to sell version 2.0. For example, sales of upgrades are ubiquitous in the modern software business, where companies bundle their "lite" version of software with the modern for free in the hope that consumers will upgrade to the "professional" version. However the model is not limited to software; an author might give away a short story as a way to build demand for a "further adventures" sequel story or the movie.

5. Sale of Complementary Technology

The truest application of Gillette's maxim, the Internet version might be "give away the client software to sell the server software." For example, the Internet's "browser software wars" have focused heavily on the free distribution of client software. With a large installed base of client software, the server software—which is sold and provides added functionality for people using the client software—becomes more attractive. More generally, software companies who also have hardware businesses may give away software to encourage the use of complementary proprietary hardware.

6. Sales of Physical Goods

Companies may use the free distribution of intellectual property to foster the sale of physical goods in many ways. For example, Digital initially intended to popularize its Alta Vista search engine in order to showcase the speed of its Alpha servers. Digital thus intended to give away a search tool as a way to enhance sales of its physical goods. Similarly, in the area of character merchandising, many companies may seek to build character awareness on-line through free distribution of character-related content; the increased character awareness may translate into increased demand for character-branded merchandise. Finally, electronic distribution of intellectual property could be used to create demand for physical copies of intellectual property that have been bolstered with additional content or experience-enhancing elements.
7. Sales of Services

Companies may stimulate demand for services by distributing free intellectual property online. For example, consultants may find it relatively easy to attract potential customers by distributing free content that demonstrates expertise. Alternatively, software companies can give away software as a way to sell systems integration or customized application development.

A notable example of the use of cross-subsidization to sell services is the free distribution of software as an avenue to sell technical support. For example, Microsoft gives away its Internet Explorer browser without a licensing fee, but users must purchase technical support. The sale of technical support unbundled from the underlying software has become increasingly popular.

8. Personal Information Collection and Data Mining

Internet sites can easily collect a fair amount of information about their users, much of it within the user's consent. For example, Internet sites can learn the user's IP address and most recently visited site. Furthermore, by placing a unique identifier into the user's "cookie"(45) or, with less precision, by analyzing the server logs, the Internet site can trace the user's activity through the site and glean insights into what the user looks at and for how long. In addition, many sites may request or require users to fill out registration forms which call for the disclosure of extensive personal information.

Companies can then exploit this information for commercial gain in a number of ways, such as selling email mailing lists to other companies or selling advertising space to companies that want to provide users with customized product offerings or page views based on their perceived preferences.(47) Although the commercial use of this personal information can create some significant privacy issues, (48) such use is generally not subject to legal restrictions in the United States.

9. Communities

The Internet is particularly useful for facilitating community formation. In physical space, community formation may be inhibited by geography, the cost of communication, or the asynchronous methods of communication. On the Internet, however, groups can form quickly and cheaply since these barriers are absent. Moreover, the absence of these barriers may facilitate the formation of communities devoted to extremely narrow topics, which otherwise would not form.

The formation of Internet communities offers one of the most promising Internet business opportunities. If an Internet site can successfully attract like-minded people to interact with each other on the site, it will have a number of ways to extract value from these relationships. (49) In addition to the obvious methods, such as selling the demographics to advertisers and selling the mailing list to merchants interested in reaching the target audience, the Internet site can extract value by enhancing the community members' ability to communicate with each other. The site could accomplish this by providing proprietary tools to facilitate onsite communicatio and tools and methods to facilitate and enrich physical-space meetings between members.

For example, WebGenesis <http://www.theglobe.com> provides chat rooms oriented primarily towards young adults. While the general public can access the chat rooms for free, subscribe receive "bonus" onsite privileges, including an onsite home page to which all their onsite chat postings are hypertext linked automatically, access to private chat rooms available only to other subscribers (who presumably are also dedicated chatters), and the ability to use tools such a Java that enhance the chatting experience. In other words, by providing the chat rooms for free WebGenesis is able to identify those members of the communities who desire a greater relationship to the community and target these people for the sale of advanced onsite communications products.

Companies could also derive revenue opportunities from Internet communities by organizing conferences and other events of interest to the community. A site that forms a community dedicated to river rafting, for example, could sell river rafting trips to its members, an endeavor that would have the added value of creating an opportunity to meet other members of the community in physical space.

10. Reinforcement of Physical-Space Messages

Internet sites can be used to reinforce marketing and sales efforts being made elsewhere. Such reinforcement can occur in the form of customer support and outreach, such as Federal Express' <http://www.fedex.com>, use of its website to provide data tracking services to its
customers, or a software company’s use of the Internet to distribute bug fixes, FAQs, usage tips and other forms of customer assistance.

Alternatively, some companies use Internet sites to increase customer loyalty or provide branding opportunities. For example, the websites prepared by Zima (http://www.zima.com/) and Miller Genuine Draft (http://www.mgdraftroom.com/) contain offerings designed to allow their consumers to feel like part of a community and to encourage brand loyalty. The Internet market has been described as a “relationship” market; free intellectual property can be the way to initiate, build or reinforce the relationship.

C. Importance of Attribution

As the prior section has indicated, companies can try a myriad of methods of creating value by giving away intellectual property. However, for cross-subsidization to work, buyers impressed with product X (freely given away) must be led to product Y (for sale). In most cases, this will mean that product X must give proper attribution to the seller of product Y so that buyers can make the connection. U.S. copyright law affords no “right of attribution” to owners of intellectual property distributed on the Internet. While some trademark, unfair competition, or right of publicity theories may limit the ability of users of intellectual property to falsely represent the origin of the intellectual property, there is no copyright obligation of attribution.

In some cases, attribution may be the only right that matters on the Internet. In fact, an intellectual property owner seeking cross-subsidization may encourage people to “infringe” the intellectual property through wide distribution, so long as attribution is given. Thus, existing copyright law lacks an important right, the absence of which could hinder the deployment of business models on the Internet.

The NII White Paper recognized that attribution could be important and therefore recommend that copyright law be amended to “prohibit the provision, distribution or importation for distribution of copyright management information known to be false and the unauthorized removal or alteration of copyright management information.” The White Paper defines copyright management information as the name of the copyright owner and the terms and conditions for use of the work.

While not adopted into law in the United States, a virtually identical proposal was adopted at the proceedings of the World Intellectual Property Organization (“WIPO”). Time will tell if the treaty will be adopted without changes in the United States.

The White Paper proposal and the WIPO treaty represent an important step toward the recognition of the right of attribution in the United States. However, the proposed law could have profound effects on some current Internet practices. First, website operators commonly incorporate content maintained on remote servers into the pages delivered to user through a direct hypertext link to the remote content. Intellectual property owners whose file are linked this way may object (1) because these direct-linked users do not actually visit their site, and (2) because the file may be displayed so as to suggest that the site providing the link is the source of the file. Does this form of direct linking run afoul of the White Paper’s proposal? Should it? Would it matter if the linked-to site provided a notice denying access to others who attempted to link to the site?

Second, robots and agents can, for example, survey multiple search engines and display the search results to the end user in summary form, without displaying any advertising contained on the search engine’s site (or, for that matter, giving any attribution to the search engine). As a result, the search engine sites must bear the costs of providing the service without getting the anticipated benefits from the consumers of the information. Does this type of robot behavior run afoul of White Paper’s proposal? Should it? Would it matter if the search engine’s site contained a notice that notified others that robots and agents were not welcome?

D. Conclusion

The large number of alternative business models presented above is necessarily incomplete; entrepreneurs have proven highly capable of developing new ways of extracting value from the Internet. However, the mere existence of so many alternatives reinforces the fundamental message: intellectual property creators can cross-subsidize the production of their works in many ways.

The impact of this concept is powerful: if even one person is able to produce and freely distribute a type of intellectual property through cross-subsidization, why would consumers
continue to pay for an equivalent work? While each copyrightable creation is theoretically unique, many types of intellectual property have substitutes which consumers would readily choose if they were available for free.\(^{(62)}\) In other words, if the Internet is a relatively efficient market and intellectual property is somewhat fungible, then the free availability of a type of work should establish the market price for that type of intellectual property at zero.\(^{(63)}\)

The implications of this proposition are truly profound. It suggests that intellectual property owners who expect to be paid directly by end users will face extreme competitive pressures. Single entrepreneur able to cross-subsidize the production of substitute intellectual property should theoretically drive the market price to zero and eliminate all prospects that end users directly pay for the intellectual property. Given the plethora of methods an entrepreneur could use to achieve this result, zero pricing may be inevitable for many classes of intellectual property.

However, some categories of intellectual property almost certainly will not be given away for free.\(^{(64)}\) For those categories that will support user payments, entrepreneurs can deploy various technologies to protect their intellectual property and increase the likelihood of payment. These technologies are discussed in part VI.

V. SOCIOLOGY OF THE INTERNET

While business and technological factors significantly impact the market for intellectual property, some noteworthy features about users' attitudes towards intellectual property also warrant attention. This section describes certain sociological aspects of the Internet culture about how they may influence users' willingness to pay.

A. Attitudes Towards Intellectual Property

Attitudes towards intellectual property can be placed on a spectrum ranging from "intellectual property should not be protected" to "intellectual property should be highly protected." Though not discrete nodes, five distinguishable segments of this spectrum can be identified:\(^{(65)}\)

1. Information Wants to be Free

Adherents to this perspective believe that any intellectual property should be in the public domain and available for all to use. While finding dogmatic adherents to this perspective may be difficult, finding people who believe that anything they find on the Internet is "fair game" for free use is relatively easy.

2. Right of Attribution

Adherents to this perspective believe that intellectual property can be freely "infringed" so long as the source is attributed. Again, though it may difficult to find people who strictly adhere to this perspective, it is very easy to find people—even among creators of intellectual property—who subscribe to this perspective at least some of the time. Interestingly, U.S. copyright law rarely requires attribution (see part IV.C, supra), although netiquette usually encourages it.

3. Limited Use of Works Subject to Copyright

Adherents to this perspective believe that intellectual property creators should have protectable rights in their creations, but they do not believe that these rights are absolute. Often, adherents want to strike a balance between protecting creators' interests and permitting "infringement" of the intellectual property in a manner consistent with their lifestyle or business. This position arguably represents the framework for existing U.S. copyright law, which gives significant protection to copyright holders but provides the fair use defense and statutory exemptions.

4. Moral Rights

"Moral rights" are the rights of the author to be attributed as the author of the work and to object to a particular use of the work.\(^{(66)}\) As between the author and any potential user (including assignees or licensees), this perspective strongly favors the author; often the author cannot assign his or her rights, and in some jurisdictions the author cannot waive the enforcement of his or her moral rights.\(^{(67)}\) Generally, moral rights reflect a belief that the author's creations are an extension of the author, and therefore the author can control how the public views author through his or her creations. U.S. copyright law does not explicitly recognize moral rights except in a very limited set of circumstances.\(^{(68)}\)
5. Strong Intellectual Property Rights

Adherents to this perspective believe that the author should have significant power to control the use of his or her intellectual property. Adherents would extend the author's power beyond moral rights and permit the author to control all uses of his or her work.

From a policy perspective, it is useful to think about how our copyright laws can conform the behavior of people who subscribe to the perspectives outlined above. Importantly, people who subscribe to the "information wants to be free" theory may very well abuse copyright restrictions regardless of the strength of intellectual property laws, in which case strengthening copyright laws to conform their behavior serves little purpose.\(^{68}\)

To the extent that the Internet culture has increased the number of people unsupportive of strong intellectual property rights, new copyright laws designed to increase creators' rights are unlikely to produce the desired results.

B. Internet Culture and Micro-Infringements

Historically, the Internet has been populated by academics and technologists, many of whom would properly be categorized in the "Information Wants to be Free" segment (or perhaps the "Right of Attribution" segment) of the intellectual property attitude spectrum.\(^{72}\) While waves of newcomers to the Internet have diluted this culture, many of these newcomers bring complementary attitudes towards intellectual property.

Take, for example, people under the age of thirty. During most of or all of their life, they have had easy access—often in their home—to a number of devices they could use to infringe copyright audio cassette recorders (and cheap blank tapes); video cassette recorders (and again cheap blank tapes); high quality, low cost photocopy machines; fax machines; and perhaps the most powerful copying device of all, the personal computer (and cheap blank disks and hard drives). As a result, the under-thirty generation has grown up being able to freely expropriate intellectual property easily and at little cost.\(^{21}\) As college students, how many of them bought most (or even some) of the software on their computer, rather than "borrowing" it from their folks or from a friend down the hall? How many of them put together a compilation tape of their favorite songs? How many of them made a cassette tape of someone else's music album? What mechanisms are in place—or could be put into place—to effectively convince these people that these acts are impermissible under the existing system?

The early Net users and the under-thirty crowd appear to have combined to create an interesting psychology on the Internet. The Internet community reacts with widespread disbelief when someone tries to assert that web browsing is an infringement.\(^{22}\) That linking to a third party's materials is an infringement,\(^{23}\) that forwarding an email to a mailing list could be copyright infringement,\(^{24}\) or that setting up a fan site could be an infringement.\(^{25}\) Conceivably, the Internet community could be educated to understand why these actions implicate copyright rights, but changing the state of the Internet to conform to expansive readings of the copyright law would cause major upheaval. Furthermore, the logistics involved in trying to police these "micro-infringements" are daunting, and perhaps not efficient from a social cost versus social benefit standpoint.\(^{26}\) Indeed, such an approach could ultimately prove economically counterproductive for intellectual property owners as well.\(^{27}\)

More generally, the combination of the Internet culture and the general effect of technological evolution may be affecting our collective attitudes toward intellectual property. We have become a culture largely comfortable with serial micro-infringements. Generally, we want to respect other people's intellectual property rights, but we also want to run our lives in a way that ultimately results in numerous minor, almost trivial, but still theoretically actionable infringements.\(^{28}\) The effect of trying to try to apply copyright laws (or worse, to try to strengthen them) to overcome this attitude would likely be regressive.

C. Conditioning to Expect Freebies

Because so many intellectual property owners are giving away valuable intellectual property for free, users are becoming conditioned to expect free intellectual property everywhere they go. This environment, users become very reluctant to pay for intellectual property, since they know that free substitutes are likely to be available elsewhere. Even minor non-cash impediments, such as required registration forms, may be sufficient to drive users away. This conditioning makes it increasingly difficult for intellectual property owners to charge users directly for intellectual property.
VI. TECHNOLOGIES AND METHODS FOR CONTROLLING INTELLECTUAL PROPERTY

This section analyzes existing technological tools and other methods that enable intellectual property owners to protect their property. Technology will by necessity play an essential role in the controlled distribution of intellectual property on the Internet, despite the fact that many categories of intellectual property will be made available to consumers free of charge. Technology will help support revenue-producing markets in those categories of intellectual property that are not going to be freely given away, and it may also help those intellectual property owners who desire attribution.

Some people believe that the availability of the technologies described in this section will lead to the development of a micropayment economy, where even minor uses of intellectual property will result in micropayments to the intellectual property owners. In addition to this result being unlikely for the reasons described in part IV, micropayments raise other difficult issues. In particular, the transaction costs of micropayments can be relatively large—and any customer support is likely to be too costly to provide.\footnote{79}

Clearly no single technology or method can prevent all forms of infringement. However, it is both theoretically and practically possible that a combination of technologies and other methods will provide significant protection against unwanted infringement throughout the productive life of the intellectual property. By setting up impediments to infringement, the intellectual property owner can conform the behavior of those who are unwilling to invest the extra effort to infringe. Furthermore, while the pirates will have plenty of incentive to defeat the technology, "technology does tend to favor the good guys because the good guys are better funded."\footnote{80}

A. Pre-Infringement

This section describes technologies and methods that copyright owners may put into place before distributing their intellectual property to control or inhibit infringement of their works.

1. Limited functionality

Under this approach, intellectual property owners provide a copy of the work which is functionally limited. This approach provides one way to technically implement the "try before you buy" and "sell the upgrades" business models. For example, software creators can distribute software that cannot print or save. Under a slightly different approach, a software vendor can distribute "buggy" software, such as beta versions. While buggy software gives people the opportunity to use and become familiar with it, buggy software also induces those who desire stable software to purchase it. As a last example, database providers or other vendors of large pieces of intellectual property can deliver the content in small chunks, making it difficult to compile the complete work.\footnote{81}

2. Date bomb

Analogous to the limited functionality approach, under this approach the intellectual property owner distributes fully functional intellectual property but locks off access at a pre-specified date.\footnote{82} Under a variant of this approach, the vendor can lock off access after a certain number of usages (i.e., after viewing the file 10 times, the file may no longer be viewed).

3. Copy protection

Under this approach, the vendor limits the number of times a file can be copied. Copy protection was standard in the 1980s, but it fell into disfavor largely because consumers resented the inconvenience and because copy protection was relatively easy to break.\footnote{83} While users are unlikely to be significantly more responsive to copy protection schemes now, copy protection is currently being used in certain situations.\footnote{84} For example, a creator can save a file in Adobe Acrobat's PDF format in a manner that prevents others from making copies, either directly or by such indirect means as printing the screen or copying the text displayed on the screen.\footnote{85} While this form of copy protection is not "hack-proof," it is sufficient to inhibit the vast majority of users from copying files.\footnote{86}

4. Encryption Envelopes

Encryption envelopes are software devices which encrypt intellectual property in such a way that access can be obtained only using the proper key.\footnote{87} These devices are often referred to by IBM's trademark name "cryptolopes." Creators can protect their works by distributing file
in cryptolopes and requiring users to pay for keys that remove the work from the envelope.

5. Contracts

Contracts are an underrated pre-infringement control. When properly formed, contracts enable intellectual property owners to restrict the use of their intellectual property in excess of the rights granted under copyright laws. An unresolved debate continues about the extent to which on-line shrinkwrap contracts (sometimes referred to as "clickthrough agreements") are enforceable. If such agreements are enforceable, intellectual property owners may choose to rely heavily on contract law to control the use of their intellectual property.

B. Metering

This section describes technologies and methods that intellectual property owners can use to ensure payment prior to or at the time of a consumer’s use of the intellectual property.

1. Access codes

Many of the devices described in the pre-infringement section can be coupled with "access code" devices. These devices permit users "unlock" protective mechanisms embedded in intellectual properties themselves, such as date bombs or functional limitations. This method allows the intellectual property owner to meter usage of the intellectual property, either by unlocking the intellectual property for a one-time license fee or by requiring periodic procurement of access codes.

2. Rights-Management Envelopes

As with encryption envelopes, the creator places intellectual property inside special software envelopes. However, under this approach the envelope periodically communicates with a host to implement the business parameters imposed by the intellectual property owner. For example, Wave Interactive Networks provides a system which allows publishers to encrypt a file as a .wmx file, which when activated causes the Wave plug-in to debit the user’s account maintained at Wave’s website.

3. Hardware Devices

Hardware device approaches require the user to acquire and install the requisite hardware device. For example, using a debit card approach, the user purchases a debit card that is pre-loaded with a certain amount of value. After installation, the debit card is debited automatically as the user consumes the intellectual property. In a "superdistribution" approach the hardware device meters the usage of intellectual property and automatically debits an account maintained at a central base.

In this way, even if the recipient has received a copy forwarded from a third party, the hardware device can ensure payment to the intellectual property owner.

4. Downloadable Executables

Downloadable executables, such as Java applets and ActiveX scripts, are pieces of code which download from the server to the client on a "use and discard" basis. In other words, the executable runs during a particular session but will be flushed from RAM at the end of the session. These executables can be metered out because they need to be downloaded each session.

5. Centralized Computing

Under this approach, all of the executables, other than a user interface on the client side, remain at the server. Therefore, the user’s computer must establish contact with the server each time the executable is used, allowing the central computer to meter access. Centralized computing is actually the old "timeshare" model used in the early days of computing, when the client’s processing power was so weak that centralizing processing power at the server level was more efficient.

6. Digital Certificates

In the digital signature context, a certification authority issues to a user an electronic file (a "digital certificate") which identifies the user as the owner of a public key. However, digital certificates can be used to certify more information than mere identity. For example, they can
be used to identify rights associated with a particular person. In these ways, vendors can use
digital certificates to control access to system resources, including intellectual property files, b
making files available to users who can provide a digital certificate with specified rights (such
access, downloading, use, etc., including time limits). A user would obtain the digital certificat
from either the vendor or a third party.

7. Copyright Clearinghouses

Under this approach, intellectual property owners would vest "clearinghouses" with the ability
license usage of their intellectual property. A user would pay a license fee to such a
clearinghouse to obtain rights to the intellectual property. Copyright clearinghouses currently
exist for music-related intellectual property, although these are products of statutory
compulsory licensing. No similar comprehensive mechanisms have developed for other
forms of intellectual property despite some long-standing attempts to do so and the
widely recognized benefits of having such a scheme in place. As a result, some technological
efforts are being made to include copyright management information in all electronic files so
that contact information for procuring copyright permissions will always be available.

8. Sale of Physical Copies

As anachronistic as it may sound, selling physical copies of intellectual property remains a
highly effective method of metering the usage of intellectual property. While the electronic
distribution of intellectual property has many advantages, numerous advantages to purchasing
physical copies of works available on the Internet still remain. First, many people still prefer
reading physical copies over reading electronic copies. Second, obtaining a mass-produced
physical copy rather than printing out the electronic copy may be beneficial from a cost or
quality standpoint. Third, in the case of large electronic files, obtaining a physical copy may be
more time-effective or convenient than downloading the electronic copy. Fourth, the consumer
may use devices that have been optimized for use with physical copies, providing results that
exceed the results available from using the downloaded electronic copy. Therefore, we should
expect that certain categories of intellectual property will continue to be demanded in physical
versions.

C. Post-Infringement

This section describes technologies and methods that creators can use to identify
infringements and thus enhance enforcement of intellectual property rights.

1. Agents

Agents are programs that can implement specified commands automatically. Intellectual
property owners can use agents to search the public spaces of the Internet to find infringing
copies. While agent technology is still being developed and refined, even today creators can
perform a relatively powerful set of searches using full-text search engines such as HotBot
(http://www.hotbot.com/) and Alta Vista (http://www.altavista.digital.com/).

2. Steganography

Steganography, as applied to electronic files, refers to the process of hiding information in file
in such a way that the hidden information is not easily detected by the user. Intellectual property
owners can use steganography in a number of different ways on the Internet. One approach is
to insert into the file a "digital watermark" which can be used to prove that an infringing file was
the creation of the intellectual property owner and not the pirate. The owner of the work
could also store copyright management information using this technology. Another approach is
to encode a unique serial number into each authorized copy of the file, enabling the owner to
trace infringing copies to a particular source.

3. Copyright Litigation

Copyright litigation is a powerful tool for enforcing intellectual property rights, one that should
not be overlooked. While not every infringement will be the subject of litigation, the threat of
litigation helps keep large pirate operations in check. Copyright litigation not only helps the
intellectual property owner obtain relief for specific acts of infringement, it publicly warns othe
of the dangers of infringement. Indeed, a number of intellectual property owners have had
well-publicized successes enforcing their copyrights against on-line infringers.

D. Additional Problems Under Copyright Law Possibly Solvable by Technology
This section discusses some additional complex issues under U.S. copyright law that are not fully addressed by the technologies and methods described in parts VI.A-C, supra, but are still addressable by technology. In particular, linking and caching are both techniques used in the normal functioning of the Internet, yet their permissibility under U.S. copyright law is unclear.

When the technologies available for controlling linking and caching are combined with the technologies and methods described in parts VI.A-C, supra, the mosaic of the overall set of protection technologies and methods available to intellectual property owners becomes clear. This clarity will lead to the question, discussed in part VI.E, infra, of whether situations exist in which intellectual property owners should have the obligation—i.e., if he or she wants to exercise it—to prevent users from infringing before the owner is given the right to claim infringement.

1. Linking

Hypertext linking is one of the blessings of the Internet, but its application has proven problematic. Most copyright experts generally believe that linking should not lead to copyright liability because the mechanical operation of the hypertext link does not implicate one of the exclusive rights of copyright owners; a hypertext-linked URL is merely an instruction which is loaded into the user's browser software, and the browser software does all of the work from there. As a result, the server providing the hypertext link never makes a copy or otherwise processes any of the data from the linked site.

While the plain language of the copyright statute suggests the above conclusion, commentators, to ensure that linking is not copyright infringement, have argued that uploading intellectual property to the Internet grants an "implied license" to link. Alternatively, linking might be considered fair use.

Of course, given the alternative business models discussed earlier, in many cases Internet sites eagerly seek out linking as an entree to generate ancillary values. In fact, a nascent business of providing links has developed. However, if an Internet site does desire to keep others from linking to some or all of its pages, a number of technologies are available to inhibit linking:

- The system operator (the "sysop") can make the page a "dynamic" page by building the page only when the user causes the execution of a program resident on the server. This prevents linking because dynamic pages have no fixed reference point to which to link. This technique, while effective, is also currently somewhat expensive. Alternatively, a low-technology approach is for the sysop to manually change the page's URL periodically, so that any links made to the page will become ineffective.
- If the sysop desires to prevent a specific site from linking to a page, the sysop may code the page in such a way that it refuses browsers who access the site from the forbidden linking site.
- In the case of automatic linking performed by robots and spiders (such as those used by the search engines), the sysop may load information into the header of the page that instructs the robots and spiders not to index the page.
- The page can be password protected; although this practice inhibits the page's free accessibility to people browsing the Internet.
- To address the problem of unattributed graphics being incorporated into pages on a remote system, the graphic may contain a program that automatically causes a notice to appear to users who access it that the graphic is the copyrighted work of the intellectual property owner.

2. Caching

Caching is a loosely used term that generally refers to the process of making an extra copy of a file or set of files for more convenient retrieval. On the Internet, caching of third party files can occur both locally on the user's client computer (either in RAM or on the hard drive) or at the server level (called "proxy caching"). When a user requests a file that has been cached, the browser will deliver the file from the cache rather than retrieving a fresh copy over the Internet.

Although different concepts, similar issues to caching arise with mirroring (establishing an identical copy of an Internet site on a different server), archiving (providing an historical repository for information, such as with newsgroups and mail lists, where the proceedings would otherwise be evanescent), and full-text indexing (the copying of a document for loading into a full text or nearly full-text database which is searchable for key words or concepts).
Caching is an integral part of the Internet's operation, in part because it speeds the user's access to files and in part because it reduces the infrastructure required for operation of the Internet (by reducing the number of files that must be transferred using the infrastructure). Without caching, our already taxed infrastructure would be even more clogged, to the point where it may become unworkable. As a result, a number of serious business plans have been predicated on using caching.\footnote{106}

However, caching could cause harm because the copies in the cache are not necessarily the most current and up-to-date copies.\footnote{109} For example, users relying on the cached copy may unwittingly use out-of-date material; similarly, harms such as defamation or infringement that existed on the original page may propagate for years until flushed from each cache where have been replicated.\footnote{110} Also, since caching is an infringement under a literal reading of U. copyright law, either caching must be the subject of an implied license or fair use defense or is (at least theoretically) actionable.

Internet sites can deploy a number of technologies to restrict or prevent caching:

- Sysops can make the page a "dynamic" page by building the page only when the user causes the execution of a program resident on the server. As in the case of linking, this solution may be expensive.
- Sysops may place information on the page's header which tells the party trying to cache the page when to replace the copy in the cache with a new copy (this is called an "expiry header"). In the case of a sysop who does not want the page cached at all, the sysop merely sets the expiry date as a date before the date on which the information is loaded. Unfortunately, no technology standards presently exist under which caching entities can read and manage this process automatically, so a sysop's instructions may well be ignored or not processed.
- The page can be password protected, although again this inhibits the page's free accessibility to Internet browsers.

Finally, parties trying to establish caches have an incentive to deploy software that automatically updates the cache every time the cached page changes. While this practice solves many of the problems, it leaves control of the process with the entity doing the caching rather than with the website being cached.

E. Is Technology a Substitute for Copyright Law?

Many on the Internet implicitly believe that the failure of an intellectual property owner to use available technology to prevent infringement controls grants to all comers an implied license to infringe. This attitude is seen most often in the arguments raised against copyright infringement for linking and caching. However, based on all of the possible technological controls available to intellectual property owners as described in this part VI, the "use technology or accept infringement" argument might be expanded to apply to all types of infringement, going far beyond just linking and caching.

In some ways, this argument is unprecedented. No other situation come to mind where a copyright owner's failure to use technological protective controls has the effect of diminishing their rights under copyright law.\footnote{111} Why should the Internet create a new paradigm?

On the other hand, the normal functioning of the Internet is predicated on multiple infringement of copyright rights. If we want the Internet to work as it currently operates and as it can operate in the future, we must reduce the chilling effect of the threat of copyright litigation by changing the rules (or interpreting them differently) or placing some burden on intellectual property owners to "opt out" of the system by deploying technology controls.

Given that many intellectual property owners' business models are based on encouraging "infringement" by users, and that many users believe (innocently but mistakenly) that intellectual property found on the Internet is free for the taking, a trend is emerging toward increasing the burden placed on intellectual property owners to adopt technology controls rather than relying on copyright infringement litigation. Interestingly, this trend is incompatible with the efforts of those seeking to increase the scope of the copyright laws.\footnote{112}

VII. CONCLUSION

Even though many of this article's specifics will be out-of-date soon after it is published, its general conclusions should have lasting relevancy to the policies of future U.S. copyright law. This article has marshaled evidence to support the following conclusions:
- The creation and dissemination of intellectual property, both on the Internet and more
generally, seems highly robust despite all of the threats.
- The economics of the Internet dictate that, in many cases, businesses must find a way
generate revenues without charging users for intellectual property.
- A wide variety of sustainable business models permit businesses to accomplish that
del.
- Users are becoming increasingly unwilling to pay directly for intellectual property.
- The elimination of all infringements is an impossible and possibly undesirable goal.
- A cadre of entrepreneurs and existing companies are introducing a wide variety of
technologies that intellectual property owners can use to manage the process of
infringements.
- The perception is increasing that intellectual property owners should be required to use
the available technological tools rather than relying on the threat of litigation over
micro-infringements.

As a practical reality of these conclusions, the real battle between intellectual property owner
and Internet users is being waged using the business models and technological tools available
to intellectual property owners. Combined with the trends in sociological beliefs about the
Internet, the business models and technological tools will evolve over time to make copyright
law increasingly less important as a tool for conforming behavior on the Internet.

Concluding that copyright law's unimportance on the Internet suggests that copyright law
should be abolished generally would be inaccurate. The fact that the existing copyright laws
may have no effect on the way creators and consumers operate on the Internet does not mean
that we no longer need these laws. Existing copyright laws are critically important to the world
of physical space. This holds true even though the Internet may become the preeminent
vehicle for the dissemination of intellectual property.

However, except in the possible case of attribution rights, no new laws designed to increase the
rights of intellectual property owners on the Internet are currently needed. Any such legislatio
would most likely destroy the delicate balance being struck in the marketplace right now.
Furthermore, any anomaly in the existing laws is likely to be resolved by technological and
business innovation, which is occurring at a dizzying rate.

We live in an energizing information age, where we are beginning to realize many of
yesterday's dreams about information exchange on a global scale. We should facilitate this
environment by letting the marketplace reach its own equilibrium. We can do this best by
pursuing legislation which regulates only the most extreme behavior, leaving the rest of the
spectrum of behavior for marketplace solutions.

FOOTNOTES

© 1997 Cooley Godward L.L.P.

+ UCLA B.A. 1988, M.B.A., J.D. 1994. The author is an attorney practicing cyberspace law with
Cooley Godward L.L.P., Palo Alto, California, and is also an adjunct professor of Cyberspace
Law at the Santa Clara University School of Law. The author wishes to extend special thanks
to the members of the CNI-COPYRIGHT mail list, whose contributions to an initial draft of this
paper were invaluable in refining his interest in this topic; Stephen Paternot and Todd
Krizelman of Cooley Godward's client WebGenesis, whose leading edge business models have
led to numerous insights; and Lisa Sanger, a constant source of inspiration. The author also
appreciates the comments to prepublication drafts of this paper given by Brad Biddle, John
Cummerford, Viraj Jha, Michael Lean, Mark Lemley, Shawn Molodow, Ross Mutton, Mark

The views expressed in this article are the author's own and do not necessarily reflect those
Cooley Godward or its clients. Cooley Godward represents some of the companies referred
in this article.

The author can be reached at schlachtere@cooley.com.

[BTLJ Web Editor's note: After reading a footnote, use your browser's "back" button to return
to the main text.]


[Throughout this article, websites are referenced as both primary and secondary sources. Unless otherwise noted, all websites were verified on May 1, 1995.]


Although this article focuses on the Internet, much of the analysis applies with equal force to other networks such as BBSs and on-line services.


5. This article discusses only U.S. copyright law, although other copyright law schemes are similarly worthy of analysis.


7. U.S. Const. art. 1, sec. 8, cl. 8.


11. Id. sec. 302.

12. Id. sec. 107.


students couldn't understand it. Indeed, their teachers couldn't understand it. Copyright lawy

don't understand it.

17. See Steve G. Steinberg, Seek and Ye Shall Find (Maybe), Wired, May 1996, at 108, available at <http://www.hotwired.com/wired/4.05/features/indexweb.html> (noting that "at its current growth rate, the Web will contain more words than the giant Lexis-Nexis database by [summer 1996], and more than today's Library of Congress by the end of 1998").

18. See Netbot <http://www.netbot.com/>. For example, the Internet provides numerous "agents" for buying music CDs. These agents search the available pricing databases on the Internet and deliver a comprehensive set of results, allowing customers to easily compare prices and, presumably, choose the lowest. See, e.g., BargainFinder Agent <http://bf.cs.tor.ac.com/blf/).

19. See part III.B supra. In part, transaction costs are limited due to current market conditions pricing for access that does not vary with usage. There has been much discussion suggestin

g that per-byte or per-unit pricing will be required because of the problems inherent in a system where users can get unlimited use of the scarce resources of the Internet without paying marginal costs. See Jeffrey K. MacKie-Mason & Hal R. Varian, Economic FAQs About the Internet (June 1995) <http://www.spp.umich.edu/
ipps/papers/info-nets/Economic_FAQs/FAQs/FAQs.html>.

20. A producer will continue to produce so long as the marginal revenue from an additional un

of output is greater the marginal cost of such output, since the difference represents a contribution towards fixed costs. In an efficient market, the party with the lowest marginal cost sets the price, since it is able to undercut its competitors' prices and therefore win customers.

21. In the long run, all costs are variable costs. However, in the short run, costs that cannot be varied easily are fixed costs. Therefore, costs such as salaries, hardware and software expenses and contractual commitments for Internet service are all fixed costs in the short run


23. See Hal R. Varian, Differential Pricing and Efficiency (June 1996) <http://alfred.sims.berkeley.edu/Different/different.html> (arguing that it is optimal for intellect

ual property to be offered on a price-discriminated basis). Price discrimination is tricky because it requires careful definition of the product being price-discriminated. If the business model adopted by an Internet company is to provide free intellectual property as an inducement to s

other goods or services, is the "product" the intellectual property or the package of intellectual property plus the ancillary goods or services?


25. It is generally believed that few, if any, Internet businesses are currently making a profit. See, e.g., Kathy Rebello, Making Money on the Net: Bus. Week, Sept. 27, 1996, at 104, available at <http://www.businessweek.com/1996/39/b34941.htm> (indicating that Internet businesses losing money outnumber moneymakers two to one); See Jeff Moad, Web Shakeout, PC Week, July 15, 1996, at E1, available at <http://www8.zdnet.com/pclweek/ExecConnect/0715/15emain.html> (describing a number of high-profile failures of Internet businesses). This limited empirical evidence does not yet prov

that the Internet will provide insufficient profits to induce the creation of intellectual property. The Internet is far from mature, either as a commercial environment or in terms of the predictability its technical or legal framework. Further, in most industries, significant upfront investments must be made before profits accrue--and most Internet businesses are less than years old. Instead, the high stock valuations of many Internet companies indicates that many investors forecast significant future profits.

26. See, e.g., Juno On-line <http://www.juno.com> and Hotmail <http://www.hotmail.com/>. Other companies, such as Cyber FreeWay <http://cyberfreeway.net/> and @bigger.net <http://bigger.net/> are offering lifetime email accounts for a low one-time fee. However, Freemark, one of the early entrants in this arena, has already gone defunct.


30. See Lauren Gibbons Paul, Web Rewards Wait Only for the Patient, PC Week, July 15, 1996, at E4, available at <http://www8.zdnet.com/pcweek/archive/1328/pcwk0007.htm> (suggesting that content sites should not expect to break even before the year 2000); Rosalind Resnick, Follow the Money, Internet World, May 1996, at 34, 34-36 [hereinafter Resnick, Follow the Money], available at <http://www.IW.com/1996/05/money.html> (noting that advertising revenue is heavily concentrated among a small number of sites, leaving few advertising dollars for other sites); See also Hunter Madsen, Reclaim the Deadzone, Wired, Dec. 1996, at 206, 212, available at <http://www.wired.com/wired4.12/emsadsen.html> (describing how the limited real estate for banner advertisements suggests that banner advertisements will be insufficient to support Web publishing). Web advertisement revenues were $71.7 million in the first six months of 1996, although they are expected to increase to $5 billion in 2000. Rebellino, supra note 25, at 107.


32. See Craig R. Evans, The Web's REAL Opportunity—Advertising!, Elec. Retailing, Sept./Oct 1996, at 6 (describing a survey of Web users indicating that 46% of those who used the Web research products and services went on to buy the product at retail).


34. Madsen, supra note 30, at 220.

35. In another example, IBM makes the full text of patents issued to it since 1971 available for free on its website. IBM's motivation is, in part, to reinforce the message that IBM has record more patents than anyone else in the past several years. See IBM Patent Server <http://patent.womplex.ibm.com/>.

36. Resnick, Banner Advertising, supra note 33.

37. See Margie Wylie, Can Copyright Survive the Digital Age? Should It?, Digital Media: A Seybold Report, July 3, 1995 (on file with author) ("Some of the more popular spreadsheet wordprocessing programs were greatly aided by being ripped off to a certain degree. It let people use them enough that they were convinced it was worth the money to buy a legitimate copy, with documentation, support and upgrades." (quoting R.W. Lucky of Bellcore Labs)).

38. This model is exemplified by the long-standing "shareware" industry. See, e.g., McAfee, <http://www.mcafee.com/> , which makes anti-virus shareware software, and Netscape <http://www.netscape.com/> , which gives its browser away as shareware. Id Software, the makers of Doom II, a popular (and violent) computer game, took a slightly different approach—they gave away the first 3 basic "levels" of the Doom II dungeon; the other 47 levels were made available for a charge.

39. Numerous pornography sites on the Internet offer a few free photos for browsing as a teas to purchasing access to the remaining database of photos. See generally <http://www.yahoo.com/Society_and_Culture/Sexuality/>.


41. See Paulina Borsook, Steal This Article, Upside, Mar. 1996 at 80, 88 [hereinafter Borsook, Steal This Article], available at <http://www.upside.com/txsis/archive/search/article.html?UID=9603011002> (describing how music groups have a love/hate relationship with their underground fans, knowing that infringement by the underground is often a way to expand their fan base). Spectrum Press <http://users.aol.com/specpress/free.htm> gives away samples of short stories and novels that it sells in electronic form delivered on
floppy disks. But see id. ("You can upgrade software, not music." (quoting Judith Saffer, in house attorney for BMI)).

42. See Caryn Gillooly, Cabletron's Unbeatable Price Plan, Info. Week, July 24, 1995, at 28 (describing how Cabletron was giving away its Spectrum software, worth $20,000, as an entr to sell its other network management products).


44. This model may explain why companies tolerate unauthorized fan sites. Cf. Constance Sommer, Film Rights Falling Through the Net, San Jose Mercury News, Dec. 10, 1996, at 10 (referring to Disney's laissez-faire attitude toward on-line fan sites).

45. See Paulina Borsook, Music Lessons, Upside, Mar. 1996 at 84, [hereinafter Borsook, Mus Lessons] (describing how music companies can add value to free on-line music sufficient to induce purchases of CDs through better packaging, thicker CD booklets, and accompanying video).

46. A "cookie" is a file on the user's hard drive where websites may store user-specific information. Most browser software programs support the use of the cookie.

47. See, e.g., CyberGold <www.cybergold.com> (a service which will pay users to read advertisements sent to them based on their articulated preferences).


50. See Neil Gross & Peter McCoy, The Technology Paradox, Business Week, Mar. 6, 1995, 76, 80 (describing how giving intellectual property away for free can build mindshare in the coming "attention economy").

51. Id. at 77.

52. 17 U.S.C. sec. 106A applies only to "visual works," which include paintings, drawings, prin or sculptures in a limited edition of less than 200 copies which are signed and consecutively numbered, or a still photographic image which is a single copy signed by the author or is a limited edition of less than 200 copies signed and consecutively numbered. Id. sec. 101. Whil it theoretically possible for a work existing on the Internet to be categorized as such, this possibility is highly remote.

53. None of the six exclusive rights of copyright have been interpreted to require attribution. S Mark A. Lemley, Rights of Attribution and Integrity in On-line Communications, 1995 J. On-lin L. art. 2 <http://warthog.cc.wm.edu/law/publications/ jol/lemley.html>.

54. See John S. Erickson, Open Commerce through Enhanced Attribution (1996) <http://www.netrights.com/EnhancedAttribution.html>; cf. Borsook, Music Lessons, supra not 44, at 84 (describing how a musical group used the name of a Japanese character for one of the group's songs; the litigation over the use of the name was amicably settled when the group pointed out that the character owner could not buy the kind of free advertising it had received

Some of the business models, such as advertising, may require the attribution to occur o the site where the advertising is located. Therefore, not every business using cross-subsidization will necessarily encourage widespread infringement.


56. Id. The reference to terms and conditions of use may be problematic because it suggests that owners can unilaterally impose "contract" terms on all consumers of the file. See Julie E.
Cohen, A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace, 28 Conn. L. Rev. 981 (1996) [hereinafter Cohen, Right to Read Anonymously]. While this unilateral contract approach might be the right result, as found in ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), available at <http://www.kentlaw.edu/7circuit/1996/unr/96-1139.htm>, no consensus currently exists that the federal government should be dictating that licensors should be permitted to unilaterally impose contract terms on licensees. See U.C.C. Proposed Article 2B (Mar. 21, 1997 draft) <http://www.lawlib.uch.edu/ucc2b/> (a controversial attempt to develop model state legislation permitting increased ease in the formation of unilateral contracts by licensors); See also Maureen O'Rourke, Copyright Preemption After the ProCD Case: A Market-Based Approach, 12 Berkeley Tech. L.J. 53, 71 (1997). This issue is particularly important because presumably the licensor-imposed terms will exceed the licensor's rights under copyright law (otherwise, why would they need to impose them?). However, terms and conditions would be less problematic if they were merely grants of licensor's copyright rights (i.e., "you may use this material for any noncommercial use").


58. Prof. Samuelson also notes that the proposal could protect devices incorporated into files that effectively report on users' behavior, raising potentially serious privacy concerns. Samuelson, supra note 3, at 188; See also Cohen, Right to Read Anonymously, supra note 55.

59. The HTML command "img src," followed by a URL, instructs the user's browser software to access the file contained at the referenced URL and to incorporate that file into the page displayed to the user. The user will see the file displayed on the page, but the user will not see the site from which the file originated, nor will the linking site store a copy of the linked-to file its server. Issues related to linking are discussed in part VI.D.1 infra.

60. Cf. CompuServe, Inc. v. Cyber Promotions, Inc., 1997 U.S. Dist. LEXIS (S.D. Ohio Feb. 3, 1997), available at <http://www.bna.com/e-law/cases/compus1.html> (discussing how when a mass email sender was notified by CompuServe that their "junk" email was no longer welcomed the sender's continued sending of mass emails was a trespass to chattels; however, notice "may be insufficiently communicated to potential third-party users when it is merely posted at some location on the network.").


A recent case involving the use of "frames" raises similar issues which arise when one site engages in "free riding" on the efforts of other sites. See Washington Post Co. v. Totalnews, Inc. (complaint filed Feb. 20, 1997) <http://www.lx.com/internet/complain.html>. However, Totalnews does provide attribution to the sites it frames.

62. But see Cohen, Right to Read Anonymously, supra note 55 (assuming that each intellectual property is unique to the point that owners are able to exercise monopoly powers sufficient to impose unfair terms on consumers seeking access to the work).

63. See generally Gross & McCoy, supra note 50 (describing the recurring phenomenon of valuable goods and services being given away for free, even where manufacturing and distribution have marginal costs).

64. Which categories these are is presently unclear, but presumably they will be categories lacking high fungibility between specific intellectual property outputs.


67. See NII White Paper, supra note 2, at 146.
69. See Rose, supra note 15, at 104.
70. See Rebello, supra note 25, at 113-14.
71. Cf. Litman, supra note 16, at 34-35 ("Most of us can no longer spend even an hour without colliding with copyright law. Reading one’s mail or picking up one’s telephone messages these days requires many of us to commit acts that [the NII White Paper] now tells us ought to be viewed as unauthorized reproductions or transmissions.").
72. See NII White Paper, supra note 2, at 64-65.
73. See The Shetland Times Ltd v. Wills, Court of Sessions, Edinburgh, October 24, 1996 <http://www.shetland-news.co.uk/opinion.html> (a United Kingdom court enjoined one newspaper from hypertext linking to stories at a competing newspaper’s website).
74. See Mitch Betts, On-line Pay Per View, ComputerWorld, June 5, 1995, at 58, available at <http://www.computerworld.com/search/AT-html/9506/950605SL22 rights.html> (citing a survey of 255 information systems professionals which indicating that 72% believed they "should be able to download on-line news articles and share them with as many people as they want").
75. For example, when Lucasfilm’s, the owner of Star Wars, contacted a dedicated fan who has established a Star Wars appreciation website regarding alleged infringements, the fan transcribed the conversation and posted the transcription on the website. After Lucasfilm’s was flooded “with angry emails, demanding to know how it could presume to assert such totalitarian control over a product some fans had woven into the very fabric of their lives,” Lucasfilm’s backed down. Sommer, supra note 44, at 10E.
76. See Wylie, supra note 37 ("Copyright doesn’t work today because people pay 100 percent of the time. It works because people pay often enough that intellectual property owners make a profit."); cf. Borsook, supra note 45, at 84 (noting that the music industry long ago accepted that it would lose 15-20% of its potential revenues to home copying).
77. A good example can be found in the movie studios’ action against video cassette recorder manufacturers, Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), where the studios’ victory would have inhibited the development of an industry (video cassette rental) that generated $13 billion in revenues for the studios in 1993. See Current Revenue of Target Markets, Upside, Dec. 1994 at 18 (graph referencing a Yankee Group study); cf. Litman, supra note 16, at 46 ("Whenever we have discovered or enacted a copyright exception, an industry has grown up within its shelter.").
80. Ross, supra note 15, at 137.
81. Id. Compare the approach used by Lexis in delivering cases on a screen-by-screen basis; compiling the full case by capturing each screen would be arduous.
84. Cf. id. (describing how Macrovision "spoilers" are inserted into movies; the spoilers confus VCRs and produce distorted versions of the movies if copied).
85. Maximized Software’s SiteShield software <http://www.maximized.com/products/siteshield/> encodes files in such a way that they may be browsed but not otherwise copied.
86. "Now, people say to themselves "Hey, let me take this for free," but with [Maximized Software’s SiteShield], they’d have to decide to be trespassers... People would have to put effort into stealing the images, and they’d know they were violating the copyright." Ross, supra note 15, at 139 (quoting Kenneth Spreitzer, president of Maximized Software).

88. In some circumstances the enforcement of the contract will be limited because the contract provisions are preempted by copyright law. See Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 268-70 (5th Cir. 1988). See generally I. Trotter Hardy, Contracts, Copyright and Preemption in a Digital World, 1 Rich. J.L. & Tech. 2 (1995) <http://www.uncc.edu/~jolt/v11/hardy.html>; See also, O'Rourke, supra, note 56.


90. See InterTrust <http://www.intertrust.com/products/flow.html> (describing the DigiBox envelope, which communicates with a clearancehouse based on business rules encapsulated in the envelope); Gary N. Griswold, A Method for Protecting Copyright on Networks, 1994 <http://www.cni.org/docs/ima.io-workshop/www/Griswold.html> (describing a software envelope which requires periodic confirmation with a home base prior to permitting further access); Stefl, supra note 2 (describing protocols to permit the permanent transfer or temporary lendi of files while holding the number of files to the number actually paid for).


93. 17 U.S.C. secs. 115 (making and distributing phonorecords), 116 (public performances by means of coin-operated phonorecorder players ("juke boxes").

94. The Copyright Clearance Center <http://www.copyright.com> can grant licenses to reproduce 1.75 million documents—an impressive number, but clearly far short of the overall of works subject to copyright available in the world.

95. Project Xanadu, an attempt to ensure compensation to creators whenever even small chunks of intellectual property are used, was initiated in 1960. Xanadu FAQ, sec. 1b, June 29 1996 <http://www.xanadu.com.au/xanadufaq.html>.


97. See Stanford Copy Analysis Mechanism (SCAM) <http://www-db.stanford.edu/~shiva/SCAM/scamInfo.html>; see also Hyperstamps CyberGumshoe Services <http://www.hyperstamps.com/misc/gumshoe.html> (offering a robotic search of the Internet for documents containing serialized document numbers that developers may insert (for a cost) into an HTML page); Intellectual Protocols' Copyright <http://www.ip2.com/copyight.cgi> (offering a service similar to Hyperstamps); cf. MarkWatch <http://www.markwatch.com/> (providing an automated monitoring service for trademark use on the Internet); Alex Alpen, The Death of Copyright in a Digital World: The Reports are Sligh Exaggerated, Ent. Law Rep., July 1995 (describing "bounty hunter" programs used by intellectual property owners to cut down on infringements; third-party attorneys bringing suits against infringers were allowed to keep any damages won in the actions).


100. See Borsook, Steal This Article, supra note 41.


There have also been well-publicized criminal indictments, including actions against Davey Jones Locker. Rose, supra note 15, at 104, and Rusty & Edie's BBS, Michael A. Hobbs, ACL Cries Foul in Computer Raid, The Plain Dealer, Feb. 19, 1993 at 3B.


103. If browsing the Web is an infringement because a copy of the page is made and sent to the user's computer, as proposed by the Nil White Paper, supra note 2 at 64-65, then the linking site has arguably committed contributory infringement by substantially contributing to the user infringement (which occurred during the process of browsing). See Niva Elkin-Koren, Copyrig Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators, 13 Cardozo Arts & Ent. L.J. 345, 353-56 (1995), available at <http://yu1.yu.edu/80/el/ijournals/eel/articles/13-2/elkin.html>. The assertion that browsing is an actionable infringement has met with some criticism. See id. at 354; Samuelson, supra note at 137.

104. Although the term "implied license" is frequently bandied about on the Internet, the concept is rather amorphous under copyright law. At its heart, an implied license is an estoppel doctrine arising because the infringing party detrimentally and unjustifiably relied on the intellectual property owner's actions.


106. See Maximized Software's SiteShield <http://www.maximized.com/products/siteshield/> (providing a product that prevents linking from all URLs other than those on the specific website); Kristo Coale, Intellecast Smartens Up to Banner Bypass, Wired News (Mar. 28, 1999 <http://www.wired.com/news/technology/story/2844.html> (describing how Intellecast, a wealth of site, prevented links to its weather maps which bypassed the associated banner advertisements).

107. This is one of the features of the Copysight service from Intellectual Protocols <http://www.ip2.com/copysight.cgi>.

108. For example, @home <http://www.home.net/> is deploying a network that permits users to use high-speed cable modems for Internet access. So that users will experience cable modem speeds as often as possible, @home will cache (or archive or mirror, depending on the terminology) the entire Internet on regional servers to which users will connect via their cable modems.

The recent start-up Marimba <http://www.marimba.com/> uses caching as a way to make the use of Java programs more robust.

Also, the number of offline browsers is growing. Offline browsers are software that automatically download some or all of an Internet site to the user's computer, allowing the user to browse without having to wait for the delivery of each page. See, e.g., WebEx <http://www.q叙webex.com>, WebWhacker <http://www.fiq.com/whacker/index.html>, InContext FlashSite <http://www.incontext.com/products/flashsite/index.html> and DocuMag HotCargo Express <http://www.documagix.com/products/hotcargo_exprase/welcome.html>.


110. Toys R Us v. Akkaoui, 1996 U.S. Dist. LEXIS 17090 (N.D. Cal. Oct. 29, 1996) (describing injunction granted in favor of a trademark owner against an infringing website requiring the website to notify all publishers of directories or lists to remove reference to the website and to flush all references to the website from their caches).

111. A different analysis might apply in regard to trade secret and trademark law. In the case of trade secrets, the owner must use efforts, whether technological or otherwise, to keep the information secret in order to preserve the information's status as a trade secret. In the case of trademarks, the owner must use quality control, whether technological or otherwise, to maintain the trademark.

112. See, e.g., NIL White Paper, supra, note 2, at 7-17.

113. At least two important exceptions to this general statement exist. First, the conclusion that loading a copy into RAM is an infringement creates a great deal of uncertainty for browsing. A minimum, clarifying that browsing is not an actionable infringement would be helpful. Second, although generally a topic outside the scope of this paper, the conclusion reached in some cases that sysops are directly liable for copyright infringements occurring because users upload works subject to copyright onto their system has caused a great deal of consternation. If as a policy matter a consensus exists that sysops should not be liable in this circumstance, statutory clarification would be useful.

Reprinted with permission from The Berkeley Technology Law Journal.
907 F. Supp. 1361

RELIGIOUS TECHNOLOGY CENTER, a California non-profit corporation; and Bridge Publications, Inc., a California non-profit corporation, Plaintiffs,

v.

NETCOM ON-LINE COMMUNICATION SERVICES, INC., a Delaware corporation; Dennis Erlich, an individual; and Tom Klemesrud, an individual, dba Clearwood Data Services, Defendants.

United States District Court,
N.D. California.
Nov. 21, 1995.

ORDER DENYING DEFENDANT NETCOM'S MOTION FOR SUMMARY JUDGMENT; DENYING DEFENDANT KLEMESRUD'S MOTION FOR JUDGMENT ON THE PLEADINGS; AND DENYING PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION AGAINST NETCOM AND KLEMESRUD

WHYTE, District Judge.

This case concerns an issue of first impression regarding intellectual property rights in cyberspace. [FN1] Specifically, this order addresses whether the operator of a computer bulletin board service ("BBS"), and the large Internet [FN2] access provider that allows that BBS to reach the Internet, should be liable for copyright infringement committed by a subscriber of the BBS.


FN2. "The Internet today is a worldwide entity whose nature cannot be easily or simply defined. From a technical definition, the Internet is the 'set of all interconnected IP networks'--the collection of several thousand local, regional, and global computer networks interconnected in real time via the TCP/IP Internetworking Protocol suite...." Daniel P. Dern, THE INTERNET GUIDE FOR NEW USERS 16 (1994). One article described the Internet as a collection of thousands of local, regional, and global Internet Protocol networks. What it means in practical terms is that millions of computers in schools, universities, corporations, and other organizations are tied together via telephone lines. The Internet enables users to share files, search for information, send electronic mail, and log onto remote computers. But it isn't a program or even a particular computer resource. It remains only a means to link computer users together. Unlike on-line computer services such as CompuServe and America On Line, no one runs the Internet.... No one pays for the Internet because the network itself doesn't exist as a separate entity. Instead various universities and organizations pay for the dedicated lines linking their computers. Individual users may pay an Internet provider for access to the Internet via its server. David Bruning, Along the InfoBahn, ASTRONOMY, Vol. 23, No. 6, p. 76 (June 1995).

Plaintiffs Religious Technology Center ("RTC") and Bridge Publications, Inc. ("BPI") hold copyrights in the unpublished and published works of L. Ron Hubbard, the late founder of the Church of Scientology ("the Church"). Defendant Dennis Erlich ("Erlich") [FN3] is a former minister of Scientology turned vocal critic of the Church, whose pulpit is now the Usenet newsgroup [FN4] alt.religion.scientology ("a.r.s.") , an on-line forum for discussion and criticism of Scientology. Plaintiffs maintain that Erlich infringed their copyrights when he posted portions of their works on a.r.s. Erlich gained his access to the Internet through defendant Thomas Klemesrud's...
FSN3. Issues of Erlich's liability were addressed in this court's order of September 22, 1995. That order concludes in part that a preliminary injunction against Erlich is warranted because plaintiffs have shown a likelihood of success on their copyright infringement claims against him. Plaintiffs likely own valid copyrights in Hubbard's published and unpublished works and Erlich's near-verbatim copying of substantial portions of plaintiffs' works was not likely a fair use. To the extent that Netcom and Klemesrud argue that plaintiffs' copyrights are invalid and that Netcom and Klemesrud are not liable because Erlich had a valid fair use defense, the court previously rejected these arguments and will not reconsider them here.

FSN4. The Usenet has been described as a worldwide community of electronic BBSs that is closely associated with the Internet and with the Internet community. The messages in Usenet are organized into thousands of topical groups, or "Newsgroups".... As a Usenet user, you read and contribute ("post") to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings from other sites. Usenet traffic typically consists of as much as 30 to 50 Mbytes of messages per day.

Usenet is read and contributed to on a daily basis by a total population of millions of people.... There is no specific network that is the Usenet. Usenet traffic flows over a wide range of networks, including the Internet and dial-up phone links. Bern, supra, at 196-97.

After failing to convince Erlich to stop his postings, plaintiffs contacted defendants Klemesrud and Netcom. Klemesrud responded to plaintiffs' demands that Erlich be kept off his system by asking plaintiffs to prove that they owned the copyrights to the works posted by Erlich. However, plaintiffs refused Klemesrud's request as unreasonable. Netcom similarly refused plaintiffs' request that Erlich be allowed to gain access to the Internet through its system. Netcom contended that it would be impossible to prescreen Erlich's postings and that to kick Erlich off the Internet meant kicking off the hundreds of users of Klemesrud's BBS. Consequently, plaintiffs named Klemesrud and Netcom in their suit against Erlich, although only on the copyright infringement claims. [FSN5]

FSN5. The First Amended Complaint ("FAC") contains three claims: (1) copyright infringement of BPI's published literary works against all defendants; (2) copyright infringement of RTC's unpublished confidential works against all defendants; and (3) misappropriation of RTC's trade secrets against defendant Erlich only.

On June 23, 1995, this court heard the parties' arguments on eight motions, three of which relate to Netcom and Klemesrud and are discussed in this order: (1) Netcom's motion for summary judgment; (2) Klemesrud's motion for judgment on the pleadings; [FSN6] and (3) plaintiffs' motion for a preliminary injunction against Netcom and Klemesrud. For the reasons set forth below, the court grants in part and denies in part Netcom's motion for summary judgment and Klemesrud's motion for judgment on the pleadings and denies plaintiffs' motion for a preliminary injunction.

FSN6. Klemesrud alternatively filed a motion for summary judgment, which will not be considered at this time because Klemesrud was unavailable to be deposed in time for plaintiffs' opposition. In a previous order, the court struck those portions of the motion that referred to matters outside of the pleadings.
I. NETCOM'S MOTION FOR SUMMARY JUDGMENT OF NONINFRINGEMENT

A. Summary Judgment Standards

Because the court is looking beyond the pleadings in examining this motion, it will be treated as a motion for summary judgment rather than a motion to dismiss. Grove v. Mead School District, 753 F.2d 1528, 1532 (9th Cir. 1985). Summary judgment is proper when "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed.R.Civ.P. 56(c). There is a "genuine" issue of material fact only when there is sufficient evidence such that a reasonable juror could find for the party opposing the motion. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 251-52, 106 S.Ct. 2505, 2511-12, 91 L.Ed.2d 202 (1986). Entry of summary judgment is mandated against a party if, after adequate time for discovery and upon motion, the party fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial. Celotex Corp. v. Catrett, 477 U.S. 317, 322, 106 S.Ct. 2548, 2552, 91 L.Ed.2d 265 (1986). The court, however, must draw all justifiable inferences in favor of the nonmoving parties, including questions of credibility and of the weight to be accorded particular evidence. Masson v. New Yorker Magazine, Inc., 501 U.S. 496, 520, 111 S.Ct. 2419, 2434-35, 115 L.Ed.2d 447 (1991).

B. Copyright Infringement

To establish a claim of copyright infringement, a plaintiff must demonstrate (1) ownership of a valid copyright and (2) "copying" [FN7] of protectable expression by the defendant. Baxter v. MCA, Inc., 812 F.2d 421, 423 (9th Cir.), cert. denied, 484 U.S. 954, 108 S.Ct. 346, 98 L.Ed.2d 372 (1987). Infringement occurs when a defendant violates one of the exclusive rights of the copyright holder. 17 U.S.C. § 501(a). These rights include the right to reproduce the copyrighted work, the right to prepare derivative works, the right to distribute copies to the public, and the right to publicly display the work. 17 U.S.C. §§ 106(1)-(3) & (5). The court has already determined that plaintiffs have established that they own the copyrights to all of the Exhibit A and B works, except item 4 of Exhibit A. [FN8] The court also found plaintiffs likely to succeed on their claim that defendant Erlich copied the Exhibit A and B works and was not entitled to a fair use defense. Plaintiffs argue that, although Netcom was not itself the source of any of the infringing materials on its system, it nonetheless should be liable for infringement, either directly, contributorily, or vicariously. [FN9] Netcom disputes these theories of infringement and further argues that it is entitled to its own fair use defense.

FN7. In this context, "copying" is "shorthand for the infringing of any of the copyright owner's five exclusive rights." S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1085 n. 3 (9th Cir. 1989).

FN8. The court has under submission plaintiffs' request to expand the preliminary injunction against Erlich.

FN9. Plaintiffs have argued at times during this litigation that Netcom should only be required to respond after being given notice, which is only relevant to contributory infringement. Nevertheless, the court will address all three theories of infringement liability.

1. Direct Infringement

Infringement consists of the unauthorized exercise of one of the exclusive rights of the copyright holder delineated in section 106. 17 U.S.C. § 501. Direct infringement does not require intent or any particular state of mind, [FN10] although willfulness is relevant to the award of statutory damages. 17 U.S.C. § 504(c).

FN10. The strict liability for copyright infringement is in contrast to another area of liability affecting online service providers:
Defamation. Recent decisions have held that where a BBS exercised little control over the content of the material on its service, it was more like a "distributor" than a "republisher" and was thus only liable for defamation on its system where it knew or should have known of the defamatory statements. Cubby, Inc. v. CompuServe, Inc., 76 F.Supp. 2d 136 (S.D.N.Y. 1999). By contrast, a New York State court judge found that Prodigy was a publisher because it held itself out to be controlling the content of its services and because it used software to automatically prescreen messages that were offensive or in bad taste. Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710, THE RECORDER, June 1, 1995, at 7 (excerpting May 24, 1995 Order Granting Partial Summary Judgment to Plaintiffs).

Many of the facts pertaining to this motion are undisputed. The court will address the relevant facts to determine whether a theory of direct infringement can be supported based on Netcom's alleged reproduction of plaintiffs' works. The court will look at one controlling Ninth Circuit decision addressing copying in the context of computers and two district court opinions addressing the liability of BBS operators for the infringing activities of subscribers. The court will additionally examine whether Netcom is liable for infringing plaintiffs' exclusive rights to publicly distribute and display their works.

a. Undisputed Facts

The parties do not dispute the basic processes that occur when Erlich posts his allegedly infringing messages to a.r.s. Erlich connects to Klemesrud's BBS using a telephone and a modem. Erlich then transmits his messages to Klemesrud's computer, where they are automatically briefly stored. According to a prearranged pattern established by Netcom's software, Erlich's initial act of posting a message to the Usenet results in the automatic copying of Erlich's message from Klemesrud's computer onto Netcom's computer and onto other computers on the Usenet. In order to ease transmission and for the convenience of Usenet users, Usenet servers maintain postings from newsgroups for a short period of time—ten to eleven days for Netcom's system and three days for Klemesrud's system. Once on Netcom's computers, messages are available to Netcom's customers and Usenet servers, who may then download the messages to their own computers. Netcom's local server makes available its postings to a group of Usenet servers, which do the same for other servers until all Usenet sites worldwide have obtained access to the postings, which takes a matter of hours. Francis Decl. ¶ 5. Unlike some other large on-line service providers, such as CompuServe, America Online, and Prodigy, Netcom does not create or control the content of the information available to its subscribers. It also does not monitor messages as they are posted. It has, however, suspended the accounts of subscribers who violated its terms and conditions, such as where they had commercial software in their posted files. Netcom admits that, although not currently configured to do this, it may be possible to reprogram its system to screen postings containing particular words or coming from particular individuals. Netcom, however, took no action after it was told by plaintiffs that Erlich had posted messages through Netcom's system that violated plaintiffs' copyrights, instead claiming that it could not shut out Erlich without shutting out all of the users of Klemesrud's BBS.

b. Creation of Fixed Copies

The Ninth Circuit addressed the question of what constitutes infringement in the context of storage of digital information in a computer's random access memory ("RAM"). MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993). In MAI, the Ninth Circuit upheld a finding of copyright infringement where a repair person, who was not authorized to use the computer owner's licensed operating system software, turned on the computer, thus loading the operating system into RAM for long enough to check an "error log." Id. at 518-19. Copyright protection subsists in original works of authorship "fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 102 (emphasis added). A work is "fixed" when its
"embodiment in a copy … is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." Id. at 101. MAI established that the loading of data from a storage device into RAM constitutes copying because that data stays in RAM long enough for it to be perceived. MAI Systems, 991 F.2d at 518.

In the present case, there is no question after MAI that "copies" were created, as Erlich's act of sending a message to a.r.s. caused reproductions of portions of plaintiffs' works on both Klemesrud's and Netcom's storage devices. Even though the messages remained on their systems for at most eleven days, they were sufficiently "fixed" to constitute recognizable copies under the Copyright Act. See Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights 66 (1995) ("ITTF Report").

c. Is Netcom Directly Liable for Making the Copies?

Accepting that copies were made, Netcom argues that Erlich, and not Netcom, is directly liable for the copying. MAI did not address the question raised in this case — whether or not of MAI's computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party. Netcom correctly distinguishes MAI on the ground that Netcom did not take any affirmative action that directly resulted in copying plaintiffs' works other than by installing and maintaining a system whereby software automatically forwards messages received from subscribers onto the Usenet, and temporarily stores copies on its system. Netcom's actions, to the extent that they created a copy of plaintiffs' works, were necessary to having a working system for transmitting Usenet postings to and from the Internet. Unlike the defendants in MAI, neither Netcom nor Klemesrud initiated the copying. The defendants in MAI turned on their customers' computers thereby creating temporary copies of the operating system, whereas Netcom's and Klemesrud's systems can operate without any human intervention. Thus, unlike MAI, the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean Netcom has caused the copying. [FN11] The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. [FN12] Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement. See, e.g., RCA Records v. All-Past Systems, Inc., 594 F.Supp. 335 (S.D.N.Y. 1984); 3 Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT § 12.04[A][2][b], at 12-78 to -79 (1995) ("NIMMER ON COPYRIGHT"); Elkin-Koren, supra, at 363 (arguing that "contributory infringement is more appropriate for dealing with BBS liability, first, because it focuses attention on the BBS-users relationship and the way imposing liability on BBS operators may shape this relationship, and second because it better addresses the complexity of the relationship between BBS operators and subscribers"). Plaintiffs' theory would create many separate acts of infringement and, carried to its natural extreme, would lead to unreasonable liability. It is not difficult to conclude that Erlich infringes by copying a protected work onto his computer and by posting a message to a newsgroup. However, plaintiffs' theory further implicates a Usenet server that carries Erlich's message to other servers regardless of whether that server acts without any human intervention beyond the initial setting up of the system. It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer. These parties, who are liable under plaintiffs' theory, do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed. There is no need to construe the Act to make all of these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.

FN11. One commentator addressed the difficulty in translating
copyright concepts, including the public/private dichotomy, to the digitized environment. See Niva Elkin-Koren, Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators, 13 CARDOZO ARTS & ENT. L.J. 346, 356 (1993). This commentator noted that one way to characterize a BBS operation is that it "provides subscribers with access and services. As such, BBS operators do not create copies, and do not transfer them in any way. Users post the copies on the BBS, which other users can then read or download." Id. at 356.

FN12. 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 highway, or at least the operator of a toll booth, liable for the criminal activities that occur on its roads. Since other similar carriers of information are not liable for infringement, there is some basis for exempting Internet access providers from liability for infringement by their users. The IITF Report concluded that "[i]f an entity provided only the wires and conduits--such as the telephone company, it would have a good argument for an exemption if it was truly in the same position as a common carrier and could not control who or what was on its system." IITF Report at 122. Here, perhaps, the analogy is not completely appropriate as Netcom does more than just "provide the wire and conduits." Further, Internet providers are not natural monopolies that are bound to carry all the traffic that one wishes to pass through them, as with the usual common carrier. See id. at 122 n. 392 (citing Federal Communications Commission v. Midwest Video Corp., 440 U.S. 528, 539-40 (1979)) ("The Act is not a monopoly or exclusivity act.") Section 111 of the Copyright Act codifies the exemption for passive carriers who are otherwise liable for a secondary transmission. 3 Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT § 12.04[B][3], at 12-99 (1995).

However, the carrier must not have any direct or indirect control over the content or selection of the primary transmission. Id.; 17 U.S.C. § 111(a)(3). Cf. infra part I.B.3.a. In any event, common carriers are granted statutory exemptions for liability that might otherwise exist. Here, Netcom does not fall under this statutory exemption, and thus faces the usual strict liability scheme that exists for copyright. Whether a new exemption should be carved out for online service providers is to be resolved by Congress, not the courts. Compare Comment, "Online Service Providers and Copyright Law: The Need for Change," 1 SYRACUSE J.LEGIS. & POL'Y 197, 202 (1995) (citing recommendations of online service providers for amending the Copyright Act to create liability only where a "provider has 'actual knowledge that a work that is being or has been transmitted onto, or stored on, its system is infringing,' and has the 'ability and authority' to stop the transmission, and has, after a reasonable amount of time, allowed the infringing activity to continue'") with IITF Report at 122 (recommending that Congress not exempt service providers from strict liability for direct infringements).

Plaintiffs point out that the infringing copies resided for eleven days on Netcom's computer and were sent out from it onto the "Information Superhighway." However, under plaintiffs' theory, any storage of a copy that occurs in the process of sending a message to the Usenet is an infringement. While it is possible that less "damage" would have been done if Netcom had heeded plaintiffs' warnings and acted to prevent Erlich's message from being forwarded, [FN13] this is not relevant to its direct liability for copying. The same argument is true of Klemesrud and any Usenet server. Whether a defendant makes a direct copy that constitutes infringement cannot depend on whether it received a warning to delete the message. See D.C. Comics, Inc. v. Mini Gifts, 912 F.2d 29, 35 (2d Cir. 1990). This distinction may be relevant to contributory infringement, however, where knowledge is an element. See infra part I.B.2.a.
FN13. The court notes, however, that stopping the distribution of information once it is on the Internet is not easy. The decentralized network was designed so that if one link in the chain is closed off, the information will be dynamically rerouted through another link. This was meant to allow the system to be used for communication after a catastrophic event that shuts down part of it. Francis Decl. P 4.

The court will now consider two district court opinions that have addressed the liability of BBS operators for infringing files uploaded by subscribers.

d. Playboy Case

Playboy Enterprises, Inc. v. Frena involved a suit against the operator of a small BBS whose system contained files of erotic pictures. 839 F.Supp. 1552, 1554 (M.D.Fla. 1993). A subscriber of the defendant's BBS had uploaded files containing digitized pictures copied from the plaintiff's copyrighted magazine, which files remained on the BBS for other subscribers to download. Id. The court did not conclude, as plaintiffs suggest in this case, that the BBS is itself liable for the unauthorized reproduction of plaintiffs' work; instead, the court concluded that the BBS operator was liable for violating the plaintiff's right to publicly distribute and display copies of its work. Id. at 1556-57.

In support of their argument that Netcom is directly liable for copying plaintiffs' works, plaintiffs cite to the court's conclusion that "[t]here is no dispute that [the BBS operator] supplied a product containing unauthorized copies of a copyrighted work. It does not matter that [the BBS operator] claims he did not make the copies [him]self." Id. at 1556. It is clear from the context of this discussion [FN14] that the Playboy court was looking only at the exclusive right to distribute copies to the public, where liability exists regardless of whether the defendant makes copies. Here, however, plaintiffs do not argue that Netcom is liable for its public distribution of copies. Instead, they claim that Netcom is liable because its computers in fact made copies. Therefore, the above-quoted language has no bearing on the issue of direct liability for unauthorized reproductions. Notwithstanding Playboy's holding that a BBS operator may be directly liable for distributing or displaying to the public copies of protected works, [FN15] this court holds that the storage on a defendant's system of infringing copies and retransmission to other servers is not a direct infringement by the BBS operator of the exclusive right to reproduce the work where such copies are uploaded by an infringing user. Playboy does not hold otherwise. [FN16]

FN14. The paragraph in Playboy containing the quotation begins with a description of the right of public distribution. Id. Further, the above quoted language is followed by a citation to a discussion of the right of public distribution in Jay Dratler, Jr., INTELLECTUAL PROPERTY LAW: COMMERCIAL, CREATIVE AND INDUSTRIAL PROPERTY s 6.01[3], at 6-15 (1991). This treatise states that "the distribution right may be decisive, if, for example, a distributor supplies products containing unauthorized copies of a copyrighted work but has not made the copies itself." Id. (citing to Williams Electronics, Inc. v. Arctic International, Inc., 685 F.2d 870, 876 (3d Cir. 1982)). In any event, the Williams holding regarding public distribution was dicta, as the court found that the defendant had also made copies. Id.

FN15. Given the ambiguity in plaintiffs' reference to a violation of the right to "publish" and to Playboy, it is possible that plaintiffs are also claiming that Netcom infringed their exclusive right to publicly distribute their works. The court will address this argument infra.

FN16. The court further notes that Playboy has been much criticized. See, e.g., L. Rose, NETLAW 91-92 (1995). The finding of direct infringement was perhaps influenced by the fact that there was some evidence that defendants in fact knew of the infringing nature of the works, which were digitized photographs labeled "Playboy" and "Playmate."
e. Sega Case

A court in this district addressed the issue of whether a BBS operator is liable for copyright infringement where it solicited subscribers to upload files containing copyrighted materials to the BBS that were available for others to download. Sega Enterprises Ltd. v. MAPHIA, 857 F.Supp. 679, 683 (N.D. Cal. 1994). The defendant's "MAHIA" BBS contained copies of plaintiff Sega's video game programs that were uploaded by users. Id. at 683. The defendant solicited the uploading of such programs and received consideration for the right to download files. Id. Access was given for a fee or to those purchasing the defendant's hardware device that allowed Sega video game cartridges to be copied. Id. at 683-84. The court granted a preliminary injunction against the defendant, finding that plaintiffs had shown a prima facie case of direct and contributory infringement. Id. at 687. The court found that copies were made by unknown users of the BBS when files were uploaded and downloaded. Id. Further, the court found that the defendant's knowledge of the infringing activities, encouragement, direction and provision of the facilities through his operation of the BBS constituted contributory infringement, even though the defendant did not know exactly when files were uploaded or downloaded. Id. at 686-87.

This court is not convinced that Sega provides support for a finding of direct infringement where copies are made on a defendant's BBS by users who upload files. Although there is some language in Sega regarding direct infringement, it is entirely conclusory: Sega has established a prima facie case of direct copyright infringement under 17 U.S.C. s 501. Sega has established that unauthorized copies of its games are made when such games are uploaded to the MAPHIA bulletin board, here with the knowledge of Defendant Scherman. These games are thereby placed on the storage media of the electronic bulletin board by unknown users. Id. at 686 (emphasis added). The court's reference to the "knowledge of Defendant" indicates that the court was focusing on contributory infringement, as knowledge is not an element of direct infringement. Perhaps, Sega's reference to direct infringement and that "copies ... are made" are to the direct liability of the "unknown users," as there can be no contributory infringement by a defendant without direct infringement by another. See 3 NIMMER ON COPYRIGHT s 12.04[A][3][a], at 12-89. Thus, the court finds that neither Playboy nor Sega requires finding Netcom liable for direct infringement of plaintiffs' exclusive right to reproduce their works. [FN17]

(FN17...To the extent that Sega holds that BBS operators are directly liable for copyright infringement when users upload infringing works to their systems, this court respectfully disagrees with the court's holding for the reasons discussed above. Further, such a holding was dicta, as there was evidence that the defendant knew of the infringing uploads by users and, in fact, actively encouraged such activity, thus supporting the contributory infringement theory. Id. at 683.

f. Public Distribution and Display?

Plaintiffs allege that Netcom is directly liable for making copies of their works. See FAC P 25. They also allege that Netcom violated their exclusive rights to publicly display copies of their works. FAC PP 44, 51. There are no allegations that Netcom violated plaintiffs' exclusive right to publicly distribute their works. However, in their discussion of direct infringement, plaintiffs insist that Netcom is liable for "maintaining" copies of [Erlich's] messages on its server for eleven days for access by its subscribers and 'USENET neighbors' " and they compare this case to the Playboy case, which discussed the right of public distribution. Opp'n at 7. Plaintiffs also argued this theory of infringement at oral argument. Tr. [FN18] 5:22. Because this could be an attempt to argue that Netcom has infringed plaintiffs' rights of public distribution and display, the court will address these arguments.

(FN18. References to "Tr." are to the reporter's transcript of the June 23, 1995 hearing on these motions.

Playboy concluded that the defendant infringed the plaintiff's exclusive rights to publicly distribute and display copies of its works. 839 F.Supp.
at 1556-57. The court is not entirely convinced that the mere possession of a digital copy on a BBS that is accessible to some members of the public constitutes direct infringement by the BBS operator. Such a holding suffers from the same problem of causation as the reproduction argument. Only the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are automatic and indiscriminate. Erlich could have posted his messages through countless access providers and the outcome would be the same: anyone with access to Usenet newsgroups would be able to read his messages. There is no logical reason to draw a line around Netcom and Klemesrud and say that they are uniquely responsible for distributing Erlich's messages. Netcom is not even the first link in the chain of distribution—Erlich had no direct relationship with Netcom but dealt solely with Klemesrud's BBS, which used Netcom to gain its Internet access. Every Usenet server has a role in the distribution, so plaintiffs' argument would create unreasonable liability. Where the BBS merely stores and passes along all messages sent by its subscribers and others, the BBS should not be seen as causing these works to be publicly distributed or displayed. Even accepting the Playboy court's holding, the case is factually distinguishable. Unlike the BBS in that case, Netcom does not maintain an archive of files for its users. Thus, it cannot be said to be "supply[ing] a product." In contrast to some of its larger competitors, Netcom does not create or control the content of the information available to its subscribers; it merely provides access to the Internet, whose content is controlled by no single entity. Although the Internet consists of many different computers networked together, some of which may contain infringing files, it does not make sense to hold the operator of each computer liable as an infringer merely because his or her computer is linked to a computer with an infringing file. It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration. Finding such a service liable would involve an unreasonably broad construction of public distribution and display rights. No purpose would be served by holding liable those who have no ability to control the information to which their subscribers have access, even though they might be in some sense helping to achieve the Internet's automatic "public distribution" and the users' "public" display of files.

g. Conclusion

The court is not persuaded by plaintiffs' argument that Netcom is directly liable for the copies that are made and stored on its computer. Where the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet. Such a result is unnecessary as there is already a party directly liable for causing the copies to be made. Plaintiffs occasionally claim that they only seek to hold liable a party that refuses to delete infringing files after they have been warned. However, such liability cannot be based on a theory of direct infringement, where knowledge is irrelevant. 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. 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. Cf. IITF Report at 69 (noting uncertainty regarding whether BBS operator should be directly liable for reproduction or distribution of files uploaded by a subscriber). [FN19]

FN19. Despite that uncertainty, the IITF Report recommends a strict liability paradigm for BBS operators. See IITF Report at 122-24. It recommends that Congress not exempt on-line service providers from strict liability because this would prematurely deprive the system of an incentive to get providers to reduce the damage to copyright holders by reducing the chances that users will infringe by educating them, requiring indemnification, purchasing insurance, and, where
efficient, developing technological solutions to screening out infringement. Denying strict liability in many cases would leave copyright owners without an adequate remedy since direct infringers may act anonymously or pseudonymously or may not have the resources to pay a judgment. Id.; see also Hardy, supra.

2. Contributory Infringement

Netcom is not free from liability just because it did not directly infringe plaintiffs' works; it may still be liable as a contributory infringer. Although there is no statutory rule of liability for infringement committed by others, [t]he absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringement on certain parties who have not themselves engaged in the infringing activity. For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 435, 104 S.Ct. 774, 785, 78 L.Ed.2d 574 (1984) (footnote omitted). Liability for participation in the infringement will be established where the defendant, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

a. Knowledge of Infringing Activity

Plaintiffs insist that Netcom knew that Erlich was infringing their copyrights at least after receiving notice from plaintiffs' counsel indicating that Erlich had posted copies of their works onto a.r.s. through Netcom's system. Despite this knowledge, Netcom continued to allow Erlich to post messages to a.r.s. and left the allegedly infringing messages on its system so that Netcom's subscribers and other Usenet servers could access them. Netcom argues that it did not possess the necessary type of knowledge because (1) it did not know of Erlich's planned infringing activities when it agreed to lease its facilities to Klemesrud, (2) it did not know that Erlich would infringe prior to any of his postings, (3) it is unable to screen out infringing postings before they are made, and (4) its knowledge of the infringing nature of Erlich's postings was too equivocal given the difficulty in assessing whether the registrations were valid and whether Erlich's use was fair. The court will address these arguments in turn.

Netcom cites cases holding that there is no contributory infringement by the lessors of premises that are later used for infringement unless the lessor had knowledge of the intended use at the time of the signing of the lease. See, e.g. Deutsch v. Arnold, 98 F.2d 686, 688 (2d Cir. 1938). [FN20] The contribution to the infringement by the defendant in Deutsch was merely to lease use of the premises to the infringer. Here, Netcom not only leases space but also serves as an access provider, which includes the storage and transmission of information necessary to facilitate Erlich's postings to a.r.s. Unlike a landlord, Netcom retains some control over the use of its system. See infra part I.B.3.a. Thus, the relevant time frame for knowledge is not when Netcom entered into an agreement with Klemesrud. It should be when Netcom provided its services to allow Erlich to infringe plaintiffs' copyrights. Cf. Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F.Supp. 399, 403 (S.D.N.Y. 1966) (analyzing knowledge at time that defendant rendered its particular service). It is undisputed that Netcom did not know that Erlich was infringing before it received notice from plaintiffs. Netcom points out that the alleged instances of infringement occurring on Netcom's system all happened prior to December 29, 1994, the date on which Netcom first received notice of plaintiffs' infringement claim against Erlich. See Pisani Feb. 8, 1995 Decl., P 6 & Exs. (showing latest posting made on December 29, 1994); McShane Feb. 8, 1995 Decl.; FAC PP 36-38 & Ex. I. Thus, there is no question of fact as to whether Netcom knew or should have known of Erlich's infringing activities that occurred more than 11 days before receipt of the December 28, 1994 letter.

FN20. Adopting such a rule would relieve a BBS of liability for
failing to take steps to remove infringing works from its system even after being handed a court's order finding infringement. This would be undesirable and is inconsistent with Netcom's counsel's admission that Netcom would have an obligation to act in such circumstances. Tr. 35:25; see also Tr. 42:18-42:20.

However, the evidence reveals a question of fact as to whether Netcom knew or should have known that Erlich had infringed plaintiffs' copyrights following receipt of plaintiffs' letter. Because Netcom was arguably participating in Erlich's public distribution of plaintiffs' works, there is a genuine issue as to whether Netcom knew of any infringement by Erlich before it was too late to do anything about it. If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement since its failure to simply cancel Erlich's infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in Erlich's public distribution of the message. Cf. R.T. Nimmer, THE LAW OF COMPUTER TECHNOLOGY P 15.11B, at S15-42 (2d ed. 1994) (opining that "where information service is less directly involved in the enterprise of creating unauthorized copies, a finding of contributory infringement is not likely").

Netcom argues that its knowledge after receiving notice of Erlich's alleged infringing activities was too equivocal given the difficulty in assessing whether registrations are valid and whether use is fair. Although a mere unsupported allegation of infringement by a copyright owner may not automatically put a defendant on notice of infringing activity, Netcom's position that liability must be unequivocal is unsupportable. While perhaps the typical infringing activities of BBSes will involve copying software, where BBS operators are better equipped to judge infringement, the fact that this involves written works should not distinguish it. Where works contain copyright notices within them, as here, it is difficult to argue that a defendant did not know that the works were copyrighted. To require proof of valid registrations would be impractical and would perhaps take too long to verify, making it impossible for a copyright holder to protect his or her works in some cases, as works are automatically deleted less than two weeks after they are posted. The court is more persuaded by the argument that it is beyond the ability of a BBS operator to quickly and fairly determine when a use is not infringement where there is at least a colorable claim of fair use. Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is a likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system. Since Netcom was given notice of an infringement claim before Erlich had completed his infringing activity, there may be a question of fact as to whether Netcom knew or should have known that such activities were infringing. Given the context of a dispute between a former minister and a church he is criticizing, Netcom may be able to show that its lack of knowledge that Erlich was infringing was reasonable. However, Netcom admits that it did not even look at the postings once given notice and that had it looked at the copyright notice and statements regarding authorship, it would have triggered an investigation into whether there was infringement.

Kobrin June 7, 1995 Decl. Ex. H, Hoffman Depo. at 125-126. These facts are sufficient to raise a question as to Netcom's knowledge once it received a letter from plaintiffs on December 29, 1994. [FN21]

FN21. The court does not see the relevance of plaintiffs' argument that Netcom's failure to investigate their claims of infringement or take actions against Erlich was a departure from Netcom's normal procedure. A policy and practice of acting to stop postings where there is inadequate knowledge of infringement in no way creates a higher standard of care under the Copyright Act as to subsequent claims of user infringement.

b. Substantial Participation

Where a defendant has knowledge of the primary infringer's infringing activities, it will be liable if it "induces, causes or materially

Providing a service that allows for the automatic distribution of all Usenet postings, infringing and noninfringing, goes well beyond renting a premises to an infringer. See Fonovisa, Inc. v. Cherry Auction, Inc., 847 F.Supp. 1492, 1496 (E.D.Cal. 1994) (finding that renting space at swap meet to known bootleggers not "substantial participation" in the infringers' activities). It is more akin to the radio stations that were found liable for rebroadcasting an infringing broadcast. See, e.g., Select Theatres Corp. v. Ronzoni Macaroni Corp., 59 U.S.P.Q. 288, 291 (S.D.N.Y. 1943). Netcom allows Erlich's infringing messages to remain on other Usenet servers worldwide. It does not completely relinquish control over how its system is used, unlike a landlord. Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs' copyrighted works, to hold Netcom liable for contributory infringement where Netcom has knowledge of Erlich's infringing postings yet continues to aid in the accomplishment of Erlich's purpose of publicly distributing the postings. Accordingly, plaintiffs do raise a genuine issue of material fact as to their theory of contributory infringement as to the postings made after Netcom was on notice of plaintiffs' infringement claim.

3. Vicarious Liability

Even if plaintiffs cannot prove that Netcom is contributarily liable for its participation in the infringing activity, it may still seek to prove vicarious infringement based on Netcom's relationship to Erlich. 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. See Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963). Unlike contributory infringement, knowledge is not an element of vicarious liability. 3 NIMMER ON COPYRIGHT s 12.04[A][1], at 12-70.

a. Right and Ability To Control

The first element of vicarious liability will be met if plaintiffs can show that Netcom has the right and ability to supervise the conduct of its subscribers. Netcom argues that it does not have the right to control its users' postings before they occur. Plaintiffs dispute this and argue that Netcom's terms and conditions, to which its subscribers [FN22] must agree, specify that Netcom reserves the right to take remedial action against subscribers. See, e.g., Francis Depo. at 124-126. Plaintiffs argue that under "netiquette," the informal rules and customs that have developed on the Internet, violation of copyrights by a user is unacceptable and the access provider has a duty to take measures to prevent this; where the immediate service provider fails, the next service provider up the transmission stream must act. See Castlemen Decl. PP 32-43. Further evidence of Netcom's right to restrict infringing activity is its prohibition of copyright infringement and its requirement that its subscribers indemnify it for any damage to third parties. See Kobrin May 5, 1995 Decl., Ex. G. Plaintiffs have thus raised a question of fact as to Netcom's right to control Erlich's use of its services.

FN22. In this case, Netcom is even further removed from Erlich's activities. Erlich was in a contractual relationship only with Klemesrud. Netcom thus dealt directly only with Klemesrud. However, it is not crucial that Erlich does not obtain access directly through Netcom. The issue is Netcom's right and ability to control the use of its system, which it can do indirectly by controlling Klemesrud's use.

Netcom argues that it could not possibly screen messages before they are posted given the speed and volume of the data that goes through its system. Netcom further argues that it has never exercised control over the content
of its users' postings. Plaintiffs' expert opines otherwise, stating that with an easy software modification Netcom could identify postings that contain particular words or come from particular individuals. Castlemen Decl. PP 39-43; see also Francis Depo. at 262-63; Hoffman Depo. at 173-74, 178. [FN23] Plaintiffs further dispute Netcom's claim that it could not limit Erlich's access to Usenet without kicking off all 500 subscribers of Klemesrud's BBS. As evidence that Netcom has in fact exercised its ability to police its users' conduct, plaintiffs cite evidence that Netcom has acted to suspend subscribers' accounts on over one thousand occasions. See Ex. J (listing suspensions of subscribers by Netcom for commercial advertising, posting obscene materials, and off-topic postings). Further evidence shows that Netcom can delete specific postings. See Tr. 9:16. Whether such sanctions occurred before or after the abusive conduct is not material to whether Netcom can exercise control. The court thus finds that plaintiffs have raised a genuine issue of fact as to whether Netcom has the right and ability to exercise control over the activities of its subscribers, and of Erlich in particular.

FN23. However, plaintiffs submit no evidence indicating Netcom, or anyone, could design software that could determine whether a posting is infringing.

b. Direct Financial Benefit

Plaintiffs must further prove that Netcom receives a direct financial benefit from the infringing activities of its users. For example, a landlord who has the right and ability to supervise the tenant's activities is vicariously liable for the infringements of the tenant where the rental amount is proportional to the proceeds of the tenant's sales. Shapiro, Bernstein, 316 F.2d at 306. However, where a defendant rents space or services on a fixed rental fee that does not depend on the nature of the activity of the lessee, courts usually find no vicarious liability because there is no direct financial benefit from the infringement. See, e.g., Roy Export Co. v. Trustees of Columbia University, 344 F.Supp. 1350, 1353 (S.D.N.Y. 1972) (finding no vicarious liability of university because no financial benefit from allowing screening of bootlegged films); Fonovisa, 847 F.Supp. at 1496 (finding swap meet operators did not financially benefit from fixed fee); see also 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, 415 (1995) (arguing that BBS operators "lease cyberspace" and should thus be treated like landlords, who are not liable for infringement that occurs on their premises). Plaintiffs argue that courts will find a financial benefit despite fixed fees. In Polygram International Publishing, Inc. v. Nevada/TIG, Inc., 855 F.Supp. 1314, 1330-33 (D.Mass. 1994), the court found a trade show organizer vicariously liable for the infringing performance of an exhibitor because, although the infringement did not affect the fixed rental fee received by the organizers, the organizers benefitted from the performances, which helped make the show a financial success. But see Artists Music, Inc. v. Reed Publishing, Inc., 31 U.S.P.Q.2d 1623, 1994 WL 191643, at (S.D.N.Y. 1994) (finding no vicarious liability for trade show organizers where revenues not increased because of infringing music performed by exhibitors). Plaintiffs cite two other cases where, despite fixed fees, defendants received financial benefits from allowing groups to perform infringing works over the radio without having to get an ASCAP license, which minimized the defendants' expenses. See Boz Scaggs Music v. KNQ Corp, 491 F.Supp. 908, 913 (D.Conn. 1980); Realsons v. Gulf Broadcasting Corp., 824 F.Supp. 89, 92 (M.D.La. 1993). Plaintiffs' cases are factually distinguishable. Plaintiffs cannot provide any evidence of a direct financial benefit received by Netcom from Erlich's infringing postings. Unlike Shapiro, Bernstein, and like Fonovisa, Netcom receives a fixed fee. There is no evidence that infringement by Erlich, or any other user of Netcom's services, in any way enhances the value of Netcom's services to subscribers or attracts new subscribers. Plaintiffs argue, however, that Netcom somehow derives a benefit from its purported "policy of refusing to take enforcement actions against its subscribers and others who transmit infringing messages over its computer networks." Opp'n at 18. Plaintiffs point to Netcom's advertisements that, compared to competitors like CompuServe and America Online, Netcom provides easy, regulation-free Internet access. Plaintiffs
assert that Netcom's policy attracts copyright infringers to its system, resulting in a direct financial benefit. The court is not convinced that such an argument, if true, would constitute a direct financial benefit to Netcom from Erlich's infringing activities. See Fonovisa, 847 F.Supp. at 1496 (finding no direct financial benefit despite argument that lessees included many vendors selling counterfeit goods and that clientele sought "bargain in basement prices"). Further, plaintiffs' argument is not supported by probation evidence. The only "evidence" plaintiffs cite for their supposition is the declaration of their counsel, Elliot Abelson, who states that [o]n April 7, 1995, in a conversation regarding Netcom's position related to this case, Randolf Rice, attorney for Netcom, informed me that Netcom's executives are happy about the publicity it is receiving in the press as a result of this case. Mr. Rice also told me that Netcom was concerned that it would lose business if it took action against Erlich or Klemesrud in connection with Erlich's infringements. Abelson Decl. P 2.

Netcom objects to this declaration as hearsay and as inadmissible evidence of statements made in compromise negotiations. Fed.R.Ev. 801, 408. Whether or not this declaration is admissible, it does not support plaintiffs' argument that Netcom either has a policy of not enforcing violations of copyright laws by its subscribers or, assuming such a policy exists, that Netcom's policy directly financially benefits Netcom, such as by attracting new subscribers. Because plaintiffs have failed to raise a question of fact on this vital element, their claim of vicarious liability fails. See Roy Export, 344 F.Supp. at 1353.

4. First Amendment Argument

Netcom argues that plaintiffs' theory of liability contravenes the first amendment, as it would chill the use of the Internet because every access provider or user would be subject to liability when a user posts an infringing work to a Usenet newsgroup. While the court agrees that an overbroad injunction might implicate the First Amendment, see In re Capital Cities/ABC, Inc., 918 F.2d 140, 144 (11th Cir. 1990), [FN24] imposing liability for infringement where it is otherwise appropriate does not necessarily raise a First Amendment issue. The copyright concepts of the idea/expression dichotomy and the fair use defense balance the important First Amendment rights with the constitutional authority for "promot[ing] the progress of science and useful arts," U.S. CONST. art. I, s 8, cl. 8; 1 NIMMER ON COPYRIGHT s 1.10(B), at 1-71 to -83.

Netcom argues that liability here would force Usenet servers to perform the impossible--screening all the information that comes through their systems. However, the court is not convinced that Usenet servers are directly liable for causing a copy to be made, and absent evidence of knowledge and participation or control and direct profit, they will not be contributorily or vicariously liable. If Usenet servers were responsible for screening all messages coming through their systems, this could have a serious chilling effect on what some say may turn out to be the best public forum for free speech yet devised. See Jerry Berman & Daniel J. Weitzner, Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media, 104 YALE L.J. 1619, 1624 (1995) (praising decentralized networks for opening access to all with no entity stifling independent sources of speech); Rose, supra, at 4. [FN25] Finally, Netcom admits that its First Amendment argument is merely a consideration in the fair use argument, which the court will now address. See Reply at 24.

FN24. For example, plaintiffs' demand that the court order Netcom to terminate Klemesrud's BBS's access to the Internet, thus depriving all 500 of his subscribers, would be overbroad, as it would unnecessarily keep hundreds of users, against whom there are no allegations of copyright infringement, from accessing a means of speech. The overbreadth is even more evident if, as plaintiffs contend, there is a way to restrict only Erlich's access to a.r.s.

FN25. Netcom additionally argues that plaintiffs' theory of liability would have a chilling effect on users, who would be liable for merely browsing infringing works. Browsing technically causes an infringing copy of the digital information to be made in the screen memory. MAI holds that such a copy is fixed even when information is temporarily placed in RAM, such as the screen RAM. The temporary copying involved
in browsing is only necessary because humans cannot otherwise perceive
digital information. It is the functional equivalent of reading,
which does not implicate the copyright laws and may be done by anyone
in a library without the permission of the copyright owner. However,
it can be argued that the effects of digital browsing are different
because millions can browse a single copy of a work in cyberspace,
while only one can read a library's copy at a time. Absent a
commercial or profit-depriving use, digital browsing is probably a
feasible one; there could hardly be a market for licensing the temporary
copying of digital works onto computer screens to allow browsing.
Unless such a use is commercial, such as where someone reads a
copyrighted work online and therefore decides not to purchase a copy
from the copyright owner, fair use is likely. Until reading a work
online becomes as easy and convenient as reading a paperback,
copyright owners do not have much to fear from digital browsing and
there will not likely be much market effect. Additionally, unless a
user has reason to know, such as from the title of a message, that the
message contains copyrighted materials, the browser will be protected
by the innocent infringer doctrine, which allows the court to award no
damages in appropriate circumstances. In any event, users should
hardly worry about a finding of direct infringement; it seems highly
unlikely from a practical matter that a copyright owner could prove
such infringement or would want to sue such an individual.

5. Fair Use Defense

Assuming plaintiffs can prove a violation of one of the exclusive rights
guaranteed in section 106, there is no infringement if the defendant's use
is fair under section 108. The proper focus here is on whether Netcom's
actions qualify as fair use, not on whether Erlich himself engaged in fair
use; the court has already found that Erlich was not likely entitled to his
own fair use defense, as his postings contained large portions of
plaintiffs' published and unpublished works quoted verbatim with little
added commentary. Although the author has the exclusive rights to reproduce,
publicly distribute, and publicly display a copyrighted work under section
106, these rights are limited by the defense of "fair use." 17 U.S.C. §
107. The defense permits and requires courts to avoid rigid application of
the copyright statute when, on occasion, it would stifle the very creativity
which that law is designed to foster." Campbell v. Acuff-Rose Music, Inc.,
--- U.S. ----, ----, 114 S.Ct. 1164, 1170, 127 L.Ed.2d 500 (1994) (citation
omitted). Congress has set out four nonexclusive factors to be considered
in determining the availability of the fair use defense: (1) the purpose and
character of the use, including whether such use is of a commercial nature
or is for nonprofit educational purposes; (2) the nature of the copyrighted
work; (3) the amount and substantiality of the portion used in relation to
the copyrighted work as a whole; and (4) the effect of the use upon the
potential market for or value of the copyrighted work. 17 U.S.C. § 107. The
fair use doctrine calls for a case-by-case analysis. Campbell, --- U.S. at
----, 114 S.Ct. at 1170. All of the factors "are to be explored, and the
results weighed together, in light of the purposes of copyright." Id. at
----. ----, 114 S.Ct. at 1170-71.

a. First Factor: Purpose and Character of the Use

The first statutory factor looks to the purpose and character of the
defendant's use. Netcom's use of plaintiffs' works is to carry out its
commercial function as an Internet access provider. Such a use, regardless
of the underlying uses made by Netcom's subscribers, is clearly commercial.
Netcom's use, though commercial, also benefits the public in allowing for
the functioning of the Internet and the dissemination of other creative
works, a goal of the Copyright Act. See Sega v. Accolade, 977 F.2d 1510,
1523 (9th Cir. 1992) (holding that intermediate copying to accomplish
reverse engineering of software fair use despite commercial nature of
activity; considering public benefit of use). The Campbell Court
emphasized that a commercial use does not dictate against a finding of fair
use, as most of the uses listed in the statute are "generally conducted for
profit in this country." --- U.S. at ----, 114 S.Ct. at 1174. Although
Netcom gains financially from its distribution of messages to the Internet,
it's financial incentive is unrelated to the infringing activity and the
defendant receives no direct financial benefit from the acts of infringement. Therefore, the commercial nature of the defendant's activity should not be dispositive. Moreover, there is no easy way for a defendant like Netcom to secure a license for carrying every possible type of copyrighted work onto the Internet. Thus, it should not be seen as "profit[ing] from the exploitation of the copyrighted work without paying the customary prices." Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 562, 105 S.Ct. 2218, 2231, 85 L.Ed.2d 588 (1985).

It is undisputed that, unlike the defendants in Playboy and Sega, Netcom does not directly gain anything from the content of the information available to its subscribers on the Internet. See supra part I.B.3.b. Because it does not itself provide the files or solicit infringing works, its purpose is different from that of the defendants in Playboy and Sega. Because Netcom's use of copyrighted materials served a completely different function than that of the plaintiffs, this factor weighs in Netcom's favor, see Hustler Magazine, Inc. v. Moral Majority, Inc., 606 F.Supp. 1525, 1535 (C.D.Cal. 1985), aff'd, 796 F.2d 1148 (9th Cir. 1986), notwithstanding the otherwise commercial nature of Netcom's use.

b. Second Factor: Nature of the Copyrighted Work

The second factor focuses on two different aspects of the copyrighted work: whether it is published or unpublished and whether it is informational or creative. [FN26] Plaintiffs rely on the fact that some of the works transmitted by Netcom were unpublished and some were arguably highly creative and original. However, because Netcom's use of the works was merely to facilitate their posting to the Usenet, which is an entirely different purpose than plaintiffs' use (or, for that matter, Erlich's use), the precise nature of those works is not important to the fair use determination. See Campbell, --- U.S. at ----, 114 S.Ct. at 1175 (finding creative nature of work copied irrelevant where copying for purposes of parody); Hustler Magazine, 606 F.Supp. at 1537; 3 NIMMER ON COPYRIGHT § 13.05[A][2][a], at 13-177 ("It is sometimes necessary, in calibrating the fair use defense, to advert to the defendant's usage simultaneously with the nature of the plaintiff's work.").

FN26. A recent report noted that a third aspect of the nature of the work may be relevant: whether it is in digital or analog form. ITTF Report at 78. Although the copyright laws were developed before digital works existed, they have certainly evolved to include such works, and this court can see no reason why works should deserve less protection because they are in digital form, especially where, as here, they were not put in such form by plaintiffs.

c. Third Factor: Amount and Substantiality of the Portion Used

The third factor concerns both the percentage of the original work that was copied and whether that portion constitutes the "heart" of the copyrighted work. Harper & Row, 471 U.S. at 564-65, 105 S.Ct. at 2232-33. Generally, no more of a work may be copied than is necessary for the particular use. See Supermarket of Homes v. San Fernando Valley Board of Realtors, 786 F.2d 1400, 1409 (9th Cir. 1986). The copying of an entire work will ordinarily militate against a finding of fair use, although this is not a per se rule.

Sony, 464 U.S. at 449-450, 104 S.Ct. at 792-793.

Plaintiffs have shown that Erlich's postings copied substantial amounts of the originals or, in some cases, the entire works. Netcom, of course, made available to the Usenet exactly what was posted by Erlich. As the court found in Sony, the mere fact that all of a work is copied is not determinative of the fair use question, where such total copying is essential given the purpose of the copying. Id. (allowing total copying in context of time-shifting copyrighted television shows by home viewers). For example, where total copying was necessary to carry out the defendants' beneficial purpose of reverse engineering software to get at the ideas found in the source code, the court found fair use. Sega v. Accolade, 977 F.2d at 1526-27. Here, Netcom copied no more of plaintiffs' works than necessary to function as a Usenet server. Like the defendant in Sega v. Accolade, Netcom had no practical alternative way to carry out its socially useful purpose;
a Usenet server must copy all files, since the prescreening of postings for potential copyright infringement is not feasible. 977 F.2d at 1526. Accordingly, this factor should not defeat an otherwise valid defense.

d. Fourth Factor: Effect of the Use upon the Potential Market for the Work

The fourth and final statutory factor concerns "the extent of market harm caused by the particular actions of the alleged infringer" and "whether unattributed and widespread conduct of the sort engaged in by the defendant ... would result in a substantially adverse impact on the potential market" for the original." Campbell, --- U.S. at ----, 114 S.Ct. at 1177 (quoting 3 NIMMER ON COPYRIGHT s 13.05[A] [4] ) (remanding for consideration of this factor). Although the results of all four factors must be weighed together, id. at ----, 114 S.Ct. at 1171, the fourth factor is the most important consideration, 3 NIMMER ON COPYRIGHT s 13.05[A] [4], at 13-188 to -189 (citing Harper & Row, 471 U.S. at 566, 105 S.Ct. at 2233), 13-207 (observing that fourth factor explains results in recent Supreme Court cases). Netcom argues that there is no evidence that making accessible plaintiffs' works, which consist of religious scriptures and policy letters, will harm the market for these works by preventing someone from participating in the Scientology religion because they can view the works on the Internet instead. Further, Netcom notes that the relevant question is whether the postings fulfill the demand of an individual who seeks to follow the religion's teachings, and not whether they suppress the desire of an individual who is affected by the criticism posted by Erlich. Netcom argues that the court must focus on the "normal market" for the copyrighted work, which in this case is through a Scientology-based organization. Plaintiffs respond that the Internet's extremely widespread distribution--where more than 25 million people worldwide have access--multiplies the effects of market substitution. In support of its motion for a preliminary injunction against Erlich, plaintiffs submitted declarations regarding the potential effect of making the Church's secret scriptures available over the Internet. Plaintiffs point out that, although the Church currently faces no competition, groups in the past have used stolen copies of the Church's scriptures in charging for Scientology-like religious training. See, e.g., Bridge Publications, Inc. v. Vien, 827 F.Supp. 629, 633-34 (S.D.Cal. 1993); Religious Technology Center v. Wollersheim, 796 F.2d 1076, 1078-79 (9th Cir. 1986), cert. denied, 479 U.S. 1103, 107 S.Ct. 1336, 94 L.Ed.2d 187 (1987). This evidence raises a genuine issue as to the possibility that Erlich's postings, made available over the Internet by Netcom, could hurt the market for plaintiffs' works.

e. Equitable Balancing

In balancing the various factors, the court finds that there is a question of fact as to whether there is a valid fair use defense. Netcom has not justified its copying plaintiffs' works to the extent necessary to establish entitlement to summary judgment in light of evidence that it knew that Erlich's use was infringing and had the ability to prevent its further distribution. While copying all or most of a work will often preclude fair use, courts have recognized the fair use defense where the purpose of the use is beneficial to society, complete copying is necessary given the type of use, the purpose of the use is completely different than the purpose of the original, and there is no evidence that the use will significantly harm the market for the original. This case is distinguishable from those cases recognizing fair use despite total copying. In Sony, the home viewers' use was not commercial and the viewers were allowed to watch the entire shows for free. In Sega v. Accolade, the complete copying was necessitated to access the unprotectable idea in the original. Here, plaintiffs never gave either Erlich or Netcom permission to view or copy their works. Netcom's use has some commercial aspects. Further, Netcom's copying is not for the purpose of getting to the unprotected idea behind plaintiffs' works. Although plaintiffs may ultimately lose on their infringement claims if, among other things, they cannot prove that posting their copyrighted works will harm the market for these works, see Religious Technology Center v. Lerma, 897 F.Supp. 260, ---- (E.D.Va. August 30, 1995) (finding fair use defense exists where no separate market for works because Scientologists cannot effectively use them without the Church's supervision); Religious Technology Center v. P.A.C.T.NET, Inc., 901 F.Supp. 1519, 1522-26 (D.Colo.
September 15, 1995) (finding no showing of a potential effect on the market for plaintiffs' works), fair use presents a factual question on which plaintiffs have at least raised a genuine issue of fact. Accordingly, the court does not find that Netcom's use was fair as a matter of law.

C. Conclusion

The court finds that plaintiffs have raised a genuine issue of fact regarding whether Netcom should have known that Erlich was infringing their copyrights after receiving a letter from plaintiffs, whether Netcom substantially participated in the infringement, and whether Netcom has a valid fair use defense. Accordingly, Netcom is not entitled to summary judgment on plaintiffs' claim of contributory copyright infringement. However, plaintiffs' claims of direct and vicarious infringement fail.

II. KLEMSERUD'S MOTION FOR JUDGMENT ON THE PLEADINGS

A. Standards for Judgment on the Pleadings

A motion for judgment on the pleadings pursuant to Federal Rule of Civil Procedure 12(c) is directed at the legal sufficiency of a party's allegations. A judgment on the pleadings is proper when there are no issues of material fact, and the moving party is entitled to judgment as a matter of law. General Conference Corp. v. Seventh Day Adventist Church, 887 F.2d 228, 230 (9th Cir. 1989), cert. denied, 493 U.S. 1079, 110 S.Ct. 1134, 107 L.Ed.2d 1039 (1990); Hal Roach Studios v. Richard Feiner & Co., 896 F.2d 1542, 1550 (9th Cir. 1989). In ruling on a motion for judgment on the pleadings, district courts must accept all material allegations of fact alleged in the complaint as true, and resolve all doubts in favor of the nonmoving party. Id. The court need not accept as true conclusory allegations or legal characterizations. Western Mining Council v. Watt, 643 F.2d 618, 624 (9th Cir. 1981). Materials submitted with the complaint may be considered. Hal Roach Studios, 896 F.2d at 1555. All affirmative defenses must clearly appear on the face of the complaint. McCalden v. California Library Ass'n, 955 F.2d 1214, 1219 (9th Cir. 1990).

B. Copyright Infringement

1. Direct Infringement

First, plaintiffs allege that Klemsrud directly infringed their copyrights by "reproducing and publishing plaintiffs' works." FAC P 35. The complaint alleges that "Erlich ... caused copies of [plaintiffs' works] to be published, without authorization, on the BBS computer maintained by Klemsrud" and that "Klemsrud's BBS computer, after receiving and storing for some period of time the copies of the Works sent to it from Erlich, created additional copies of the works and sent these copies to Netcom's computer." FAC P 34. The allegations against Klemsrud fail for the same reason the court found that Netcom was entitled to judgment as a matter of law on the direct infringement claim. There are no allegations that Klemsrud took any affirmative steps to cause the copies to be made. The allegations, in fact, merely say that "Erlich ... caused" the copies to be made and that Klemsrud's computer, not Klemsrud himself, created additional copies. There are no allegations in the complaint to overcome the missing volitional or causal elements necessary to hold a BBS operator directly liable for copying that is automatic and caused by a subscriber. See supra part I.B.1.

2. Contributory Infringement

Second, the complaint alleges that Klemsrud is contributorily liable. FAC P 35. It further alleges that plaintiffs repeatedly objected to Klemsrud's actions and informed him that Erlich's (and his) actions constituted infringement. FAC P 36. A letter attached to the complaint indicates that such notice was first sent to Klemsrud on December 30, 1994. FAC, Ex. I. Despite the warnings, Klemsrud allegedly refused to assist plaintiffs in compelling Erlich to stop his postings and refused to stop receiving, copying, transmitting and publishing the postings. FAC P 38. To state a claim for contributory infringement, plaintiffs must allege that Klemsrud
knew or should have known of Erlich's infringing actions at the time they occurred and yet substantially participated by "induc[ing], caus[ing] or materially contribut[ing] to the infringing conduct" of Erlich. Gershwin, 443 F.2d at 1162. For the reasons discussed in connection with Netcom's motion, the court finds plaintiffs' pleadings sufficient to raise an issue of contributory infringement.

3. Vicarious Liability

The third theory of liability argued by plaintiffs, vicarious liability, is not specifically mentioned in the complaint. Nonetheless, this theory fails as a matter of law because there are insufficient factual allegations to support it. Plaintiffs must show that Klemesrud had the right and ability to control Erlich's activities and that Klemesrud had a direct financial interest in Erlich's infringement. Shapiro, Bernstein, 316 F.2d at 306. A letter from Klemesrud to plaintiffs' counsel states that Klemesrud would comply with plaintiffs' request to take actions against Erlich by deleting the infringing postings from his BBS if plaintiffs mailed him the original copyrighted work and he found that they matched the allegedly infringing posting. FAC, Ex. J. Plaintiffs argue that this letter indicates Klemesrud's ability and right to control Erlich's activities on his BBS. The court finds that this letter, construed in the light most favorable to plaintiffs, raises a question as to whether plaintiffs can show that Klemesrud, in the operation of his BBS, could control Erlich's activities, such as by deleting infringing postings. However, plaintiffs' failure to allege a financial benefit is fatal to their claim for vicarious liability.

The complaint alleges that Klemesrud is in the business of operating a BBS for subscribers for a fee. The complaint does not say how the fee is collected, but there are no allegations that Klemesrud's fee, or any other direct financial benefit received by Klemesrud, varies in any way with the content of Erlich's postings. Nothing in or attached to the complaint states that Klemesrud in any way profits from allowing Erlich to infringe copyrights. Plaintiffs are given 30 days leave in which to amend to cure this pleadings deficiency if they can do so in good faith.

III. PRELIMINARY INJUNCTION AGAINST NETCOM AND KLEMESEKUD

A. Legal Standards for a Preliminary Injunction

A party seeking a preliminary injunction may establish its entitlement to equitable relief by showing either (1) a combination of probable success on the merits and the possibility of irreparable injury, or (2) serious questions as to these matters and the balance of hardships tipping sharply in the movant's favor. First Brands Corp. v. Fred Meyer, Inc., 809 F.2d 1378, 1381 (9th Cir. 1987). These two tests are not separate, but represent a "continuum" of equitable discretion whereby the greater the relative hardship to the moving party, the less probability of success need be shown. Regents of University of California v. American Broadcasting Cos., 747 F.2d 511, 515 (9th Cir. 1984). The primary purpose of a preliminary injunction is to preserve the status quo pending a trial on the merits. Los Angeles Memorial Coliseum Commission v. National Football League, 634 F.2d 1197, 1200 (9th Cir. 1980).

B. Likelihood of Success

The court finds that plaintiffs have not met their burden of showing a likelihood of success on the merits as to either Netcom or Klemesrud. The only viable theory of infringement is contributory infringement, and there is little evidence that Netcom or Klemesrud knew or should have known that Erlich was engaged in copyright infringement of plaintiffs' works and was not entitled to a fair use defense, especially as they did not receive notice of the alleged infringement until after all but one of the postings were completed. Further, their participation in the infringement was not substantial. Accordingly, plaintiffs will not likely prevail on their claims.

C. Irreparable Injury

The court will presume irreparable harm for the copyright claim where
plaintiffs have shown a likelihood of success on their claims of infringement. Johnson Controls, Inc. v. Phoenix Control Systems, Inc., 886 F.2d 1173, 1174 (9th Cir. 1989). Here, however, plaintiffs have not made an adequate showing of likelihood of success. More importantly, plaintiffs have not shown that the current preliminary injunction prohibiting Erlich from infringing plaintiffs' copyrights will not be sufficient to avoid any harm to plaintiffs' intellectual property rights.

D. First Amendment Concerns

There is a strong presumption against any injunction that could act as a "prior restraint" on free speech, citing CBS, Inc. v. Davis, --- U.S. ----, 114 S.Ct. 912, 913-14, 127 L.Ed.2d 358 (1994) (Justice Blackmun, as Circuit Justice, staying a preliminary injunction prohibiting CBS from airing footage of inside of meat packing plant). Because plaintiffs seek injunctive relief that is broader than necessary to prevent Erlich from committing copyright infringement, there is a valid First Amendment question raised here. Netcom and Klemesrud play a vital role in the speech of their users. Requiring them to prescreen postings for possible infringement would chill their users' speech. Cf. In re Capital Cities/ABC, Inc, 918 F.2d at 144.

E. Conclusion

Plaintiffs have not shown a likelihood of success on the merits of their copyright claims nor irreparable harm absent an injunction against defendants Netcom and Klemesrud. Accordingly, plaintiffs are not entitled to a preliminary injunction.

IV. ORDER

The court denies Netcom's motion for summary judgment and Klemesrud's motion for judgment on the pleadings, as a triable issue of fact exists on the claim of contributory infringement. The court also gives plaintiffs 30 days leave in which to amend to state a claim for vicarious liability against defendant Klemesrud, if they can do so in good faith. Plaintiffs' application for a preliminary injunction against defendants Netcom and Klemesrud is denied. The parties shall appear for a case management conference at 10:30 a.m. on Friday, January 19, 1996. The deadline for completing required disclosures is January 5, 1996. The joint case management conference statement must be filed by January 12, 1996.

-----------------------------------------------------------------------------------

NETCOM ON-LINE COMMUNICATION SERVICES, INC., Dennis Erlich, and
Tom Klemesrud, Defendants.

United States District Court, N.D. California.

Not Reported in F.Supp.

AMENDED TEMPORARY RESTRAINING ORDER

WHYTE, District Judge.

On February 10, 1995, this court issued a temporary restraining order ("TRO") against defendants Dennis Erlich ("Erlich"), Netcom On-Line Communication Services, Inc. ("Netcom"), and Tom Klemesrud ("Klemesrud"). At a hearing to show cause why a preliminary injunction should not be issued held on February 21, 1995, the court dissolved the temporary restraining order as to defendants Netcom and Klemesrud and denied plaintiffs' request for a preliminary injunction against them. As to those defendants the plaintiffs have not established a sufficient continuing threat of irreparable harm or a probability of success on the merits. Further, the
(2) in the second undesignated paragraph N

(A) by inserting "or receives," after "takes";

(B) by inserting "or interactive computer service (as defined in
section 230(f)(2) of the Communications Act of 1934)" after "common
carrier"; and

(C) by inserting "or importation" after "carriage".

(b) TRANSPORTATION FOR PURPOSES OF SALE OR DISTRIBUTION. NThe first
undesignated paragraph of section 1465 of title 18, United States Code,
is amended -

(1) by striking "transports in" and inserting "transports or
travels in, or uses a facility or means of,";

(2) by inserting "or an interactive computer service (as defined in
section '230(f)(2) of the Communications Act of 1934) in or
affecting such commerce" after "foreign commerce" the first place
it appears;

(3) by striking ", or knowingly travels in" and all that follows
through "obscene material in inter state or foreign commerce," and
inserting "of".

(c) INTERPRETATION. N The amendments made by this section are clarifying
and shall not be interpreted to limit or repeal any prohibition
contained in sections 1462 and 1465 of title 18, United States Code,
before such amendment, under the rule established in United States v.

SEC. 508. COERCION AND ENTICEMENT OF MINORS.

Section 2422 of title 18, United States Code, is amended N

(1) by inserting "(a)" before "Whoever knowingly"; and

(2) by adding at the end the following

"(b) Whoever, using any facility or means of inter state or foreign
commerce, including the mail, or within the special maritime and
territorial jurisdiction of the United States, knowingly persuades,
duces, entices, or coerces any individual who has not attained the age
of 18 years to engage in prostitution or any sexual act for which
person may be criminally prosecuted, or attempts to do so shall be fined
under this title or imprisoned not more than 10 years, or both."

SEC. 509. ONLINE FAMILY EMPOWERMENT.

Title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is
amended by adding at the end the following new section:

"SEC. 230. PROTECTION FOR PRIVATE BLOCKING AND SCREENING OF OFFENSIVE
MATERIAL

"(a) FINDINGS. N The Congress finds the following:

"(1) The rapidly developing array of Internet and other interactive
computer services available to individual Americans represent an
extraordinary advance in the availability of educational and
informational resources to our citizens.

"(2) These services offer users a great degree of control over the
information that they receive, as well as the potential for even
greater control in the future as technology develops.

"(3) The Internet and other interactive computer services offer a
forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

"(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

"(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

"(b) POLICY.Ñ It is the policy of the United StatesÑ

"(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

"(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

"(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

"(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

"(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

"(c) PROTECTION FOR 'GOOD SAMARITAN BLOCKING AND SCREENING OF OFFENSIVE MATERIAL.Ñ

"(1) TREATMENT OF PUBLISHER OR SPEAKER.ÑNo provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

"(2) CIVIL LIABILITY.ÑNo provider or user of an interactive computer service shall be held liable on account of

"(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

"(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

"(d) EFFECT ON OTHER LAWS.Ñ

"(1) NO EFFECT ON CRIMINAL LAW.ÑNothing in this section shall be construed to impair the enforcement of section 223 of this Act, chapter 71 (relating to obscenity) or 110 (relating to exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

"(2) NO EFFECT ON INTELLECTUAL PROPERTY LAW.ÑNothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

"(3) STATE LAW.ÑNothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with
this section. No cause of action may be brought and no liability may be imposed under any State or local law that is in consistent with this section.

"(4) NO EFFECT ON COMMUNICATIONS PRIVACY LAW. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

"(f) DEFINITIONS. As used in this section:

"(1) INTERNET. The term 'Internet' means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

"(2) INTERACTIVE COMPUTER SERVICE. The term 'interactive computer service' means an 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.

"(3) INFORMATION CONTENT PROVIDER. The term 'information content provider' means 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.

"(4) ACCESS SOFTWARE PROVIDER. The term 'access software provider' means 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."
PUBLISHED

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

KENNETH M. ZERAN, Plaintiff-Appellant,

v.

AMERICA ONLINE, INCORPORATED, Defendant-Appellee.

No. 97-1523

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria.

T. S. Ellis, III, District Judge.

(CA-96-1564-A)

Argued: October 2, 1997

Decided: November 12, 1997

Before WILKINSON, Chief Judge, RUSSELL, Circuit Judge, and BOYLE, Chief United States District Judge for the Eastern District of North Carolina, sitting by designation.

Affirmed by published opinion. Chief Judge Wilkinson wrote the opinion, in which Judge Russell and Chief Judge Boyle joined.

COUNSEL

ARGUED: John Saul Edwards, LAW OFFICES OF JOHN S. EDWARDS, Roanoke, Virginia; Leo Kayser, III, KAYSER & REDFERN, New York, New York, for Appellant.

Patrick Joseph Carome, WILMER, CUTLER & PICKERING, Washington, D.C., for Appellee.

ON BRIEF: John Payton, Samir Jain, WILMER, CUTLER & PICKERING, Washington, D.C.; Randall J. Boe, AMERICA ONLINE, INC., Dulles, Virginia, for Appellee.

OPINION

WILKINSON, Chief Judge:

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The district court granted judgment for AOL on the grounds that the Communications Decency Act of 1996 ("CDA") -- 47 U.S.C. Section[s] 230 -- bars Zeran's claims. Zeran appeals, arguing that Section(s) 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that Section(s) 230 does not apply here
because his claims arise from AOL's alleged negligence prior to the CDA's enactment. Section 230, however, plainly immunizes computer service providers like AOL from liability for information that originates with third parties. Furthermore, Congress clearly expressed its intent that Section(s) 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgement of the district court.

I.

"The Internet is an international network of interconnected computers." currently used by approximately 40 million people worldwide. Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997). One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. Id. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgment on the pleadings, see Fed. R. Civ. P. 12(c), so we accept the facts alleged in the complaint as true. Bruce v. Riddle, 631 F.2d 272, 273 (4th Cir. 1980). On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRKO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRKO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRKO made an on-air apology, the number of calls to Zeran's residence
finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRKO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages.1 After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. Section(s) 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. Section(s) 230 as an affirmative defense. AOL then moved for judgment on the pleadings pursuant to Fed. R. Civ. P. 12(c). The district court granted AOL's motion, and Zeran filed this appeal.

II.

A.

Because Section(s) 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

The relevant portion of Section(s) 230 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. Section(s) 230(c)(1).2 By its plain language, Section(s) 230 creates a policy of immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, Section(s) 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content -- are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Id. Section(s) 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, with a minimum of government regulation." Id. Section(s) 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." Id. Section(s) 230(b)(2) (emphasis added).

None of this, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of
computer." Id. Section(s) 230(b)(5). Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages.

Congress’ purpose in providing the Section(s) 230 immunity was thus evident. Interactive computer services have millions of users. See Reno v. ACLU, 117 S. Ct. at 2334 (noting that at time of district court trial, "commercial online services had almost 12 million individual subscribers"). The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of Section(s) 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, Section(s) 230 responded to a New York state court decision, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). There, the plaintiffs sued Prodigy -- an interactive computer service like AOL -- for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

Congress enacted Section(s) 230 to remove the disincentives to self-regulation created by the Stratton Oakmont decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted Section(s) 230’s broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. Section(s) 230(b)(4). In line with this purpose, Section(s) 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

B.

Zeran argues, however, that the Section(s) 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion. W. Page Keeton et al., Prosser and Keeton on the Law of Torts Section(s) 113, at 810 (5th ed. 1984). According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Id. at 811 (explaining that distributors are not liable "in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published").
Zeran contends that he provided AOL with sufficient notice of
the defamatory statements appearing on the company's bulletin board.
This notice is significant, says Zeran, because AOL could be held liable
as a distributor only if it acquired knowledge of the defamatory
statements' existence.

Because of the difference between these two forms of liability,
Zeran contends that the term "distributor" carries a legally distinct
meaning from the term "publisher." Accordingly, he asserts that
Congress' use of only the term "publisher" in Section(s) 230 indicates a
purpose to immunize service providers only from publisher liability. He
argues that distributors are left unprotected by Section(s) 230 and,
therefore, his suit should be permitted to proceed against AOL. We
disagree. Assuming arguendo that Zeran has satisfied the requirements
for imposition of distributor liability, this theory of liability is
merely a subset, or a species, of publisher liability, and is therefore
also foreclosed by Section(s) 230.

The terms "publisher" and "distributor" derive their legal
significance from the context of defamation law. Although Zeran attempts
to artfully plead his claims as ones of negligence, they are
indistinguishable from a garden variety defamation action. Because the
publication of a statement is a necessary element in a defamation
action, only one who publishes can be subject to this form of tort
liability. Restatement (Second) of Torts Section(s) 558(b) (1977);
Keeton et al., supra, Section(s) 113, at 802. Publication does not only
describe the choice by an author to include certain information. In
addition, both the negligent communication of a defamatory statement and
the failure to remove such a statement when first communicated by
another party -- each alleged by Zeran here under a negligence label --
constitute publication. Restatement (Second) of Torts Section(s) 577;
see also Tacket v. General Motors Corp., 836 F.2d 1042, 1046-47 (7th
Cir. 1987). In fact, every repetition of a defamatory statement is
considered a publication. Keeton et al., supra, Section(s) 113, at 799.

In this case, AOL is legally considered to be a publisher.
"[E]very one who takes part in the publication . . . is charged with
publication." Id. Even distributors are considered to be publishers for
purposes of defamation law:

Those who are in the business of making their facilities
available to disseminate the writings composed, the speeches made, and
the information gathered by others may also be regarded as participating
to such an extent in making the books, newspapers, magazines, and
information available to others as to be regarded as publishers. They
are intentionally making the contents available to others, sometimes
without knowing all of the contents -- including the defamatory
content -- and sometimes without any opportunity to ascertain, in
advance, that any defamatory matter was to be included in the matter
published.

Id. at 803. AOL falls squarely within this traditional
definition of a publisher and, therefore, is clearly protected
by Section(s) 230's immunity.

Zeran contends that decisions like Stratton Oakmont and Cubby,
legal distinction between publishers and distributors. He misapprehends,
however, the significance of that distinction for the legal issue we
consider here. It is undoubtedly true that mere conduits, or
distributors, are subject to a different standard of liability. As
explained above, distributors must at a minimum have knowledge of the
existence of a defamatory statement as a prerequisite to liability. But
this distinction signifies only that different standards of liability
may be applied within the larger publisher category, depending on the
specific type of publisher concerned. See Keeton et al., supra,
Section(s) 113, at 799-800 (explaining that every party involved is
charged with publication, although degrees of legal responsibility
differ). To the extent that decisions like Stratton and Cubby utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. Stratton and Cubby do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeran seeks to impose liability on AOL for assuming the role for which Section(s) 230 specifically proscribes liability -- the publisher role.

Our view that Zeran's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeran's logic, AOL is legally at fault because it communicated to third parties an allegedly false statement. This is precisely the theory under which the original poster of the offensive messages would be found liable. If the original party is considered a publisher of the offensive messages, Zeran certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeran next contends that interpreting Section(s) 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part II A. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by Section(s) 230 of the CDA. Like the strict liability imposed by the Stratton Oakmont court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement -- from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgement concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Cf. Avil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot editorial judgment"). Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. See Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767, 777 (1986) (recognizing that fears of unjustified liability produce a chilling effect antithetical to First Amendment's protection of speech). Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible
lawsuits, service providers would likely eschew any attempts at selfregulation.

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Wheneve one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to Section(s) 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact.

Zeran finally contends that the interpretive canon favoring retention of common law principles unless Congress speaks directly to the issue counsels a restrictive reading of the Section(s) 230 immunity here. See United States v. Texas, 507 U.S. 529, 534 (1993). This interpretive canon does not persuade us to reach a different result. Here, Congress has indeed spoken directly to the issue by employing the legally significant term "publisher," which has traditionally encompassed distributors and original publishers alike.

The decision cited by Zeran, United States v. Texas, also recognized that abrogation of common law principles is appropriate when a contrary statutory purpose is evident. Id. This is consistent with the Court's earlier cautions against courts' application of the canon with excessive zeal: ""The rule that statutes in derogation of the common law are to be strictly construed does not require such an adherence to the letter as would defeat an obvious legislative purpose or lessen the scope plainly intended to be given to the measure."" Isbrandtsen Co. v. Johnson, 343 U.S. 779, 783 (1952) (quoting Jamison v. Encarnacion, 281 U.S. 635, 640 (1930)); cf. Astoria Fed. Sav. & Loan Ass'n v. Solimino, 501 U.S. 104, 110-11 (1991) (statute need not expressly delimit manner in which common law principle is abrogated). Zeran's argument flies in the face of this warning. As explained above, interpreting Section(s) 230 to leave distributor liability in effect would defeat the two primary purposes of the statute and would certainly "lessen the scope plainly intended" by Congress' use of the term "publisher."

Section 230 represents the approach of Congress to a problem of national and international dimension. The Supreme Court underscored this point in ACLU v. Reno, finding that the Internet allows "tens of millions of people to communicate with one another and to access vast amounts of information from around the world. [I]t is "a unique and wholly new medium of worldwide human communication." 117 S. Ct. at 2334 (citation omitted). Application of the canon invoked by Zeran here would significantly lessen Congress' power, derived from the Commerce Clause, to act in a field whose international character is apparent. While Congress allowed for the enforcement of "any State law that is consistent with [Section(s) 230]," 47 U.S.C. Section(s) 230(d)(3), it is equally plain that Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action. Section 230(d)(3) continues: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." With respect to federal-state preemption, the Court has advised: ""[W]hen Congress has `unmistakably . . .' ordained, that its enactments alone are to regulate a part of commerce, state laws regulating that aspect of commerce must fall. The result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose." Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977) (citations omitted). Here, Congress' command is explicitly stated. Its exercise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.
The CDA was signed into law and became effective on February 8, 1996. Zeran did not file his complaint until April 23, 1996. Zeran contends that even if Section(s) 230 does bar the type of claim he brings here, it cannot be applied retroactively to bar an action arising from AOL's alleged misconduct prior to the CDA's enactment. We disagree. Section 230 applies by its plain terms to complaints brought after the CDA became effective. As noted in Part IIB, the statute provides, in part: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." 47 U.S.C. Section(s) 230(d)(3).

Initially, it is doubtful that a retroactivity issue is even presented here. Retroactivity concerns arise when a statute applies to conduct predating its enactment. Section 230 does not directly regulate the activities of interactive computer service providers like AOL. Instead, Section(s) 230 is addressed only to the bringing of a cause of action. Here, Zeran did not file his complaint until over two months after Section(s) 230's immunity became effective. Thus, the statute's application in this litigation is in fact prospective. See St. Louis v. Texas Worker's Compensation Comm'n, 65 F.3d 43, 46 (5th Cir. 1995) (holding "issue is not technically one of retroactivity" when statute applies to "filing of the complaint"), cert. denied, 116 S. Ct. 2563 (1996); Vernon v. Cassadega Valley Central Sch. Dist., 49 F.3d 886, 889 (2d Cir. 1995) (same).

Even if this were a case implicating the application of a federal statute to pre-enactment events, the Supreme Court's Landgraf framework would nevertheless require Section(s) 230's application to Zeran's claims. Landgraf instructs us first "to determine whether Congress has expressly prescribed the statute's proper reach." Landgraf v. USI Film Pros., 511 U.S. 244, 280 (1994). This case can be resolved at this first step. In Section(s) 230(d)(3), Congress clearly expressed its intent that the statute apply to any complaint instituted after its effective date, regardless of when the relevant conduct giving rise to the claims occurred. Other circuits have interpreted similar statutory language to clearly express Congress' intent that the relevant statutes apply to bar new actions under statutorily specified conditions. See Wright v. Morris, 111 F.3d 414, 418 (6th Cir. 1997) (holding language "No action shall be brought . . .", 42 U.S.C. Section(s) 1997(a), to "expressly govern[] the bringing of new actions"), cert. denied, 1997 WL 275340 (U.S. Oct. 6, 1997); Abdul-Wadood v. Nathan, 91 F.3d 1023, 1025 (7th Cir. 1996) (holding language "In no event shall a prisoner bring a civil action or appeal a judgment . . .," 28 U.S.C. Section(s) 1915(g), to govern the bringing of new actions or filing of new appeals).

If we were to find a directive as plain as Section(s) 230(d)(3) to be ambiguous as to Congress' intent, we would be announcing a new superclear-statement condition for the retroactive operation of statutes. Such a jurisprudential shift would be both unwise and contrary to the Court's admonitions in Landgraf: "Retroactivity provisions often serve entirely benign and legitimate purposes, whether to respond to emergencies, to correct mistakes, to prevent circumvention of a new statute in the interval immediately preceding its passage, or simply to give comprehensive effect to a new law Congress considers salutary." 511 U.S. at 267-68. Here, Congress decided that free speech on the Internet and self-regulation of offensive speech were so important that Section(s) 230 should be given immediate, comprehensive effect.

There finally is a significant contrast between statutes that impose new liabilities for already-completed conduct and statutes that govern litigants' access to courts. For example, courts often apply intervening statutes that restrict a court's jurisdiction. See Landgraf, 511 U.S. at 274. Section 230 neither imposes any new liability on Zeran nor takes away any rights acquired under prior law. No person has a
vested right in a non-final tort judgment, much less an unfiled tort claim. Hammond v. United States, 786 F.2d 8, 12 (lst Cir. 1986).

Furthermore, Zeran cannot point to any action he took in reliance on the law prior to Section(s) 230's enactment. Because Section(s) 230 has no untoward retroactive effect, even the presumption against statutory retroactivity absent an express directive from Congress is of no help to Zeran here.

IV.

For the foregoing reasons, we affirm the judgement of the district court.

AFFIRMED

***** BEGIN FOOTNOTE(S) HERE *****

*fn1 Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

*fn2 Section 230 defines "interactive computer service" 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." 47 U.S.C. Section(s) 230(e)(2). The term "information content provider" is defined 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. Section(s) 230(e)(3). The parties do not dispute that AOL falls within the CDA's "interactive computer service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."

***** END FOOTNOTE(S) HERE *****

available in the print version]

Copyright 1997 VersusLaw, Inc., (425) 250-0142
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

Cyber Promotions Inc.
vs.
America Online Inc.
C.A. NO. 96-2486

------------------------

America Online Inc.
vs.
Cyber Promotions Inc.
C.A. NO. 96-5213

MEMORANDUM OPINION AND ORDER

Weiner, J.

November 4, 1996

These cases present the novel issue of whether, under the First Amendment to the United States Constitution, one private company has the unfettered right to send unsolicited e-mail advertisements to subscribers of another private online company over the Internet and whether the private online company has the right to block the e-mail advertisements from reaching its members. The question is important because while the Internet provides the opportunity to disseminate vast amounts of information, the Internet does not, at least at the present time, have any means to police the dissemination of that information. We therefore find that, in the absence of State action, the private online service has the right to prevent unsolicited e-mail solicitations from reaching its subscribers over the Internet.

The cases have their genesis in a letter dated January 26, 1996, in which American Online, Inc. ("AOL") advised Cyber Promotions, Inc. ("Cyber") that AOL was upset with Cyber's dissemination of unsolicited e-mail to AOL members over the Internet. AOL subsequently sent a number of "e-mail bombs" [1] to Cyber's Internet service providers ("ISP").

On March 26, 1996, Cyber filed Civil Action No. 96-2486 in this Court against AOL in response to AOL's "e-mail bombing" of Cyber's ISPs. The Complaint alleges that as a result of AOL's "e-mail bombing", two of Cyber's ISPs terminated their relationship with Cyber and a third ISP refused to enter into a contract with Cyber. The Complaint asserts a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030, as well as state law claims for intentional interference with contractual relations, tortious interference with prospective contractual relations and unfair competition. The Complaint seeks certain injunctive relief and damages.

On April 8, 1996, AOL filed a ten-count Complaint against Cyber in the United States District Court for
the Eastern District of Virginia, alleging service and trade name infringement, service mark and trade name dilution, false designation of origin, false advertising, unfair competition, violations of the Virginia Consumer Protection Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and the Virginia Computer Crimes Act. AOL seeks various injunctive relief and damages.

On May 8, 1996, Cyber filed a First Amended Complaint in Civil Action No. 96-2486 in which it asserted the same four claims it asserted in its original Complaint and added a declaratory judgment claim (Count V). Cyber seeks, inter alia, a "declaration that [it] has the right to send to AOL members via the Internet unsolicited e-mail advertisements." Amended Complaint at p. 21. Cyber also asks the Court to "permanently enjoin[] AOL ... from ... directly or indirectly preventing AOL members from receiving [Cyber's] e-mail messages." Id.

On June 17, 1996, AOL filed a First Amended Complaint in the Virginia action in which it added claims for misappropriation, conversion, and unjust enrichment.

By Order dated July 24, 1996, the judge in the Eastern District of Virginia to whom AOL's action was assigned, transferred that action to this Court, finding that it arises from "the same nucleus of operative facts" as Cyber's action and that therefore "the two cases should be consolidated for trial." Upon transfer to this Court, AOL's action was assigned Civil Action No. 96-5213. The parties have agreed that the First Amended Complaint in that action will be treated as setting forth AOL's counterclaims in Civil Action No. 96-2486.

AOL has vehemently argued throughout the brief history of these suits that Cyber has no right to send literally millions of e-mail messages each day to AOL's Internet servers free of charge and resulting in the overload of the e-mail servers. Indeed, the court has received a plethora of letters from disgruntled AOL members who object to having to receive Cyber's unsolicited e-mail whenever they sign on to AOL despite repeated attempts to be removed from Cyber's lists. Cyber, on the other hand, has contended that without the right to send unsolicited e-mail to AOL members, it will go out of business.

Recognizing that Cyber's contention that it has the right to send unsolicited e-mail to AOL members over the Internet implicates the First Amendment and therefore is a threshold issue, the Court directed the parties to brief the following issue: Whether Cyber has a right under the First Amendment of the United States Constitution to send unsolicited e-mail to AOL members via the Internet and concomitantly whether AOL has the right under the First Amendment to block the e-mail sent by Cyber from reaching AOL members over the Internet. In response, AOL has filed a document entitled "Motion for Partial Summary Judgment of America Online, Inc. on First Amendment issues." Specifically, AOL seeks summary judgment on Cyber's declaratory judgment claim asserted in Count V of Cyber's First Amended Complaint. Cyber has filed a document entitled "Plaintiff's Memorandum in Support of its First Amendment Right to Send Internet E-Mail to Defendant's Members."

The Court also directed the parties to enter into a Stipulation of Facts solely for the purpose of resolving the First Amendment issue. Pursuant to the Court's directive, the parties have stipulated to the following facts:

1. Cyber is a corporation organized and existing under the laws of the Commonwealth of Pennsylvania, having a place of business at 1255 Passmore Street, 1st Floor, Philadelphia, Pennsylvania 19111.

2. AOL is a corporation organized and existing under the laws of the State of Delaware with its principal place of business at 22000 AOL Way, Dulles, Virginia 20166.

3. AOL was and is a private online company that has invested substantial sums of its own money in equipment, name, software and reputation. AOL is not owned in whole or in part by the government.

4. AOL is owned by shareholders, and its stock trades on the New York Stock Exchange.
6. AOL's members or subscribers pay prescribed fees for use of AOL resources, access to AOL and access and use of AOL's e-mail system and its connection to the Internet.

7. AOL's e-mail system operates through dedicated computers known as servers, which consist of computer hardware and software purchased, maintained and owned by AOL. AOL's computer servers have a finite, though expandable, capacity to handle e-mail. All Internet e-mail from non-AOL members to AOL customers or members and from AOL customers or members to non-AOL members requires the use of AOL's computer hardware and software in combination with the hardware and software of the Internet and the hardware and software of the non-AOL members.

9. There has been no government involvement in AOL's business decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers.

10. Although the Internet is accessible to all persons with just a computer, a modem and a service provider, the constituent parts of the Internet (namely the computer hardware and software, servers, service providers and related items) are owned and managed by private entities and persons, corporations, educational institutions and government entities, who cooperate to allow their constituent parts to be interconnected by a vast network of phone lines.

11. In order for non-AOL members to send Internet e-mail to AOL members, non-AOL members must utilize a combination of their own hardware and software, the Internet and AOL's network.

12. To obtain its initial access to the Internet, AOL obtained an Internet address and domain name from IANA, a clearing house that routinely and ministerially assigns Internet addresses and domain names.

13. Cyber, an advertising agency incorporated in 1996, provides advertising services for companies and individuals wishing to advertise their products and services via e-mail.

14. Cyber sends its e-mail via the Internet to members of AOL, members of other commercial online services and other individuals with an Internet e-mail address.

15. AOL provides its subscribing members with one or more e-mail addresses so that members can exchange e-mail with one another and exchange e-mail (both sending and receiving) over the Internet with non-AOL members.

16. AOL has attached to its Memorandum of Law in Support of its Motion for Partial Summary Judgment on First Amendment Issues three sets of examples of e-mail messages sent by Cyber to AOL members. The first set (Tab 1) consists of a multi-page set of advertisements; the second set (Tab 2) consists of an exclusive or single-advertiser e-mail; and the third set (Tab 3) consists of a document called by Cyber an "e-mag." Under each tab are two examples, the first selected by AOL and the second selected by Cyber. The Court has reviewed all of the examples and notes that many of the ads include get-rich-quick ads, weight loss ads, health aid promises and even phone sex services.

17. To attract membership, AOL offers a variety of services, options, resources and support, including content-based services, access to stock quotes, children's entertainment, news, and the ability to send and receive Internet e-mail to and from non-AOL members.

In addition to the parties's Stipulation of Facts, it is necessary for resolution of the issue before us to relate some of the factual findings about the Internet itself made earlier this year by our court in American Civil Liberties Union v. Reno, 929 F.Supp. 824 (E.D. Pa. 1996). They are as follows:
18. "The Internet is ... a unique and wholly new medium of worldwide human communication." *Id.* at 844.

19. The Internet is "a giant network which interconnects innumerable smaller groups of linked computer networks." *Id.* at 830. In short, it is "a global Web of linked networks and computers ..." *Id.* at 831.

20. "The Internet is an international system." *Id.* It is "a decentralized, global medium of communications -- or 'cyberspace' -- that links people, institutions, corporations, and governments around the world. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information." *Id.*

21. "No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers)." *Id.* at 832.

22. Computer users have a wide variety of avenues by which to access the Internet. *Id.* One such avenue is "through one of the major national commercial 'online services' such as [AOL] ..." *Id.* at 833. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available *within* each online service, the services also allow subscribers to link to the much larger resources of the Internet." *Id.* (emphasis in original). "The major commercial online services have almost twelve million individual subscribers across the United States." *Id.* Approximately six million individuals are subscribers of AOL.

23. There are a number of different ways to communicate over the Internet. One such way "is via electronic mail, or 'e-mail', comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people." *Id.* at 834.

24."[T]he content on the Internet is as diverse as human thought." *Id.* at 842.

25. "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.'" *Id.* at 844.

26. Unlike a radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial." *Id.* at 845.

**STANDARD OF REVIEW**

Under Federal Rule of Civil Procedure 56(c), summary judgment may be granted when, "after considering the record evidence in the light most favorable to the non-moving party, no genuine issue of material fact exists and the moving party is entitled to judgment as a matter of law." *Turner v. Schering-Plough Corp.*, 901 F.2d 335, 340-41 (3d Cir. 1990). For a dispute to be "genuine," the evidence must be such that a reasonable jury could return a verdict for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986); *Williams v. Borough of Chester*, 891 F.2d 458, 460 (3d Cir. 1989). To establish a genuine issue of material fact, the non-moving party must introduce evidence beyond the mere pleadings to create an issue of material fact on "an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex v. Carrett*, 477 U.S. 317, 322 (1986). The burden of demonstrating the absence of genuine issues of material fact is initially on the moving party regardless of which party would have the burden of persuasion at trial. *First Nat'l Bank of Pennsylvania v. Lincoln Nat'l Life Ins.*, 824 F.2d 177, 180 (3d Cir. 1987). Following such a showing, the non-moving party must present evidence through affidavits or depositions and admissions.
on file which comprise of a showing sufficient to establish the existence of every element essential to that party's case. Celotex, 477 U.S. at 323. If that evidence is, however, "merely colorable" or is "not significantly probative," summary judgment may be granted. Equimark Commercial Finance Co. v. C.I.T. Financial Corp. 812 F.2d 141, 144 (3d Cir. 1987) (quoting, in part, Anderson, 477 U.S. at 242-50).

In view of the parties' Stipulation of Facts and the prior factual findings of this Court in ACLU v. Reno, supra., the Court finds there are no genuine issues of material fact as to the First Amendment issue and that that issue is suitable for summary disposition.

In its Motion for Partial Summary Judgment, AOL contends that Cyber has no First Amendment right to send unsolicited e-mail to AOL members over the Internet because AOL is not a state actor, AOL's e-mail servers are not public fora in which Cyber has a right to speak, Cyber's right to use AOL's, service free of charge, does not substantially outweigh AOL's right to speak or not to speak, and that AOL's restrictions on mass e-mail solicitations are tailored to serve a substantial interest. Motion for Partial Summary Judgment at 6. Because we find AOL is not a state actor and none of its activities constitute state action, we need not consider AOL's remaining First Amendment contentions.

The First Amendment to the United States Constitution states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press." The United States Supreme Court has recognized that "the constitutional guarantee of free speech is a guarantee only against abridgement by government, federal or state." Hudgens v. NLRB, 424 U.S. 507, 513 (1976). Only recently, the Supreme Court has stated that "the guarantees of free speech ... guard only against encroachment by the government and 'erect[ ] no shield against merely private conduct." Hurley v. Irish-American Gay Group of Boston, 115 S.Ct. 2338, 2344 (1995) (citation omitted).

In the case sub judice, the parties have stipulated that AOL is a private online company that is not owned in whole or part by the government. Stipulation of Facts at para. 3. (emphasis added). The parties have further stipulated that "AOL is not a government entity or political subdivision." Id. at para. 5. They have also stipulated that there has been no government involvement in AOL's business decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers. Id. at para. 9.

Despite these stipulations, Cyber argues that AOL's conduct has the character of state action. As a general matter, private action can only be considered state action when "there is a sufficiently close nexus between the State and the challenged action of [the private entity] so that the action of the latter may be fairly treated as that of the State itself." Blum v. Yaretsky, 457 U.S. 991, 1004 (1982). Recently, our Court of Appeals observed that the Supreme Court appears to utilize three distinct tests in determining whether there has been state action. Mark v. Borough of Hatboro, 51 F.3d 1137, 1142 (3d Cir. 1995). First, we must consider whether "the private entity has exercised powers that are traditionally the exclusive prerogative of the state." Id. (quoting Blum v. Yaretsky, 457 U.S. at 1004-05. (emphasis in Mark)). This test is known as the exclusive public function test. If the private entity does not exercise such powers, we must consider whether "the private entity has acted with the help of or in concert with state officials." Mark, 51 F.3d at 1142 (quoting McKeesport Hospital v. Accreditation Council for Graduate Medical Ed., 24 F.3d 519, 524 (3d Cir. 1994)). The final test is whether "the State has so far insinuated itself into a position of interdependence with ... the acting party that it must be recognized as a joint participant in the challenged activity." Mark, 51 F.3d at 1142 (quoting Krynick v. University of Pittsburgh, 742 F.2d 94, 98 (3d Cir. 1984)).

With regard to the first test, AOL exercises absolutely no powers which are in any way the prerogative, let alone the exclusive prerogative, of the State. In ACLU, supra., this Court previously found that no single entity, including the State, administers the Internet. ACLU, 929 F.Supp. at 832. Rather, the Court found that the Internet is a "global Web of linked networks and computers" which exists and functions as the result of the desire of hundreds of thousands of computer operators and networks to use common data transfer data protocol to exchange communications and information. Id. In addition, "the constituent parts of the Internet ... are owned and managed by private entities and persons, corporations,
educational institutions and government entities, who cooperate to allow their constituent parts to be interconnected by a vast network of phone lines." Stipulation of Facts at para. 10. As a result, tens of millions of people with access to the Internet can exchange information. AOL is merely one of many private online companies which allow its members access to the Internet through its e-mail system where they can exchange information with the general public. The State has absolutely no interest in, and does not regulate, this exchange of information between people, institutions, corporations and governments around the world.

Cyber argues, however, that "by providing Internet e-mail and acting as the sole conduit to its members' Internet e-mail boxes, AOL has opened up that part of its network and as such, has sufficiently devoted this domain for public use. This dedication of AOL's Internet e-mail accessway performs a public function in that it is open to the public, free of charge to any user, where public discourse, conversations and commercial transactions can and do take place." Cyber's Memorandum in Support of its First Amendment Right to Send Internet E-Mail to Defendant's Members at 13. Cyber therefore contends that AOL's Internet e-mail accessway is similar to the company town in *Marsh v. Alabama*, 326 U.S. 501 (1946), which the Supreme Court found performed a public function and therefore was a state actor.

In *Marsh*, a Jehovah's Witness was convicted of criminal trespass for distributing literature without a license on a sidewalk in a town owned by a private company. The Supreme Court found that since the private company owned the streets, sidewalks, and business block, paid the sheriff, privately owned and managed the sewage system, and owned the building where the United States post office was located, the company, in effect, operated as the municipal government of the town. *Marsh*, 326 U.S. at 502-03. "[T]he owner of the company town was performing the full spectrum of municipal powers and stood in the shoes of the State." *Lloyd Corp. v. Tanner*, 407 U.S. 551, 569 (1972). The Court observed that "[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it." *Marsh*, 326 U.S. at 506. As a result, the Court found state action in "the State[s] ... attempt[] to impose criminal punishment on appellant for undertaking to distribute religious literature in a company town ..." *Marsh*, 326 U.S. at 509. Our Court of Appeals has noted that "*Marsh* has been construed narrowly." *Cable Investments, Inc. v. Woolley*, 867 F.2d 151, 162 (3d Cir. 1989).[2]

By providing its members with access to the Internet through its e-mail system so that its members can exchange information with those members of the public who are also connected to the Internet, AOL is not exercising any of the municipal powers or public services traditionally exercised by the State as did the private company in *Marsh*. Although AOL has technically opened its e-mail system to the public by connecting with the Internet, AOL has not opened its property to the public by performing any municipal power or essential public service and, therefore, does not stand in the shoes of the State. *Marsh* is simply inapposite to the facts of the case *sub judice*.

Cyber also argues that AOL's Internet e-mail connection constitutes an exclusive public function because there are no alternative avenues of communication for Cyber to send its e-mail to AOL members. As support for this proposition, Cyber directs our attention to the decisions of the Supreme Court in *United States Postal Service v. Greenburgh Civic Assn's*, 453 U.S. 114 (1981); *Lloyd Corp v. Tanner*, 407 U.S. 551 (1972) and *Amalgamated Food Employees Union v. Logan Valley Plaza*, 391 U.S. 308 (1968). Of these decisions, only the *Lloyd* decision is helpful to Cyber.

In *Greenburgh*, a civic association challenged a federal statue which prohibited the deposit of unstamped "mailable matter" in a letterbox approved by the United States Postal Service. The civic association contended that the First Amendment guaranteed them the right to deposit, without postage, their notices, circulars, flyers in such letterboxes. The Supreme Court upheld the constitutionality of the statute, finding that neither the enactment nor the enforcement of the statute was geared in any way to the content of the message sought to be placed in the letterbox. The Court also noted that the statute did not prevent individuals from going door-to-door to distribute their message or restrict the civic organization's right to use the mails. *Greenburgh*, however, did not involve the issue of whether there was state action. It therefore is inapplicable to the issue of whether AOL's conduct constitutes state action.
In *Logan Valley*, a case involving peaceful picketing directed solely at one establishment within a shopping center, the Court reviewed the *Marsh* decision in detail, emphasized the similarities between a shopping center and a company town and concluded that a shopping center is the "functional equivalent" of the business district in *Marsh*. As a result, the Court held that the picketers had a First Amendment right to picket within a shopping center. *Logan Valley*, however, was subsequently overruled by *Lloyd*, *supra*. *Hudgens v. National Labor Relations Board*, 424 U.S. 507 (1976). ("[W]e make clear now, if it was not clear before, that the rationale of *Logan Valley* did not survive the Court's decision in the *Lloyd* case.")

In *Lloyd*, a group of individuals sought to distribute handbills in the interior of a privately owned shopping center. The content of the handbills was not directed at any one establishment in the shopping center but instead was directed at the Vietnam War. The Court noted that, unlike the situation in *Logan Valley* where the protestors had no other alternative to convey their message at the single establishment in the shopping center, the protestors in *Lloyd* could distribute their message about the Vietnam war on any public street, sidewalk or park outside the mall. The Court therefore found that "[i]t would be an unwarranted infringement of property rights to require [the protestors] to yield to the exercise of First Amendment under circumstances where adequate alternative avenues of communication exist." *Lloyd*, 407 U.S. at 567. The *Lloyd* Court went on to reject the individuals' functional equivalency argument, finding that the private shopping center neither assumed the full spectrum of municipal powers nor stood in the shoes of the state, as did the private company in *Marsh*. The Court held that, "[t]he First and Fourteenth Amendments safeguard the rights of free speech and assembly by limitations on state action, not on action by the owner of private property used nondiscriminatorily for private purposes only." *Lloyd*, 407 U.S. at 567 (emphasis in original).

Cyber has numerous alternative avenues of sending its advertising to AOL members. An example of another avenue Cyber has of sending its advertising to AOL members over the Internet is the World Wide Web which would allow access by Internet users, including AOL customers, who want to receive Cyber's e-mail. Examples of non-Internet avenues include the United States mail, telemarketing, television, cable, newspapers, magazines and even passing out leaflets. Of course, AOL's decision to block Cyber's e-mail from reaching AOL's members does not prevent Cyber from sending its e-mail advertisements to the members of competing commercial online services, including CompuServe, the Microsoft Network and Prodigy.

Having found that AOL is not a state actor under the exclusive public function test, we evaluate whether AOL is a state actor under the remaining two tests, i.e. whether AOL is acting with the help of or in concert with state officials and whether the State has put itself in a position of interdependence with AOL such that it must be considered a participant in AOL's conduct. These tests actually overlap one another.

In its Memorandum, Cyber does not specifically argue that AOL is acting in concert with state officials. Indeed, the two major cases from the Supreme Court which have found state action under this test are clearly distinguishable from the case *sub judice*. See, *Adickes v. S.H. Kress & Co.*, 398 U.S. 144 (1970) (finding a conspiracy between a private actor and a state official to engage in unlawful discrimination constituted action under color of law for purposes of 42 U.S.C. Section 1983); *Lugar v. Edmondson Oil Co.*, 457 U.S. 922 (1982) (finding private creditor's pre-judgment attachment petition upon which clerk of state court issued a writ of attachment and sheriff executed the writ on property of private debtor was state action under Section 1983).

Rather, Cyber relies on the "joint participation" doctrine and contends that "AOL's use of the Court to obtain injunctive relief and/or damages [which it seeks in its prayer for relief in its counterclaim] and its assertions of federal and state statutory law, which if applicable to Cyber's activities, would violate Cyber's First Amendment rights." Cyber's Memorandum at 15.

In *Edmondson v. Leesville Concrete Co.*, 500 U.S. 614 (1991) the Supreme Court refined the joint participation test by announcing that courts must ask "first whether the claimed constitutional deprivation resulted from the exercise of a right or privilege having its source in state authority; and second, whether the private party charged with the deprivation could be described in all fairness as a
state actor." *Edmonson*, 500 U.S. at 620. Under the first prong, the inquiry is "under what authority did the private person engage in the allegedly unlawful acts." *Mark*, 51 F.3d at 1144.

In the case *sub judice*, the parties have stipulated that "[t]here has been no government involvement in AOL's business decisions with respect to e-mail sent by Cyber nor in any AOL decision to institute or reinstitute a block directed to Internet e-mail sent by Cyber to AOL members or subscribers." Stipulation of Facts at para. 9. As a result, Cyber is unable to satisfy even the first prong of the joint participation test.

In addition, our Court of Appeals has stated that "[m]erely instituting a routine civil suit does not transform a litigant's actions into those taken under color of state law." *Tunstall v. Office of Judicial Support*, 820 F.2d 631, 634 (3d Cir. 1987). The *Tunstall* Court concluded that the filing of a quiet title action in state court by a purchaser of land to complete the seizure of plaintiff's property did not involve state action since the suit "did not attempt any seizure of property with the cooperation of state officials as in the *Lugar* line of cases." *Id.* In addition, the United States Court of Appeals for the Eleventh Circuit has found that a regulated utility did not act under color of state law when it obtained a temporary restraining order from a state court. *Cobb v. Georgia Power Co.*, 757 F.2d 1248 (11th Cir. 1985). The United States Court of Appeals for the Second Circuit has held that the mere filing of a state law contempt proceeding does not constitute joint participation so as to satisfy the color of state law requirement under 42 U.S.C. Section 1983. *Dahlberg v. Becker*, 748 F.2d 85 (2d Cir. 1984).

Perhaps recognizing the futility of its argument, Cyber contends in its Reply Memorandum that "[i]t is not Cyber's position that the mere filing of an action provides a party with the requisite state action to assert a First Amendment violation. Rather it is the Court's participation with the litigant in issuing or enforcing an order which impinges on another's First Amendment rights. *Grandbouche v. Clancey*, 825 F.2d 1463, 1466 (10th Cir. 1987)." *Reply Memorandum at 7.* In *Grandbouche*, the United States Court of Appeals for the Tenth Circuit stated that the First Amendment "may be applicable in the context of discovery orders, even if all of the litigants are private entities." The Court found government action present as a result of a magistrate's order compelling discovery and the trial court's enforcement of that order.

decision because it has the effect of creating government action every time a magis trate simply signs, and a trial judge enforces, a discovery order. Therefore, even if this Court had enforced a discovery order (which we have not), we would not follow the *Grandbouche* decision.

In sum, we find that since AOL is not a state actor and there has been no state action by AOL's activities under any of the three tests for state action enunciated by our Court of Appeals in *Mark*, Cyber has no right under the First Amendment to the United States Constitution to send unsolicited e-mail to AOL's members. It follows that AOL, as a private company, may block any attempts by Cyber to do so.

Cyber also contends that its practice of sending e-mail advertisements to AOL's servers is also protected "under state constitutional law, which in many instances, affords even broader protection than federal First Amendment guarantees which this Court can enforce." Cyber's Memorandum at 17. Specifically, Cyber refers to the state constitutions of Pennsylvania and Virginia.[3] Although this argument is beyond the scope of the issue the Court directed the parties to brief, we will nevertheless consider it at this time.

The theory that a state constitution's free speech provisions may afford broader rights than similar provisions of the United States Constitution was first recognized by the Supreme Court in *PruneYard Shopping Center v. Robins*, 447 U.S. 74 (1980). The *PruneYard* Court held that, while the First Amendment did not grant the defendants the right to solicit in a privately owned shopping center, state (California) law might grant that right. The Supreme Court of Pennsylvania has itself recognized that "Pennsylvania may afford greater protection to individual rights under its Constitution" than the Constitution of the United States. *Western Pennsylvania Socialist Workers 1982 Campaign v. Conn.Gen.Life Ins.Co.*, 515 A.2d 1331, 1333-34 (1986) (plurality opinion); *Commonwealth v. Tate*, 432 A.2d 1382 (1981).
Article 1, Section 7 of the Pennsylvania Constitution provides:

The free communication of thoughts and opinions is one of the invaluable rights of man, and every citizen may freely speak, write and print on any subject ...

In *Tate*, the only case on which Cyber relies, the Supreme Court of Pennsylvania overturned convictions for defiant trespass stemming from a group of protestor's refusal to desist from distributing politically oriented materials in a peaceful manner on the campus of a privately owned college. The court found that the college had created a public forum by opening the campus to the public to hear the director of the FBI to speak in a campus building. Because the college had become a public forum and because the defiant trespass statute had provided a defense to a charge of defiant trespass in those circumstances [4], the *Tate* Court held that the protestors had a right to speak freely without fear of criminal conviction under Article 1, Section 7 of the Pennsylvania Constitution.

was subsequently clarified by the Supreme Court of Pennsylvania in *Western Pennsylvania Socialist Workers*, *supra*. In that case, a political committee, its chairman, a gubernatorial candidate and a campaign worker claimed they had the right under, *inter alia*, Article 1, Section 7 of the Pennsylvania Constitution to collect signatures for the gubernatorial candidate's campaign at privately owned shopping malls, including one owned by Connecticut General Life Insurance Co. Connecticut General had a policy which uniformly prohibited all political activities including solicitation at its mall. The Court distinguished *Tate*, by observing that "[b]y adhering to a strict no political solicitation policy, [Connecticut General] has uniformly and generally prevented the mall from becoming a public forum." *Western Pennsylvania*, 515 A.2d at 1337. Rather, the Court noted that Connecticut General had only invited the public into the mall for commercial purposes. Since Connecticut General had not invited the public into the mall for political purposes, the Court held that Article 1, Section 7, was inapplicable.

The *Western Pennsylvania* Court also rejected attempts to analogize the mall to the company town in *Marsh v. Alabama*, *supra* by stating:

A shopping mall is not equivalent to a town. Though it duplicates the commercial function traditionally associated with a town's business district or marketplace, the similarity ends there. People do not live in shopping malls. Malls do not provide essential public services such as water, sewers roads, sanitation or vital records, nor are they responsible for education, recreation or transportation. Thus, the *Marsh* analysis is not applicable to the instant case.

The case *sub judice* is more similar to *Western Pennsylvania* than it is to *Tate*. AOL's e-mail servers are not a traditional public forum such as a street, park or even the college in *Tate*. Instead, AOL's e-mail servers are privately owned and are only available to the subscribers of AOL who pay a fee for their usage. Moreover, unlike *Tate*, AOL has not presented its e-mail servers to the public at large for disseminating political messages at a certain event. Indeed, AOL has never presented its e-mail servers to the public at large for dissemination of messages in general as AOL's servers have a finite capacity. *Stipulation of Facts at para. 7*. As noted above, AOL's e-mail system simply provides a means for its members to communicate with those members of the public who are connected with the Internet.

Cyber also does not have the right under the Constitution of Virginia to send unsolicited e-mail over the Internet to AOL members. Article I, Section 12 of the Virginia Constitution provides:

That the freedoms of speech and of the press are among the great bulwarks of liberty, and can never be restrained except by despotic governments; that any citizen may freely speak, write, and publish his sentiments on all subjects, being responsible for the abuse of that right; that the General Assembly shall not pass any law abridging the freedom of speech or of the press, nor the right of the people peaceably to assemble, and to petition the government for the redress of grievances.

There are no decisions which interpret this provision in a manner which would be helpful to Cyber. The decisions Cyber cites, *National Capital Naturists, Inc. v. Board of Supervisors*, 878 F.2d 128, 133 (4th
Cir. 1989); Leachman v. Rector & Visitors of the Univ. of Virginia, 691 F.Supp. 961, 964 n.5 (W.D.Va. 1988), aff'd, 915 F.2d 1564 (4th Cir. 1990); Robert v. Norfolk, 188 Va. 413, 49 S.E.2d 697, 700 (1948) all merely recognize the principle enunciated by the Supreme Court in Prune Yard that states have the "sovereign right" to give their constitutions an expansive interpretation.

Although we have found that Cyber has no right under the First Amendment of the United States Constitution or under the Constitutions of Pennsylvania or Virginia to send unsolicited e-mail to members of AOL, we will not, at this time, enter judgment on Count V of Cyber's First Amended Complaint for declaratory relief. This is because Cyber contends in its Reply brief that "many more issues ... have to be addressed since there are numerous reasons beyond the First Amendment which will permit Cyber to send e-mail to AOL members." Cyber's Reply Memorandum at 1. Therefore, we will simply declare that Cyber has no right under the First Amendment to the United States Constitution or under the Constitutions of Pennsylvania or Virginia to send unsolicited e-mail over the Internet to members of AOL. We will allow Cyber ten days from the date of this Memorandum Opinion and Order to submit a list of the theories other than the First Amendment it believes entitles it to send unsolicited e-mail to members of AOL.

An Order to that effect follows.

FOOTNOTES

1. In past submissions, Cyber has stated that AOL's "e-mail bombs" occurred when AOL gathered all unsolicited e-mail sent by Cyber to undeliverable AOL addresses, altered the return path of such e-mail, and then sent the altered e-mail in a bulk transmission to Cyber's ISPs in order to disable the ISPs.

2. Indeed, our Court of Appeals has observed that the exclusive public function test itself "rarely could be satisfied." Mark, 51 F.3d at 1142. "Thus, in Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974), the Court held that a private utility company, extensively regulated by the state, and apparently holding at least a partial monopoly in its territory, did not act under color of state law, in part because the state where the utility was engaged in business had 'rejected the contention that the furnishing of utility services is either a state function or a municipal duty.' (citation omitted). Similarly, in Rendell-Baker v. Kohn, 457 U.S. 830 (1982), the Court held that a private entity engaged in the education of maladjusted high school students did not perform an exclusively public function because '[the state's] legislative policy choice [to fund the public school] in no way makes these services the exclusive province of the State.' (citation omitted); see also Black v. Indiana Area Sch. Dist., 985 F.2d 707, 710-11 (3d Cir. 1993) (private contractor providing state school bus program at state expense not performing exclusive state function)." Mark, id.

3. Cyber contends it is entitled to the protection of the Pennsylvania Constitution because Cyber's e-mail originates from Pennsylvania and that it is entitled to the protection of the Virginia Constitution because AOL's blocking actions occur in Virginia.


It is a defense to prosecution under this section that: the premises were at the time open to members of the public and the actor complied with all lawful conditions imposed on access to or remaining on the premises.

© 1997 The Bureau of National Affairs Inc., All Rights Reserved
UNIVERSITY OF SAN FRANCISCO

SCHOOL OF LAW

Final Examination
Cyberspace Law
Spring 1996

Eric Schlachter
May 14, 1996
6:30 to 9:00

Instructions--PLEASE READ CAREFULLY

1. This is an open book exam. All written and printed materials are permitted.

2. This is a multiple part exam with a total time limit of 2½ hours. There are a total of three questions, with the following approximate weighting for each question:

   Question 1: 40% (approximately 1 hour)
   Question 2: 40% (approximately 1 hour)
   Question 3: 20% (approximately ½ hour)

3. Enter your exam number in the space provided above.

4. Please write your exam in blue books or type your exam on paper provided.

5. I have the following exam tips and strategies for you:

   a. Please outline your answers carefully and deliberately. I recommend that you spend approximately ¼ of your allocated time reading the question and outlining a response.

   b. Follow the call of the question. Target your response to your audience.

   c. While generally your questions should be based on legal principles, it is always appropriate to address business issues.

   d. You are likely to find that additional information would be useful in your analysis. Please indicate what additional information would be helpful, and then make assumptions to proceed with your analysis.

6. ALL EXAM QUESTIONS MUST BE TURNED IN AT THE END OF THE EXAMINATION.
Question 1 (1 hour)

Susan James runs a 12 phone line BBS called "The Black Hole." The Black Hole is a general interest BBS, providing such functionality to users as Internet access, message boards, online games, and a software file exchange area.

Susan has decided to retain you as the attorney for the Black Hole. At your initial consultation with her, the following exchange takes place:

You: "Tell me how you run your software file exchange."
SJ: "We have divided the software file exchange into 4 main areas: Windows, Mac, DOS and GIFs [GIFs are graphics files, such as computer art or digitized photos]. Within each area, the file exchanges are divided into categories, such as games, utilities, error corrections and patch releases, communications, word processing, spreadsheet programs, and so on. The GIFs are classified by subject matter of the file. Users who want to download software or files are free to do so with no limits."
You: "Tell me about the upload process."
SJ: "Users upload files or software to a separate server where the computer automatically runs a program to check if there are any viruses contained in the software. [A virus is deleterious code embedded in a software program.] If the virus checker does not find any viruses in the software, it is automatically uploaded to our public space within 2-4 hours after initial posting. If viruses are found in the software, the software is rejected."
You: "Do you ever get pirated commercial software posted?"
SJ: "Occasionally, and when I see it, I remove it as quickly as possible."
You: "How does software get categorized, so that (for example) a Mac word processing program gets put into the right area?"
SJ: "In the uploading process, the users identify where the software should go. Most of the time, the software is properly categorized. However, sometimes we get some bozos who deliberately misclassify their stuff, in which case we usually move it to the proper category."

Later in the conversation, Susan indicates that she has been receiving complaints about a GIF file that has been uploaded to the GIF area. The GIF contains an image that, in its caption, asserts that the person who is the subject matter of the cartoon has a sexually transmitted disease. Apparently, the subject person called Susan to complain about the file. Susan is thinking about removing the file but is unsure what to do. What do you tell her to do?

END OF QUESTION 1
Question 2 (1 hour)

Soundtouch, Ltd. is a new client of yours. Soundtouch has developed a unique database of "Soundbytes." Over the years, Soundtouch has received promotional CDs from record producers and studios. Soundtouch has selected the "best" (in Soundtouch’s judgment) 30-45 seconds of each song on the CDs and digitized that portion into a computer-readable file. All these "bites" of songs have been indexed and put into a database that now numbers 50,000 bites. Soundtouch has never entered into any license agreement with record companies or artists regarding the creation or use of Soundbytes. Soundtouch also has developed some database management software to search for and retrieve Soundbytes.

A licensee named Javelin has approached Soundtouch requesting a 1 year license to the Soundbytes database and database management software. Javelin desires to set up a storefront to sell music CDs on the Web and will use the Soundbytes database to provide potential customers with the real time ability to play "samples" of the songs on CDs prior to purchase. Javelin wants a complete copy of the Soundbytes database to run on Javelin’s Web server. In addition to license rights which properly allow Javelin to use the Soundbytes database on the Web, the license agreement will permit Javelin to make modifications to and derivative works of the Soundbytes database, and Javelin will own all such modifications and derivative works. [Remember the general rule that the owner of a derivative work requires a license to the underlying copyrighted work in order to exercise copyright rights in the derivative work.]

1. Soundtouch has indicated that it believes its use of the Soundbytes is "fair use." Do you have any problems with Soundtouch using "fair use" to build its Soundbytes database?

2. What do you think about the Javelin license? Are there any problems with it as currently structured? Some issues to think about include: exactly what rights are being licensed by Soundtouch and what happens to the database and its derivative works after termination? Are there alternative ways (technological or contractual) to accomplish the parties’ intent and protect Soundtouch better?

[Do not discuss any copyrights in music that we did not discuss in class (i.e., synchronization, mechanical, master recording)].

END OF QUESTION 2
Question 3 (½ hour)

George Yee, a software licensing partner in your firm, calls you about his client Online Motion. Online Motion has executed a letter of intent with High Rollers LLC with the following terms:

- Online Motion will develop slot machine software. The software will allow web browsers to play the slot machine software over the Web. Online Motion will develop the software to High Roller’s specifications and High Roller will run the software on its server as part of High Roller’s cybercasino.
- Online Motion will assign all right, title and interest in and to the software to High Rollers.
- High Rollers will pay $200,000 to Online Motion for development costs, plus 3% of all net revenues generated from players’ use of the software for a period of 10 years.
- High Rollers will indemnify and hold Online Motion harmless from all claims by players for any actual or alleged gaming losses and for any governmental legal action which may be filed against High Rollers or Online Motion as a result of the software.

Because George does not have much experience with the Internet, he calls to get your general thoughts about the transaction. Do you have any questions for George? What do you tell George?

[Do not discuss any copyright issues]

END OF QUESTION 3

END OF EXAMINATION
"SAMPLE" ANSWER
USF School of Law/Cyberspace Law/Spring 1996
Professor Eric Schlachter (eschlach@netcom.com)

This document discusses some of the points I was looking for in my Spring 1996 exam. There were many paths to success, although most of the best answers addressed these points at least in passing. In general, I was very pleased with your performance on the exam and I felt that most of you identified and properly weighted the issues of each question. In terms of grading, there were 11 As, 18 Bs and 3 Cs.

Question 1
Most of you correctly identified this question as pertaining to sysop liability for defamation. Those of you who treated this question primarily as a copyright question missed the call of the question. I would have organized an answer as follows:

1. Is the file actually defamatory? Defamation is a defamatory statement that is published and injurious to reputation. Imputing a sexually transmitted disease to a person is defamatory per se, is published (in the defamation sense) at least to the sysop and to any others who downloaded the file, and would tend to be injurious to reputation. Some additional information would have been helpful on this point:
   * was it true? (absolute defense to defamation action)
   * was it a matter of public concern? (doubtful but possible)
   * was it about a public figure? (recognizing that the public figure definition might stretch in online communities)
   * was it a parody? was it an assertion of opinion rather than fact?
If the BBS can show that there is no defamation action, no further action would be required.

2. Is the BBS a publisher as a matter of law? If the BBS is a publisher, then the BBS is probably already liable and the best it can do is mitigate damages. If the BBS is a distributor, then the law of republication applies and the BBS will be liable as a republisher if it knows or should have known that the file was defamatory and does not remove the file within a reasonable period of time. To determine whether the BBS was a publisher as a matter of law, the facts should have been compared to the facts in the Stratton Oakmont and Cubby cases.
   * The fact that the BBS deployed an automatic virus check was meant to hearken back to the dumb word filters deployed by Prodigy. Note that unlike a word filter, a virus checker is almost an absolute necessity for the proper functioning of a file exchange, and I personally would consider a BBS negligent if it failed to deploy a virus checker.
   * The removal of pirated software is not really editorial control (see below), although it does hint at the "damned if you do, damned if you don't" problem of sysop maintenance.
   * The moving of files by category is the most problematic and the most like editorial control in my mind. Personally, I would like to have known if this review and moving was ad hoc or part of a systematic plan.
As you might expect, the decision could go either way. Personally, I think that Susan's behavior should not make the BBS into a publisher as a matter of law, but then again I disagree with the result in Stratton Oakmont.

One point to consider: all of Susan's behavior applied to the software exchange and not the GIF area. Could Susan argue that the GIF area was unfiltered but abutted the filtered area of the software exchange?

3. Even if the BBS was a distributor, now that the BBS had "knowledge" that the file may be defamatory, the BBS must promptly remove the file to avoid liability as a republisher. Other useful actions would be to offer a "retraction" or to encourage the person to exercise their own right of reply.

Many of you rightly pointed out that removal of the file here would create future evidence that the BBS was a publisher as a matter of law. I believe, however, that this should not be the state of the law and I would cite the court's analysis in the Netcom case for the proposition that removal of liability-creating material does not otherwise indicate the exercise of control. More to the point, although we did not discuss this in class, the CDA may offer some hope here--Section 230(c)(1) says "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The legislative history (such that it is) indicates that this provision was inserted to overturn the result in Stratton Oakmont. Until I get more definitive analysis, I am not prepared to rely on this provision globally, but all of you should consider this language if the issue arises.

4. Other issues worth a quick mention were invasion of privacy (which we did not really discuss in class but could definitely be implicated by the file), obscenity (a stretch), CDA/indecent material (possible although we did not get into too many parameters of a CDA action) and copyright (is Susan in danger of a copyright action generally?).

5. Some common mistakes:
   * many of you tried to apply to copyright analytical structure to the "republisher" situation. Although they are analogous, the bodies of law are completely different.
   * a number of you thought disclaimers might help here. In addition to the difficulties of properly forming binding disclaimers, these will only be effective as between the parties involved and not third parties. A user agreement could have an indemnity clause in it, where the user indemnifies the BBS for the tortious posting, but this is unlikely in practice to amount to much.
   * Finally, a few of you suggested that Susan close down the file exchange altogether. This advice is aggressive given the call of the question and a very conservative approach from a legal standpoint.

Question 2
As I indicated, Question 2 is a real life story. Indeed, the story was even worse, in that Soundtouch was truly knocking on the door to bankruptcy and Javelin was a key creditor that gave Soundtouch an option: either enter into the license agreement or Javelin would throw Soundtouch into bankruptcy the very next day (which was a real threat). I was completely new
to the client when I was given the Javelin license (and knew nothing about how Soundtouch had developed its IP) and given less than 24 hours to develop a response. If I was too aggressive, Javelin would charge Soundtouch with not being serious about the negotiations and file the bankruptcy paperwork. If I was too soft, Soundtouch would blow all of its assets by entering the license and have nothing left for its stakeholders and stockholders. Ah, the joys of being a lawyer. Fortunately (at least for my malpractice insurer), Soundtouch decided to nix the license for other reasons and is plodding along in bankruptcy as we speak (after stiffing our firm for $60k...).

In part I, I really only intended you to discuss whether Soundtouch’s use is fair use. In the question, Soundtouch freely admitted that it infringed the CDs to build its database, so there was little danger by Soundtouch conceding infringement and arguing fair use. I should note that multiple 106 rights were implicated—reproduction, distribution, derivative works and public performance/digital performance (some of you improperly asserted only one or two of the rights were implicated). The fair use factors:

* Commercial v. educational/nonprofit use. This use tends to look like commercial use, although the courts have said that this factor is not a per se presumption against use by for-profit companies. This factor weighs against Soundtouch.

* Fact/fiction and published/unpublished. Many of you misapplied this factor, but it’s a stupid one anyway. Songs are published (more like fair use) but are fiction (less like fair use). This factor is a toss-up.

* Amount and substantiality of the use. Soundtouch used 30-45 seconds of 3-5 minute long songs, or 10-25%. However, because Soundtouch took the “best” portions of the long, the substantiality rises. Personally, I believe this factor weighs against Soundtouch.

* Effect on the market. This is the most important factor and also the toughest. Soundtouch believed that the database would actually promote the sale of CDs and therefore increase the market. However, the relevant market may be the market for soundbytes, not the downstream market for songs. Further, some courts misapply the factor by making it tautological—if someone thinks the IP is important enough to use, they must value it and would have been willing to pay for it. Finally, and most importantly, there are licensing schemes for music, even portions of songs, so the court would have little problem quantifying how much the use was costing the copyright holders. Just ask any movie or TV producers how often they rely on fair use for even snippets of songs they use in their productions.

Clearly, I believe fair use is precarious at best. Most importantly, if the fair use argument actually works, any attempts to license the database are extremely difficult (see below).

Some of you mentioned that the record companies had to be aware of this scheme and their failure to act presumably could be construed as some sort of implied license. This argument is not a bad one, but if even a few of the soundbytes turned out to be infringing, Soundtouch would still be on the hook for huge dollars. Again, not the best way to build your key corporate asset.

Part II was really a difficult question and I was impressed how many of you got at least to the right issue. Some of you even shocked me by coming up with the answer I was looking for, which I thought might be so obscure as to be impossible.
If Soundtouch’s use was not fair use, clearly the license is a huge problem since Soundtouch would be liable for direct infringement (reproduction/distribution to Javelin) and contributory infringement for Javelin’s use. Javelin did ask for an indemnity from Soundtouch, but query how useful that indemnity was given that Soundtouch was sounding its death knell. Some of you tried to get Javelin to indemnify Soundtouch for infringement--nice try, but in context extremely unlikely.

Some of you suggested that Soundtouch procure the appropriate licenses. This is a good suggestion except that administratively the cost would be huge. Alternatively, Soundtouch could pay statutory fees to BMI/ASCAP, but query if these statutory fees make sense given the Net economics (i.e., will Soundtouch have to pay for every download of a promotional clip?).

If Soundtouch’s use was fair use, then Soundtouch’s intellectual property was actually quite thin. It clearly had good intellectual property in the software, but the database starts to look like the databases in Feist and ProCD--chunks of data which the possessor could not copyright but which had some selection/coordination/arrangement aspects that created a thin compilation copyright. As many of you properly deduced, giving Javelin the right to make derivative works which Javelin owned meant that Javelin would be able to quickly evade the scope of the license by modifying the database. Even though the general rule is that a derivative work may not be used without a license to the underlying work, Javelin could avoid using the copyrighted portion of the “underlying work” without much effort and then would have complete ownership of the resulting product. At that point, the license is meaningless and Soundtouch has to compete with Javelin.

Many of you suggested that Javelin should assign ownership of the derivative works back to Soundtouch. In addition to being a change in the parties’ intent (watch the call of the question!), query whether this works--is a modification to a largely uncopyrighted work a “derivative work”? The same analysis applies to the suggestion that Soundtouch not permit Javelin to make derivative works. In other words, I believe Javelin’s mere possession of a database built on fair use would create an unstable situation.

Many of you tried to get control over the database by relying on Soundtouch’s copyright in the software. For exam purposes, this was clear thinking; however, in practice, the software was rather simple and it would have been an easy task for Javelin to develop its own software.

A number of you tried to trot out a laundry list of technologies from my lecture on technology supplements to copyright. This was OK but many of the technologies simply did not apply.

The clear winning answer was for Soundtouch to keep the database on its server and allow Javelin customers to access the database via Javelin-specific hypertext links over the Net--in other words, converting the license agreement into a database access agreement. This way, Soundtouch never has to part with a complete copy of the database and yet could provide Javelin and its customers with all the benefits of possessing the database.
Question 3

Question 3 is also a true story. Since this was not really my client, I do not know if the deal was ever consummated (but I hope not!). Ironically, when I pointed out to George that gambling on the Net was presumptively illegal, his initial response was “well, then we really need to make sure that we get some good warranties and indemnities...”! Also, High Rollers was represented by a large and generally reputable Palo Alto firm (let’s call it “Billsome Obscenely”), which led George to believe that surely Billsome must have done some due diligence about gambling on the Net as part of representing High Rollers. As I stressed in class, this kind of thinking can create all kinds of problems, especially since I later discovered that Billsome had only been representing High Rollers for only 1 week and the attorney working on the account was a general corporate lawyer more known for his biotech practice... In this situation, I for one would not bet my client’s personal freedom on Billsome’s analysis.

Some questions worth asking:

* Was High Rollers going to use the software for gambling or just for play/fun? If it is the latter, there may not be that many legal issues--but then again, why the heavy indemnity and the 3% royalty...?
* Did High Rollers have a scheme to ensure that only gamblers who could legally gamble on the site would have access? This would make me more comfortable if true, but I would be very suspicious that this could be implemented at a reasonable cost. Note that disclaimers (even those purporting to “deny” access to people who are not entitled to access under their local laws) are very likely to be insufficient to prevent criminal liability, and those of you who recommended this approach should reconsider the validity of this recommendation.
* Where were High Rollers and Online Motion located? If both are located outside of the reach of any extradition efforts, maybe my attitude would change. However, remember that it is generally against professional ethics to advise your clients to break the law.

As almost all of you reasoned, gambling on the Net creates sticky legal problems. In addition to federal laws that probably prohibit gambling on the Net, states (including but not limited to Minnesota) have laws that prohibit gambling by their residents. Even advertising about gambling is restricted. In other words, successfully implementing online gambling requires extreme caution--if it even can be done at all.

As many of you pointed out, our client is not engaging in gambling on the Net but providing a tool or device for gambling. You should note that gambling devices are extremely regulated even in Nevada (basically to ensure that they are fair to the gambler). In any event, many of you properly noted the potential liability as an aider or abetter or accomplice and perhaps co-conspirator (those of you who used “vicarious” or “contributory” liability were on the right point but again were using copyright language). In addition to generally participating in the scheme, note that Online Motion was designing the device to High Roller’s specifications and participating in the profits over time (the 3% royalty). Therefore, if High Rollers is breaking the law, Online Motion is likely to go down with it.

Most of you also pointed out that the indemnity is worthless. First, there is no meaningful indemnity for jail time. Second, it is probably void against public policy to indemnify for
criminal fines. Finally, High Rollers is unlikely to be around long enough to provide a meaningful indemnity.

Many of you talked about venue. You may recall that criminal venue can attach wherever the crime is committed; hence, Minnesota will prosecute people who violate Minnesota law in Minnesota courts so long as they can extradite. A lot of you talked about civil procedure and personal jurisdiction limits under the constitution, which was fine but not the major issue.

A number of you recommended that Online Motion "sell" the software or otherwise convert the fee into a one-time payment. Although this is generally not bad advice given the precariousness of the future cash flows, I do not believe this advice minimizes the likelihood that Online Motion would be liable criminally (particularly since a gambling device is subject to its own set of regulation). It reminds me of the cases in criminal law where the vendor sells a gun to someone knowing of their criminal intent--the vendor can still be criminally liable for aiding and abetting in such circumstances.
THESE EXAMINATION QUESTIONS MUST BE RETURNED AT THE END OF THE EXAMINATION.

SANTA CLARA UNIVERSITY
SCHOOL OF LAW

FINAL EXAMINATION

57931 Cyberspace Law
Professor Eric Schlachter
3 Questions

May 3, 1997
Spring Semester
1:30 to 4:00

THE EXAMINATION RULES AS STATED IN THE CURRENT STUDENT HANDBOOK GOVERN THIS EXAMINATION, EXCEPT THAT THIS IS AN OPEN BOOK EXAM.

Instructions—PLEASE READ CAREFULLY

1. This is an open book exam. All written and printed materials are permitted.

2. This is a multiple part exam with a total time limit of 2 hours, 30 minutes. There are a total of three questions, with the following weighting for each question:

   Question 1: 50% (1 hour, 15 minutes)
   Question 2: 30% (45 minutes)
   Question 3: 20% (30 minutes)

3. Enter your student identification number in the space provided above.

4. Please write or type your exam on paper provided.

5. I have the following exam tips and strategies for you:

   (a) Please outline your answers carefully and deliberately. I recommend that you spend approximately 1/3 of your allocated time reading the question and outlining a response.

   (b) Follow the call of the question. Target your response to your audience.

   (c) While generally your answers should be based on legal principles, it is always appropriate to address business issues.

   (d) You are likely to find that additional information would be useful in your analysis. Please indicate what additional information would be helpful, and then make assumptions to proceed with your analysis.
Question 1 (1 hour, 15 minutes)

Andrew Canyoudo, a partner in your firm, has forwarded to you the following email from one of his clients, Mike Saber:

Andrew, I need your help! I and my company have been repeatedly and viciously attacked by Lew Wort on a message board located at http://www.smallinvestor.com. I have complained to the sysop and still no action!!! This is unacceptable. Andrew, please resolve this matter.

Andrew explains to you that Andrew has recently represented Mike’s company, Crumb Corp., in its negotiations with BoBo Corp. BoBo recently announced that it was acquiring Crumb Corp. in a merger. Andrew explains that we now represent Mike individually [note: assume any necessary conflict waivers have been obtained].

Attached to Mike’s email is the text of four messages posted by Lew Wort in the “BoBo Forum” at smallinvestor.com, an active message forum for the discussion of BoBo’s business. In the header for all four messages, it says that the postings were made from 98765.4321@compuserve.com [note: assume the address is consistent with CompuServe’s address scheme]:

Message 172: Why did Crumb Corp. sell to BoBo instead of going public? Because if Crumb Corp. had gone public, everyone would have seen what a fraud the company is. Mike Saber is an infamous crook.

Message 178: It’s time to sell BoBo stock. Now! By some crooked means Saber was able to peddle his miserable creation to BoBo. All the insiders are selling as a result.

Message 179: How do I know Saber is a crook? I had many friends who worked with him in Estonistan. As you know, all Estonians are very unethical as a race. But my friends say Saber tops them all.

Message 182: Jeff, thanks for your message. I’ll see you at the COMDEX conference. And if you see Saber at the conference, tell him to watch his step. I’ll be there with a couple of tough guys from our security department.

When you go to look at the smallinvestor.com site, you cannot find messages 172, 179 or 182, but message 178 is still publicly available in the BoBo forum.

What do you do to “resolve the matter”? Please outline a list of the actions you plan to take and what you hope to accomplish by doing so. If you plan to communicate with a party, please outline their legal rights and obligations and indicate how you would might use the legal context to effectuate your goals.

END OF QUESTION 1
Question 2 (45 minutes)

Your client Foreignews is launching an advertising-supported website oriented towards U.S. executives doing business in South America. Among the features your client plans to offer is a What's New area. This area will be composed of articles published by English language periodicals in the various countries in South America. Once every 12 hours, Foreignews' robot will go to each periodical's website, make a copy of their articles, and automatically upload the articles to Foreignews' website. Foreignews has decided to do this rather than just hypertext link to the articles because, by putting the articles on a server located in the U.S., Foreignews' users will not have to wait for the articles to be sent over the Internet from South America.

Your client has scheduled a conference call to discuss the advisability of launching this feature. Please prepare an outline of the points you would like to cover in the call and provide some brief analysis of why each point is an issue.

[Ignore all international copyright treaties and conflicts of laws issues; assume that the copyright laws of all foreign jurisdictions are identical to U.S. copyright law. Do not discuss any issues related to INS v. AP, NBA v. Motorola or the "hot news" misappropriation tort. While copyright is an important part of this question, there are other issues to address.]

END OF QUESTION 2
Question 3 (30 minutes)

You are approached by a potential client, crapsgambling.com. They intend to launch a gambling website, where users can play online craps, blackjack, roulette and other games of chance “against the house” for real money. The entrepreneurs are aware that there may be issues involved with the legality of what they intend to do. Therefore, their first order of business when they hire a law firm will be to prepare a user “agreement” that users will be required to accept. As far as you can tell, they expect to use this agreement to protect themselves from all legal issues.

Please briefly describe the reasons why the user agreement may not adequately protect their interests.

[Although to some degree this question requires you to identify ways in which crapsgambling.com and its principals might be liable, the focus is on how the user agreement can or cannot deal with such liability and why.]

END OF QUESTION 3

END OF EXAMINATION
This document describes some of the points that I was looking for in this year's exam answers. There was no "right" answer to the questions, and I saw many high scoring answers that took alternative paths to success. I gave 13 As, 23 Bs and 2 Cs.

General

There are two easy steps towards improved scores on this exam:

* Answer the call of the question. Many of you lost points unnecessarily by failing to answer the question asked. On question 1, many of you listed all of the causes of actions that could be brought against Wort instead of figuring out a plan to resolve the situation. (Many of you must not have picked up on my belief that litigation is rarely a good resolution to a Net problem). On question 3, many of you critiqued gambling on the Net instead of describing the difficulties in using contracts to control the risks.

* Organization. In both questions 1 and 2, a number of you were able to significantly improve your score through superior organization. On the flip side, a lot of you lost points unnecessarily through weak organization. Although there are many ways to organize answers to the questions, consider the organization I use below.

Question 1

This question was based on a real life situation I faced in my practice. Despite the similarity to Zeran, this situation occurred before the Zeran case was decided. The story goes as follows: our client (Crumb Corp.) entered into a $60 million merger agreement with BoBo. When the signing of the merger was announced, there was significant discussion about Crumb Corp. at the BoBo forum on a website that specializes in discussions about various high technology stocks. Wort launched a series of attack messages against the president of Crumb Corp., Saber. (The messages were paraphrased pretty faithfully in the exam.) The partner on the Crumb Corp. account forwarded to me a message from Saber and told me to take care of the problem. I had never spoken to Saber, had not worked on the merger, and basically had no context. This is a classic cyberspace law practice problem.

The dilemma, then, is figuring out where to go from there. Here is one possible process:

1. Talk to Saber About What He Wants to Do.

Saber is our client and the first step is to figure out what he wants to do. (I was surprised at how many of you skipped over this step!!) Here are some of Saber's options:
* He can seek to eliminate all lingering offending messages. Note that Saber already complained to the sysop and appears to have succeeded in removing at least 3 of the messages. While everyone assumed that the fourth one was still on the system, in practice it is possible that this one was also removed but cached downstream. It’s truly a case of seeing is not believing. Note also that Saber said “still no action,” implying he does not realize that some of the messages are already down. This is probably because these messages have been cached on his system, and he needs to flush his cache. Believe it or not, in real life the client’s local computer had cached the messages on his hard drive, so he always thought he was being ignored! If you are thinking this issue was too subtle, you’re right—no one got it.

* He can post his own reply. This is a powerful Net-savvy option. In particular, a topic-specific forum such as the BoBo forum is a level playing field where the readers are interested in accurate information and getting to the truth. In real life, unfortunately, the client decided to post a response without consulting us, and he posted a profanity-laced reply that caused the forum to go into a tailspin. Our client’s messages were so bad that the sysop removed his messages along with Wort’s.

* He can try to get Wort to cease posting messages. We’ll talk about this below.

* He can sue. This is definitely the weakest option. We’ll talk about why suits against CompuServe and smallinvestor.com are likely to fail, so his only recourse is against Wort. This is likely to be unsatisfying because (a) we may not be able to find the bad actor, (b) the bad actor is likely to be judgment proof, and (c) while some people claim that there is no such thing as bad press, expanding the press coverage given to this issue while a merger is pending poses significant risks. In this case, a private resolution is likely to be more desirable even if we have legal or moral right on our side.

For purposes of the rest of the question, we’ll assume Saber wants us to pursue all of these.

2. Try to Find the Bad Actor.

We have limited information about the bad actor. While the messages have been from 98765.4321@compuserve.com, an account registered to Lew Wort, we cannot assume this information is true:

* At many sites, people can register under aliases. Therefore, the bad actor may have registered using bogus information. See Zeran v. AOL.

* It is easy to forge headers. The bad actor could make it appear that he was posting from someone else’s real account by forging.

* The account holder may have lost control over his or her account. This is what happened in Stratton Oakmont v. Prodigy, where the emails were posted by a person who hacked into a former employee’s inactive account. In real life, when we finally traced down the owner of the account, we learned that it was an inactive general corporate account held by Emerald, a
competitor/customer of Crumb Corp. It actually became somewhat easy to seek a resolution when they realized their account was being abused.

The lesson here is clear: many of you were prepared to send nasty-grams and flame mail at the account holder. This is likely to be a misstep. At maximum, the account holder should be approached with a light touch. You never know if they are foe or friend. Also, remember my "wild animal" analogy—you never know when or how these people will strike next.


Our goal is to get CompuServe's help in (a) finding out more information about 98765.4321 and (b) ceasing the postings from this account. Since it is possible that the email headers are being forged or the account is an alias, we should not assume CompuServe has any control over the situation. However, they may prove to be helpful even if the headers are being forged, since the poster's actions reflect on CompuServe.

As a number of you pointed out, CompuServe is unlikely to tell us anything about 98765.4321 because of privacy concerns. Short of seeking a court order or getting discovery, there is no legal basis for disgorging this information from CompuServe. However, I was able to convince CompuServe to contact 98765.4321 and notify them of our concerns, which led to our discovery that Emerald was involved.

As a number of you also pointed out, unless there is a forged header/alias problem, the behavior of 98765.4321 likely is a violation of its agreement with CompuServe. While it is doubtful Saber would be a third party beneficiary of that agreement, it is relatively easy to convince CompuServe to terminate the account. As we saw in Zeran, terminating the account does not do much, but it is a good start.

As for CompuServe's legal liability, we are likely to find that its liability is preempted by CDA Section 509 and Zeran. CompuServe is an interactive computer service, and as we saw in Zeran, the I.C.S. is likely to be able to absolve itself of legal liability for the actions of its users.


The single biggest point of confusion on Question 1 was the identity of the sysop of smallinvestor.com. Some of you assumed that smallinvestor.com was part of CompuServe; a few of you thought it was sponsored or run by BoBo. Although I thought the facts were clear, about ½ of you were confused about this, so I tried not to penalize people for this confusion (unless the confusion extended to the rest of the analysis). I had intended smallinvestor.com to be an independent website.

Our objectives in approaching the sysop are (a) obtain more information about 98765.4321, (b) remove any remaining messages, (c) seek to have the sysop help us prevent further attacks, and (d) perhaps have the sysop post some sort of retraction. Ultimately we may need to bring suit against the sysop, but our first approach needs to be friendly.
As with CompuServe, the sysop may be reticent about disclosing information. A perusal of the site might yield some information, however.

The sysop should be responsive to removing other messages if they have already removed some of the messages. A discussion should reveal why only 3 messages were taken down—maybe it was an error, maybe our client had not complained about the fourth, or maybe there was some reason why the sysop chose to keep it. I changed the fact pattern from the real life situation. There, a different message than 178 had stayed up because it had not contained any offensive material in the sysop’s eyes; when I complained, the sysop agreed to take it down anyway. We'll talk about the legal liability issue below.

The sysop may also be responsive to preventing the user from further postings. As with CompuServe, this may be of dubious efficacy. However, note that since 98765.4321 appears to be a frequent poster, locking them out (even if it forces them to reregister under a different name) would destroy some of the reputational interest they have built. We'll talk about the legal liability issue below.

Finally, we might need to ask the sysop to post a retraction to preserve legal rights, despite the holding of It’s In the Cards. As a matter of practice, it would probably be better for our client to post a reply than to get the sysop to post a retraction.

As for the sysop’s liability, we could assert that the sysop is the publisher or speaker of the messages posted and therefore should be liable for their contents. We can support this argument by their implicit editing of the content by leaving one of the messages up (which perhaps they “selected” to stay) or by republishing it after notice from Saber. Of course, it is likely that any such argument will be preempted by the CDA Section 509 and Zeran. However, there are a few outstanding issues here:

* is a website an I.C.S.?
* will Section 509 preempt liability for all of the types of harm caused by 98765.4321? We know it preempts defamation and other “publisher or speaker” torts. Are all of the torts committed by 98765.4321 such torts?
* Will other courts follow Zeran? Or will other courts follow footnote 20 of Zeran and say that the sysop’s actions made them a “provider”?

5. Approach the Bad Actor.

Here we must be clearest about our objectives. As I have indicated, the bad actor may be hard to find, and bad actors as a general rule are unpredictable. We need to plan for other things that the bad actor might do. These could include further attacks on electronic forums, other sorts of attacks (attacks on our website, mail bombs, etc.), bringing the issue to the mass media’s attention and perhaps even physical attacks. As a result, the LAST thing I would do is send flame mail to 98765.4321 without knowing that the bad actor is there and knowing other information about their identity so that we can act quickly in the event of further misbehavior.
Perhaps we can induce the bad actor to post his or her own retraction. This would probably be a great result for our client.

*IF* we choose to approach the bad actor, Saber has numerous potential claims:

* defamatory (messages 172, 178 and 179). We have per se defamation. There are some issues here about public figure/public concern, although I doubt we'll have a problem with malice. The most problematic defense is truth.

* harassment/intentional or negligent infliction of emotional distress. We don't need to discuss all of the ways in which these claims might or might not succeed.

* threats (message 182). Note that this message is probably too "soft" to qualify for a prosecution under 18 USC 875(c) (i.e., the statute at issue in U.S v. Baker). But it may be enough to get a restraining order under state law (see Internet America v. Massey by way of example).

* interference with contract/interference with prospective economic advantage (message 178) for potentially interfering with the merger.

* rights of privacy (unlikely).

There are other potential third party claims that could be brought against the bad actor. Since this does little to "resolve the matter," they did not warrant much time on your exam except perhaps as they might have supported your leverage against the bad actor. These other claims include:

* stock fraud (especially 178). The SEC might be interested in this.

* negligent misrepresentation. The potential plaintiffs would be all of those who detrimentally relied (i.e., people who sold based on allegedly bogus information). Except in the case of a class action, this cause of action is likely to be too diffuse to be of much good. In addition, under Daniel v. Dow Jones, it is unlikely these plaintiffs will be able to assert a special relationship.

* group libel (unlikely)

* trade libel/interference with contract claims that could be brought by Crumb Corp. or even BoBo.

Note that Saber might try to get others involved to assist him to resolve the matter, such as the SEC, the FBI, the local police, or BoBo's attorneys. This might deflect further attacks being levied against Saber, and it might help defray the costs.

In conclusion, you did not have enough time to address all of these points. However, many of you ran into a time crunch by doing extensive legal analyses of all of the ways to smack the bad actor instead of focusing on the process of resolving the matter.

**Question 2**

Question 2 is also a real life question. I got a call from another attorney trying to prepare for a call with his client who was proposing this scheme. The attorney thought there might be some issues. Was he right?!
1. Copyright.

As many of you discerned, our client is doing something like caching. Technically, I would consider this to be mirroring.

As many of you pointed out, a number of copyright rights are implicated by Foreignews actions, including reproduction, distribution, creation of derivative works (in the form of compilations), public display (possibly), and public/digital performance (possibly).

Foreignews could assert the fair use defense:

* purpose and character of use. The use is pretty clearly commercial.
* nature of copyrighted work. Some of you rightly pointed out that it is likely to be more like fact than fiction and the works are clearly published.
* amount taken. 100% of each article.
* effect on the market. Some of you tried to argue that, since the periodicals were directed at South America, there was no loss in the market. In my mind, the Internet collapses geographic markets. So, for example, if these foreign periodicals were charging per page impression, they will lose these impressions. I think courts would likely find a detrimental effect on the market.

All told, it looks like our client probably loses on fair use.

Our client could also assert the implied license defense. I have always approached this defense gingerly, and I certainly would not approve of it as the basis of our client’s business here.

In fact, if anything, I think our client could be liable for criminal copyright infringement. The elements of criminal copyright infringement are willful infringement plus direct financial benefit, or willful infringement plus losses of $5,000. Under either test, I think we could have a prima facie case.

Inexplicably, some of you asserted that, while Foreignews’ business model as described was defective, our client could remedy the situation by caching. Huh? Please review my Cache 22 article.

As many of you concluded, the best we can do is recommend our client use hypertext links instead of mirroring. Even this is not free from peril (see Shetland Times case, plus the more recent cases involving Totalnews and Ticketmaster). However, it does make the risk more manageable. As a number of you pointed out, obtaining a license would also solve the problem, but this is likely to be significantly more costly.

2. Liability for Content.

Since the robot is picking up content without any review, it is possible (likely?) that the content could contain liability-creating material, such as defamatory material, material which our foreign counterpart loaded in violation of copyright, obscene material, etc. In this circumstance, we
reach the anomalous result that Foreignews is likely protected by CDA Section 509. Of course, there are still some limits to this:

* is a website an I.C.S.?
* would any court extend Section 509 protections to a party that has itself engaged in such blatant (and possibly criminal) infringement?
* will a court uphold a dichotomy in liability incurred by an online periodical versus a print periodical?
* 509 will not protect Foreignews for being a further infringer of intellectual property.

3. Jurisdiction.

Foreignews presumably will find itself liable in these foreign jurisdictions to the extent that they can reach Foreignews.

4. Trademarks.

Depending on the way in which Foreignews uses the trademarks of the other periodicals it is copying, it might be liable for trademark infringement.

5. Business Model.

As some of you pointed out, the banner ad business model has weaknesses. A few of you asserted that the audience might be too narrow; I found this perplexing, since the Internet is best at narrowcasting.

Question 3

This question was deceptively simple. I had written this question to cover a real life client situation, but that situation got murky in light of Zeran. So I tried to alter the question to make sure the sysop was liable for its own activity—hence, gambling. Many of you were excited to tell me all of the problems with gambling on the Net—but that was last year’s question! This year’s question was really intended to enumerate all of the reasons why clickthrough agreements may not achieve their desired results:

* leaky clickthrough agreements: to ensure maximum enforceability, they must be structured so that no one can access the site without clicking through. If technically someone can enter the site without clicking on the page, then they can assert they never had notice of the terms

* illegality: no matter what the sysop tries to do in the agreement, the sysop will still be liable for engaging in illegal conduct where ever its conduct is illegal. Since the site probably violates both federal and state laws, there is little we can do in the agreement to prevent a criminal action from being brought. I believe this to be true even if the agreement contains disclaimers (i.e., you are not welcome if you are from specified verboten states) or a representation or warranty that the user is not from verboten states.
Even advertising the website could be sufficient to violate state laws (see Minnesota v. Granite Gate Resorts). Again, this risk cannot easily be eliminated by contract.

* Jurisdiction. Although we presumably can have a binding governing law, jurisdiction and venue clause in our agreement with end users, this clause will be ineffective against third party plaintiffs (i.e., the government).

* Unenforceability. There are multiple reasons why the agreement might be unenforceable:

  - illegality. To the extent that the agreement is for illegal purposes, we will not be able to enforce it against the users. Some of the terms of the agreement might also be “preempted” by local law.

  - language. We are unlikely to be able to enforce the agreement against people who do not understand English.

  - minor. Unless we verify age, there is no way to enforce the agreement against minors.

  - other incapacities, such as intoxication or insanity. There is no way to know if a user clicking through is afflicted with these conditions.

  - unconscionability. The more aggressively we try to protect ourselves, the more likely the agreement could be deemed unconscionable.

Some of you asserted that there must be a refund option to have an enforceable agreement. I do not think this is a natural reading of ProCD; if anything, Easterbrook seemed to assume that agreements for services were enforceable even if the terms were disclosed later (i.e., on the back of a ticket) and without any stated refund policy.
Questions # 1

Since Crumbs, Saber's Company, is currently in the process of merging with another company, it would be wise for Saber to proceed with care—meaning he should explore other avenues before seeking litigation. While Saber seems quite sure that Worf posted these messages, whether this is true or not should be ascertained. The first order of business should be to contact CompuServe. Depending on what CompuServe's policy is with its users, it is possible CompuServe may be inclined to kick Worf off of its system (cancel his account) if it believes that he is using it to commit malicious activity. We may also request that CompuServe collate whether Worf is in fact the holder of the account, although this is unlikely to happen.

We may also request Saber's request to the small investor sysop to have the offending message that remains removed. Although Saber claims that the sysop has taken no action, it appears that three of the four messages have been removed. At the very least, having the sysop remove the fourth message will limit the dissemination of the offensive message somewhat.
If Sabor wishes to push harder against Work, he likely has a cause of action for defamation. If this were to happen, it would certainly help flush out whether Work did in fact post the messages! An action for defamation requires the publication of an untrue assertion of fact and some form of reputational injury to Sabor. The first order of business is to make sure these statements weren't actually true. We'll assume here that Mr. Sabor is an upstanding citizen (although these facts are quite similar to those in Stratten—which after the case settled turned out to be true!). Publication only requires communication to a third party, which clearly occurs when statements are made on a message forum. Finally, it should not be difficult to demonstrate reputational injury to Sabor. If these postings affected the merger talks with BoBo, some reputational harm would be shown. Moreover, the recent statements made in ¶ 179 may constitute per se reputational harm.

We also need to prepare for any defenses that could be asserted by Work. As was stated above, truth is an absolute defense to defamation, so we must make sure that our client is in fact not a crook. In addition, Work may also try to assert that this is a
matter of public concern or that Saber is a public figure (which would require us to demonstrate that Wirt acted out of actual malice.) However, nothing here indicates that Saber is a public figure. Depending upon whether BobBo is a publicly traded company and/or the pending merger has received considerable ink, Wirt has an argument that Saber’s crookedness is a matter of public concern may hold some water (albeit not very much water).

It is also possible that we could assert another stunt for harassment by Wirt, another form of speech is not Constitutionally protected. Message 18.2 is threatening in some respects. However, the threat is not very strong. More importantly, it is difficult to assert threat/ harassment occurred over the internet, because the parties can never face to face, the physical element that is frequently found in these cases is missing, so this claim is fairly weak.

If our client really wants to be aggressive, he may also wish to see the payoff of smallmuster. However, as a preliminary matter, we must determine what smallmuster Com’s relationship is with BobBo (as it is running a forum that specifically discusses BobBo... If there is some...
relationship between the sysop and Crumb's potential merger partner, this claim may best be left alone...

If Saber does wish to pursue a claim against the sysop, he should be warned that the state of the law for sysop liability for defamation is currently up in the air. The recently-adopted CDA states that "no provider or user of an interactive service shall be treated as a publisher or speaker of any third party content." *Zeran*, a recently-decided case, indicated that the CDA preempts any state law claims and therefore the sysop will not be liable for the defamation of another, even if he had notice of the defamatory statement (as was the case here.) However, the Constitutionality of the CDA is in question (and is pending before the Supreme Court.) Thus it is currently subject to an injunction. If the CDA is in fact bad law, then we must look to Cubby and Stratten Oakment. Cubby indicated that a sysop won't be liable for defamation if he has not exercised any editorial control over the messages on his board. Stratten Oakment found liability for the Sysop where he had the policy, intent and means to exercise control. It is unclear from the facts, we
currently have how much, if any, control the small investor can expect had. This issue may be critical if the COA is permanently struck down, so investigation in this area should be commenced if Sater wishes to pursue this cause of action.
QUESTION #2

Points to Cover in Client Conference Call

1. What is the client's relationship with the publications from which it will be "borrowing" articles? The U.S. copyright laws confer a monopoly to the creator for original works of authorship in a tangible medium of expression. Direct copyright infringement requires access and substantial similarity between the works to be shown, and this is strict liability. That being said, unless our client has some sort of licensing arrangement with each publication from which it will take articles, it will be violating U.S. copyright laws.

Should the client not have any licensing arrangement with these periodicals (and not wish to create any) it will be limited to asserting a fair use defense to copyright infringement. If it is sued. The test for fair use weighs four factors - the purpose and character of the use, the nature of the work, the substantiality of the work taken and the effect on the potential market. The proposed purpose of our client's use is clearly commercial, as the website is advertising-supported. The nature of the works in question is essentially fact, as it is news reporting, and it is published. This would cut in our favor.
Our client would be using 100% of each work (each individual article is copyrightable), which cuts against our client. The effect of the market practice is the most important factor typically and might hinge upon whether the publications are distributed in the US, since this website is targeted at US business executives. Nevertheless, on balance, the fair use defense would be quite weak for our client.

Thus being said, we should try to persuade the client either to (1) get licensing arrangements with all publications it wishes to borrow from, or (2) use hypertext links instead of the actual articles. While hypertext linking may technically be considered infringement (since each browsing involves making a copy of each page viewed and hypertext linking creates knowing contribution to this), the fair use defense may be stronger (slightly) and public policy would certainly be in our client’s favor (after all, what would be the point of the net without hypertext linking!).

2. What are the potential pitfalls of caching? Particularly if the client insists on setting up its site in the proposed manner, it could leave itself open to some problems that once from
caching, and thus should be prepared for them. First, if our client were to be sued for copyright infringement and loses, it will likely be responsible for doing more than just taking down its own website and paying damages. It will probably also have to notify all search engines, partners, and anyone else it thinks might have old copies of its web page cached in their systems (Atkaouei). While Atkaouei addressed a trademark issue, there is nothing preventing it from being applied to right of other wrongs. One way that Foreignness could minimize the potential impact of such a problem is to implement technology that would cause each web page to be purged after a certain time (such as expiry of headers) or that force the page to be rebuilt each time it is accessed (such as CGI scripts).

3. Jurisdictional Issues. Finally, the client should be warned that the fact it is taking articles from non-U.S. publications may leave it open for liability in the U.S. for wrongs in those publications. A publisher is not liable in every jurisdiction just for putting information on the net. However, unless there is an extradition treaty in place for the countries in which the other publications operate, a plaintiff in the U.S. may not be able to sue them for wrongs, such as defamation or copyright violation, contained in their publications. In that case, such
a plaintiff may turn to our client as its only way of getting a remedy in the U.S. Depending upon the type of wrong, Foreigners could be liable as a publisher of defamation, or as a direct or contributory infringer of a third party's copyright. Finally, the Foreigner should be wary of what it is posting as some things that are illegal in the U.S., such as child pornography, may not be illegal elsewhere.
As a preliminary note, because the crapsgambling.com's wagering will involve real money, its activities will be illegal in some many, if not most, U.S. jurisdictions. Therefore, it will be a struggle to protect any of its business interests.

First, crapsgambling wants to get each of its users to "sign" a user agreement (more simply put, a contract). While it appears that contracts formed on line are probably enforceable, there is no determinative authority for this position. That being said, crapsgambling must structure its agreement in such a way that the user is forced to read the entire agreement and sign off on it before it can access the gambling facilities. This could be done by forcing the user to scroll down through the whole agreement and type or click "OK" at the bottom before he can proceed, as long as there is no way to get around this.

However, general contract enforceability is the least of crapsgambling's problems. Contracts to provide services that are illegal are generally not enforceable. Thus, any money lost by a wagerer in signing up for the agreement could be lost to craps gambling. If crapsgambling were
to go after a user to "pay up" its gambling debts (say the users credit card went over the limit), the user could simply assert that the contract was unenforceable, stifling our potential client.

Moreover, to the extent that there is criminal liability associated with gambling in any jurisdiction to which craps gambling is subject, we would agree. Any indemnity as to criminal liability in the agreement would be ineffective, as you generally cannot contract out of criminal liability.

One way that craps gambling could limit its exposure would be to move offshore to a country that has no extradition treaty with the US and permits gambling. Because of the global nature of the internet, craps gambling would still be able to reach potential users in the US without necessarily subjecting itself to US laws. On the other hand, it would not be advisable for this firm to counsel a potential client to do so. Giving a client legal advice on how to commit a crime is at the very least unethical and could create liability for the firm as an aider/abettor.

In short, it will be difficult if not impossible for craps gambling to contract
US way out of liability for the gambling services it wishes to provide. Moreover, while bringing new business into the firm is generally a very good thing, perhaps this is one of those rare occasions when we should consider rejecting a potential client.
Cyberspace Legal Topics
by Eric Goldman (formerly Eric Schlachter)
Cooley Godward LLP, Palo Alto, CA
schlachtere@cooley.com

Sysop Liability for Third Party Content

- What is effect of CDA Section 509? Is a website a “provider or user of interactive computer services”? Is the moderator of a mail list or Usenet group a “provider or user of interactive computer services”? What torts are shielded by the protection of “publishers/speakers”? Would a physical space publisher be liable in physical space for third party content but immune for publishing the exact same content in cyberspace?
- Is a sysop liable for the content contained at the terminus of links?
- Is a sysop liable for the content of Usenet feeds?
- Is a sysop liable for user-released viruses?
- What qualifies as prescreening/editorial control? Would virus checking constitute prescreening? Would removal of off-topic postings constitute editorial control? Would employee participation in a forum constitute editorial control? Would removal of postings that are known to create tort liability constitute editorial control? Would the selection and organization of links constitute editorial control? Does the mere existence of a policy about third party content create editorial control?
- Assuming that a reckless standard is adopted for liability, at what point does the sysop “know or should have known” about the content on its site? Does maintenance of the site (including, presumably, reviewing the “form” of the site) create knowledge?
- Is a sysop liable for direct copyright infringement for content posted by users?
- Is a sysop liable for unfiltered content that is adjacent to filtered content?
- Are anonymous/pseudonymous remailers liable for material sent through their system?

Defamation

- Should the right of reply replace defamation suits?
- What is a public figure online?

Copyright

- Is Web browsing infringement?
- Is linking to third party content infringement? Does it matter if the content is inlined? Does it matter if the third party’s website contains a provision stating that linking is not permitted? Does “deep linking” constitute an infringement?
- Is caching infringement?
  - Is caching by browser software infringement?
  - Is caching by proxy servers infringement?
  - Is indexing, caching or archiving by offline browsers infringement?
- Who is liable for tortious cached data if the underlying material has been changed by the initial publisher?
  - Is the archiving of postings to a mail list/newsgroup infringement?
  - Is creating a full text index (i.e., the indexes created by HotBot, Alta Vista, Lycos, Infoseek, etc.) of copyrighted material infringement? Would it matter if the indexed site used a robot exclusion header?
  - Is there an implied copyright license to browse/link/frame/cache unless the IP owner uses technological methods to inhibit the behavior?
  - Is framing an infringement of copyright or trademark?
  - Who (if anyone) owns a compilation copyright in message boards/mail lists?
  - Is there a trend towards increased moral rights in the United States--or, at least, increased protection for the right of attribution?
  - Would a copyright clearinghouse or microtransactions be a substitute for increased copyright protections?
  - Is the HTML coding for a page copyrightable?
  - Will database access/linking agreements replace licenses of non-copyrightable databases?
  - Should there be sui generis protection for databases?
  - When does web-based publication enhance or interfere with the market?

**Trademarks**

- How will co-existing trademarks in physical space will get reconciled on the Net?
- What constitutes a trademark “use” online?
- Is meta-tagging a trademark infringement?
- When do online trademark licenses implicate franchise law?
- How can the look and feel of websites be protected?
- Would NSI be liable for contributory trademark infringement if it interpleaded contested domain names?
- Do name registrants have an obligation to trademark owners?
- Would geography-based domain names or new top level domains minimize conflicts?
- Does trademark dilution law effectively prevent any clean solution to the domain name problem?
- Does a domain name confer a trademark-like status onto generic terms? Is a domain name an address, a mnemonic, a trademark, all of the above or none of the above—and does it matter?
- Should registered trademarks confer greater rights to a domain name than other forms of trademarks or personality rights?
- Does the reservation of a domain name infringe a trademark?
- Does a trademark owner have an obligation to shut down “fan sites”?
- Does a trademark licensee have an obligation to eliminate references to the trademark from indexes, links, etc. after the termination/expiration of the license?
Commerce

- When are clickthrough agreements and disclaimers binding and enforceable?
  - Will the ProCD/Hill cases be followed in other jurisdictions?
  - Where should the agreement/disclaimer be located on the site?
  - Issues in software downloading agreements (enforceability of prohibition on reverse engineering, export control)
  - Issues in content posting agreements (license of/assignment to posted content, sysop protection for harm caused by posted content)
  - Enforceability of disclaimers of warranties and limitations on liabilities
  - Problems with privacy statements specifying what the sysop will do with user information
  - Impediments to proper contract formation (language, underage and other incapacities, ease of bypassing agreement depending on site placement, contracts of adhesion, unilateral contracts, provisions that are void for public policy under local law)
- Should information services be subject to sales tax?
- Recent trends in the permissibility of disclosures pursuant to state and federal securities laws.
- Are there viable alternatives to fixed-price Internet access pricing, such as metered/per-packet pricing, congestion pricing and transfer pricing?
- Issues in Corporate Internet Usage Policies.
- Formation of online standards and the application of antitrust law. Should the standard setters be personally liable?
- Issues in running a legal Internet contest or sweepstake.
- Does California Business & Professions Code §17538 apply to the vending of information goods?

Spam

- What can be done about forged headers?
- Analysis of the Nevada law and the need for non-Nevada residents to comply

Jurisdictional/Choice of Law Issues

- Does use of a server confer personal jurisdiction?
- Does publishing content on the Internet confer worldwide general personal jurisdiction? Is there a distinction between active and passive websites?
- Does publishing advertisements on the Internet confer worldwide specific personal jurisdiction for trademark infringement?
- When do foreign states’ sales tax laws apply to online transactions?
- Online gambling—is it legal for the gambling institution? Is it legal for the manufacturers of the gambling devices? Is it legal for the gambler?
- Setting community standards in cyberspace. Is cyberspace its own community? Are there multiple online-only communities in cyberspace?
• Effects of practice of medicine and law across geographic borders
• Liability for violating local advertising laws (i.e., European prohibitions of comparative advertising and Toubon laws).

Export Control

• Is uploading software to the Internet automatically a violation?
• What constitutes good faith compliance (checking IP addressees, checking physical addresses, real time or post hoc check of the Table of Denial Orders and List of Specially Designated Nationals)?
• Analysis of the different approaches under export control law to freeware v. beta software made freely available v. “try before you buy” software.
• Does providing a service from the U.S. that permits encryption of files violate export control?

Privacy Interests

• Who should bear the costs of truly anonymous activities?
• Are there limits on the discovery, use and disclosure of information gleaned about individuals from online data tracking?
• Analysis of legal issues regarding programs that extract information from a user’s hard drive or browser software and communicate the information back to a central server.
• Standards for government-compelled disclosure of encryption keys.
• User control over information contained in the cookie.
• Effect of European Distance Selling Directive.
• Sysop liability for disclosure of private information in violation of web-based privacy statement (breach of contract, ECPA?).
• Protection of children’s interests online.

Electronic Communications Privacy Act

• What information can an ISP disclose to third parties about its subscribers? Does it matter if the third party is the government or a private entity?
• Duties of a website distributing private communications to keep these communications private (i.e., would a website distributing a personal greeting be liable if it failed to use a security system?).
• Do spam filters deployed by ISPs violate the ECPA?

New Issues in Tort Law

• Should the definition of “reasonable person” be adjusted for the cyberspace community?
• Liability for the release of cancelbots.
• Liability under 18 USC Section 1030 for license management tools.
• When does online behavior become “harassing”?
• Can web browsers sue in tort for inaccurate information? Can liability for this tort be disclaimed? Are there enhanced standards depending on the content of the material (i.e., health information v. general information)?
• Can a website accept a banner advertisement for a gambling website?
• Who bears liability when a website permits its users to establish a governance system?
• Application of trespass law to uses of computer system resources other than in the spam context. Does trespass law create the possibility that any undesired online behavior is a tort?
• Does ignoring headers (i.e., robot exclusion headers, no-caching headers) constitute a trespass?
• What rules must a website comply with before it can offer to pay commissions to its subscribers/customers for selling on its behalf?

Right of Publicity

• Does the use of a celebrity’s name in a metatag violate their right of publicity?
• Does posting a celebrity’s photo online violate their right of publicity? Does it matter if there are banner ads on the page?
• Does indexing the page where the photo is located cause the indexer (i.e., the search engine) to violate the right of publicity? Does it matter if the search engine places banner ads on the page?

Government Issues

• Does the public forum doctrine create a right of access against private online entities?
• Does a user’s use of government-provided accounts reflect upon the institution?
• Do University Internet/Computer use policies violate the First Amendment?
• Should government employees cookies be subject to the Freedom of Information Act?
• Is NSF a government actor? Does NSI become a government actor by extension?

General Certification Authority Issues

• Role of government in certifying root Certification Authorities v. self-certification
• Licensing/qualification/financial responsibility/bonding of Certification Authorities.
• Insurance requirements and availability.
• Time limitations on the validity of certificates.
• Are digital signatures “goods” under UCC Article 2 or are they services?

Uses of Digital Signatures

• Use of digital signatures as a way to limit access to sensitive servers/documents
• Use of digital signatures to certify content delivered to users
• Use of digital signatures as anti-virus mechanism
• Use of digital signatures to facilitate credit card transactions (SET)
• Use of digital signatures as a replacement for EDI

Duties and Practices of CAs

• Duties or “best practices” of a Certification Authority to verify the accuracy of data contained in an application for a certificate.
• Duties or “best practices” of a Certification Authority in establishing a trustworthy system (e.g., security from intrusion and misuse; levels of availability, reliability and correct operation; performance of intended functions; adherence to generally accepted security principles).
• Duties or “best practices” of a Certification Authority in hiring and retention of personnel.
• Duties or “best practices” of a Certification Authority in keeping and maintaining records.
• Duties of a Certification Authority to act on instructions from the subscriber to suspend or revoke a certificate.
• Duties of a Certification Authority to suspend or revoke certificate other than at the request of the subscriber.
• Duties of a Certification Authority in handling certificate revocation and suspension.
• Duties of a Certification Authority to maintain the privacy of information submitted by subscribers.
• Duties of a Certification Authority to maintain the privacy of transactional information.
• Duties upon cessation of activities as a Certification Authority.

CA Liabilities

• Liability of Certification Authority for negligence or negligent misrepresentation in issuing a certificate (to subscriber and parties who rely on the certificate).
• Liability of Certification Authority if its key is compromised and fake certificates are issued (to purported subscribers and parties who rely on fraudulent certificates).
• Liability of Certification Authority if its security is breached and private keys issued by the Certification Authority are compromised (to subscribers and to third parties who rely on the certificate).
• Liability of Certification Authority for errors or delays in suspending or revoking certificates.
• Liability of Certification Authority to subscriber for wrongful suspension or revocation of a certificate.
• Representations and warranties implied by a Certification Authority in issuing a certificate, and the ability of the Certification Authority to disclaim implied warranties.
• Ability of Certification Authorities to limit liability and exclude damages (to subscribers and parties who rely on certificates).

**Digital Signature Presumptions**

• Presumptions which arise from use of digital signatures.
• Presumption of authenticity for digital signatures (e.g., right of receiver of digitally signed record to rely on the digital signature).
• Use of digitally signed records to satisfy writings and signature requirements under law.

**Duties of Digital Signature Subscribers**

• Duties upon a subscriber to maintain control over private key and liability of a subscriber for unauthorized use of its private key.
• Use of passphrases, hardware tokens or biometric authentication by subscribers.

**Esoterica**

• Recognizing real property like interests in user accounts (i.e., quiet enjoyment, rights after termination)
• Do physical space laws apply in MOOs and MUDs? (Punishment for virtual rape)

This document was last revised December 14, 1997.