Cyberspace Law/Law 5793
Professor Eric Goldman (formerly Eric Schlachter)
Santa Clara University School of Law
Spring 2000

1. **MEETINGS.** The class meets on Monday nights from 7:30 to 9:10, except that the class will meet on Tuesday night on February 22. The first class meets on January 10 and the last class meets on April 24. Pursuant to University regulations, class will not meet on January 17 (Martin Luther King Birthday), February 21 (President's Day) or February 28 (Spring Break).

2. **PREREQUISITES.** This class is a general survey class in nature and thus there are no prerequisites other than completion of the first year courses. Some students have found copyright law and first amendment law classes were helpful. If you do not have experience using the Internet, you will need to gain this experience during the class.

If you have taken the Ballon/Middlehurst Internet law course or Savage's e-commerce law course, I strongly discourage you from taking this course. If you have taken or are taking Professor Hammond's digitallaw.com or Davis/Boustani's Internet litigation class, you will find some overlap in the course topics.

3. **FINAL EXAM.** The final exam is scheduled for May 2 at 6:00 p.m. The class will be graded based solely on the final exam. The final exam will probably be 1½ hours long with 2 questions. The exam will emphasize real life situations and problems and test your ability to come up with practical solutions.

Prior exams are available on the Internet. Note that the law may have changed since the exam was given!

<table>
<thead>
<tr>
<th>Year</th>
<th>Exam Link</th>
<th>Sample Answer Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td><a href="http://members.theglobe.com/ericgoldman/1999exam.html">Link</a></td>
<td><a href="http://members.theglobe.com/ericgoldman/1999answer.html">Link</a></td>
</tr>
<tr>
<td>1997</td>
<td><a href="http://members.theglobe.com/ericgoldman/1997final.html">Link</a></td>
<td><a href="http://members.theglobe.com/ericgoldman/finalans.html">Link</a></td>
</tr>
</tbody>
</table>

Historically, I have given roughly 33% As and 10% Cs.

4. **PAPERS.** I do not require a paper as part of the class. I am happy to help you on an informal basis with your papers or paper topics—just let me know how I can help. If you are looking for a topic, consider my list of "difficult" issues at [Link](http://members.theglobe.com/ericgoldman/issues.html). You should also check out my list of cyberspace law source material. See [Link](http://members.theglobe.com/ericgoldman/tablecase.html).

If you want me to act as your faculty advisor for an independent study, please review the following rules. (I apologize for promulgating rules about this, but prior abuses compel me to set some clear boundaries).
• I will take no more than 3 students total, and maybe less.

• I will only consider requests made before January 14, 2000. Please email me ASAP if you are interested.

• I will require you to establish a schedule for completing the final version of the paper, and I will expect you to adhere faithfully to that schedule. I will also require you to handle all administrative aspects of dealing with the University requirements about the paper.

• In addition to fulfilling the upper division writing requirement, you must commit either to publish the paper or use it towards the High Tech certificate.

5. **EMAIL LIST.** I have created an official email list for the class. I will use this email list for class announcements, other timely messages and occasional random postings. You must subscribe to the email list as soon as possible at cyberlaw2000-subscribe@globalists.com. The list is unmoderated, so you may post to the list freely (but please do so wisely). To do so, you can send emails to cyberlaw2000@globalists.com. PLEASE DO NOT SEND SUBSCRIPTION MESSAGES TO THE LIST! The list's main page is at http://globalists.theglobe.com/computers_internet/law/cyberlaw2000-L/list.html, and you can find the list archives from there.

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

7. **OFFICE HOURS.** I do not have regular office hours on campus, but students have found that I am very accessible by phone, email or appointment. Email is usually the best way to reach me, but please understand that I may not respond to emails until the weekend.

8. **ACADEMIC FREEDOM.** Because cyberspace permits people to interact with each other in effectively unlimited ways, it is inevitable that we will discuss the seedier side of the human condition in class. If you have any concerns about this, please let me know immediately.

9. **JOBS.** I would be happy to help you with your job searching efforts. To start the process, please email me your resume (in the text of an email, not as an attachment) and schedule a time to talk.

10. **CONTACT INFORMATION.**

Eric Goldman (formerly Eric Schlachter)
Cooley Godward LLP
5 Palo Alto Square, 3000 El Camino Real, Palo Alto, CA 94306 (subject to change in February)
Phone: (650) 843-5154
Fax: (650) 857-0663 (subject to change in February)
Email: egoldman@cooley.com
Web Page: http://members.theglobe.com/ericgoldman. An electronic copy of this syllabus is available at that address.
CLASS SCHEDULE AND READING MATERIALS

This class reader is the only required reading. There are a number of general mass-market books about cyberspace law available. Because cyberspace law is developing so rapidly, all of these books are out-of-date to some degree, and former students have not indicated a need for a supplemental reader. But if you feel otherwise, please let me know and we can discuss the best supplemental resources for you.

1. **INTRODUCTION TO CYBERSPACE** (January 10 and 24).
   - ACLU v. Reno (CDA I; district court ruling; facts only) ........................................ 1
   - Cyber Promotions v. America Online (November 1996 ruling) .................................. 17

2. **JURISDICTION AND VENUE** (January 31).
   - Millennium Enterprises v. Millennium Music .......................................................... 27

3. **COMMERCE CLAUSE** (January 31).
   - American Library Association v. Pataki ................................................................. 43

4. **CONTRACTS** (February 7).
   - Caspi v. Microsoft Network ....................................................................................... 66

5. **SPAM AND TRESPASS** (February 7 and 14).
   - Cooley Godward Chart of Spam Laws (by Max Ochoa) .............................................. 70
   - Cal. Business & Professions Code §17538.4 ................................................................. 72
   - Cal. Business & Professions Code §17538.45 ............................................................... 74
   - CompuServe v. Cyber Promotions (February 1997 ruling) .......................................... 77
   - Hotmail v. Van$ Money Pie ......................................................................................... 88

6. **PRIVACY AND ANONYMITY** (February 22).
   - Children’s Online Privacy Protection Act .................................................................... 96
   - 16 CFR Part 312 (rules implementing COPPA) ............................................................ 104
   - GeoCities Agreement Containing Consent Order ......................................................... 118

7. **INFORMATION TORTS** (defamation, right of publicity/privacy, inaccurate information, harassment, gambling) (March 6).

8. **OBSCENITY, CHILD PORN AND INDECENT SPEECH** (March 13).
   - ACLU v. Reno (Supreme Court) .................................................................................. 127
   - Cyberspace Communities v. Engler ............................................................................. 151
9. **TRADEMARKS AND REGISTRAR LIABILITY** (March 20).

Anticybersquatting Consumer Protection Act ......................................................... 164
ICANN Domain Name Dispute Resolution Policy and associated Rules ................. 180
Avery Dennison v. Sumpton (9th Cir.) ....................................................................... 196
Playboy v. Welles (1998 District Court) ................................................................. 210
Bally Total Fitness Holding Corp. v. Faber .............................................................. 217
Lockheed Martin v. NSI (9th Cir) .............................................................................. 222

10. **COPYRIGHT, TRADE SECRET, PATENTS AND HOT NEWS** (March 27 and April 3).

17 U.S.C. §512 (especially subsections (a) and (b)) .................................................... 231
Eric Goldman (formerly Eric Schlachter), The Intellectual Property
Renaissance in Cyberspace: Why Copyright Law Could Be
Unimportant on the Internet ....................................................................................... 239
Intellectual Reserve v. Utah Lighthouse Ministry .................................................... 267

11. **DERIVATIVE LIABILITY FOR THIRD PARTY CONTENT** (April 10 and 17).

17 U.S.C. §512 (especially subsections (c) and (d)) .................................................... 231
47 U.S.C. §230 .............................................................................................................. 277
Cooley Godward’s Information Technology Group, Website Provider
Liability for User Content and Actions ....................................................................... 279
Playboy v. Russ Hardenburgh ...................................................................................... 283
Zeran v. America Online (4th Cir.) ............................................................................. 296
Lunney v. Prodigy Services (Court of Appeals ruling) ............................................... 304

12. **COMPUTER FRAUD & ABUSE ACT, ECPA AND OTHER COMPUTER CRIMES** (April 24).

18 U.S.C. §1030 .......................................................................................................... 310

NOTE: Most of the readings listed above can be found electronically through
http://members.theglobe.com/ericgoldman/tablecase.html, except for articles, which can be
found through http://members.theglobe.com/ericgoldman/publicat.html.
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
AMERICAN CIVIL LIBERTIES UNION, et al.,

v.

JANET RENO, Attorney General of
the United States

CIVIL ACTION No. 96-963

---------

AMERICAN LIBRARY ASSOCIATION,
INC., et al.,

v.

UNITED STATES DEPT OF JUSTICE,
et al.

CIVIL ACTION No. 96-1458

Before: Sloviter, Chief Judge, United States Court of Appeals for the Third Circuit; Buckwalter and
Dalzell, Judges, United States District Court for the Eastern District of Pennsylvania

June 11, 1996

ADJUDICATION ON MOTIONS FOR PRELIMINARY INJUNCTION

I. INTRODUCTION

Procedural Background

Before us are motions for a preliminary injunction filed by plaintiffs who challenge on constitutional
grounds provisions of the Communications Decency Act of 1996 (CDA or "the Act"), which constitutes
Title V of the Telecommunications Act of 1996, signed into law by the President on February 8,
include various organizations and individuals who, inter alia, are associated with the computer and/or
communications industries, or who publish or post materials on the Internet, or belong to various citizen
groups. See ACLU Complaint (¶¶ 7-26), ALA First Amended Complaint (¶¶ 3, 12-33).

The defendants in these actions are Janet Reno, the Attorney General of the United States, and the
United States Department of Justice. For convenience, we will refer to these defendants as the
(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
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 "listserv"), [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

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
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 unmoderated 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 scripts because the server software of these online services is 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 technologically 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. Labeling 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); Acierne v. New Castle County, 40 F.3d 645, 653 (3d Cir. 1994). The motions for preliminary injunction will therefore be granted.

The views of the members of the Court in support of these conclusions follow.
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

Cyber Promotions Inc.

v.

America Online Inc.
C.A. NO. 96-2486

America Online Inc.
v.

Cyber Promotions Inc.
C.A. NO. 96-5213

November 4, 1996

MEMORANDUM OPINION AND ORDER

Opinion: Weiner, J.

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.

5. 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.

6. 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.
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 'erecit 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 Hathoro*, 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 ""[t]he 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 *Krynicky 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 communciations 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 statute 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 protesters had no other alternative to convey their message at the single establishment in the shopping center, the protesters 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 protesters] 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 Edmonson 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. Ciancey, 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.

We are troubled by the Grandbouche decision because it has the effect of creating government action every time a magistrate 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 I, Section 7 of the Pennsylvania Constitution.

Tate 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.

Western Pennsylvania, 515 A.2d at 1338.

The case sub judice is more similar to Western Pennsylvania than it is to Tate. AOL's e-mail servers are certainly 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 PruneYard that states 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.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CYBER PROMOTIONS, INC. v. AMERICAN ONLINE, INC.
C.A. NO. 96-2486

AMERICAN ONLINE, INC. v. CYBER PROMOTIONS, INC.
C.A. NO. 96-5213

ORDER

The motion of American Online, Inc. for partial summary judgment on First Amendment issues is GRANTED in part and DENIED in part.

The Court declares that Cyber Promotions, Inc. does not have a right under the First Amendment to the United States Constitution or under the Constitutions of Pennsylvania and Virginia to send unsolicited e-mail advertisements over the Internet to members of American Online, Inc. and, as a result, American Online, Inc. may block any attempts by Cyber Promotions, Inc. to do so.

Cyber Promotions, Inc. shall, within ten days of the date of this Order, submit to the Court a list of the theories other than the First Amendment which it believes entitles it to send unsolicited e-mail to members of American Online, Inc.

Either party may request that we issue an Order certifying our decision for an immediate interlocutory appeal to the United States Court of Appeals for the Third Circuit.

IT IS SO ORDERED.

FOOTNOTES

FN1. 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.

FN2. 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.

FN3. 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.
Jurisdiction/Venue: Court Opinion and Order

In the United States District Court for the District of Oregon

Millennium Enterprises, Inc.,
dba Music Millennium and
Millennium Music, an Oregon corporation,

Plaintiff,

v.

Millennium Music, LP,
a South Carolina limited partnership;
Millennium Music, Inc.,
a South Carolina corporation,

Defendants.

Civ. No. 98-1058-AA

Opinion and Order

Darin D. Honn
James C. Loy
Christopher D. Bell
Duncan Honn, P.C.
4386 SW Macadam Ave., Suite 302
Portland, OR 97201
Attorneys for plaintiff

Julianne Ross Davis
Robert K. Lau
Chernoff, Vilhauer, McClung & Stenzel, LLP
600 Benj. Franklin Plaza
One SW Columbia St.
Portland, OR 97258
Attorneys for defendants

AIKEN, Judge:

Plaintiff files suit seeking damages and injunctive relief for alleged trademark infringement under the Lanham Act, 15 U.S.C. §§ 1051-1127. Plaintiff also alleges state statutory claims for unlawful trade practices, trademark infringement and dilution, and common law claims of unfair competition and trademark infringement. Defendants seek dismissal for lack of personal jurisdiction pursuant to Fed. R. Civ. P. 12(b)(2). For the reasons discussed below, defendants' motion is granted.
I. FACTUAL BACKGROUND

Plaintiff, Music Millennium, is a business incorporated in Oregon with its principal place of business located in Portland, Oregon. Plaintiff opened its first retail outlet under the name "Music Millennium" in 1969. Plaintiff now operates two retail music stores in Portland and also sells products through mail and telephone orders and its Internet Web site.

Defendant Millennium Music, Inc., is a South Carolina corporation and general partner of defendant Millennium Music, L.P., a South Carolina limited partnership. Defendants operate retail music stores in South Carolina under the name "Millennium Music." Defendants sell products through their retail outlets and their Internet Web site, although the vast majority of sales occur at their retail stores. From March 1998 through September 1998, defendants sold fifteen compact discs to nine separate customers in six states and one foreign country. The sales totaled approximately $225. During the same period, defendants' retail sales were $2,180,000. Defendants also offer franchising circulars through the Internet and have two franchised stores in North Carolina.

Defendants have purchased a small amount of compact discs from Allegro Corporation ("Allegro"), a distributor located in Portland, Oregon. Defendants' purchases from Allegro in 1994-1997 totaled approximately one-half of one percent of defendants' inventory purchases for those years.

On or about July 7, 1998, plaintiff received a credit document from Allegro. The credit was mailed to plaintiff in error; the document apparently was intended for defendants. See Affidavit of Donna Cleaver, Exhibit A.

On August 21, 1998, an Oregon resident, Linda Lufkin, purchased a compact disc from defendants through their Web site. During oral argument on defendants' motion to dismiss, the court learned from defendants that an attorney at the law firm for which Ms. Lufkin works requested that she purchase a compact disc from defendant. Apparently, the attorney is an acquaintance of plaintiff's counsel. Plaintiff did not dispute these facts. Defendants have sold no other merchandise to any Oregon resident.

Plaintiffs filed suit on August 28, 1998. According to plaintiff's complaint, defendants' use of the name "Millennium Music" in connection with the sale of goods in interstate commerce violates plaintiff's state and common law trademark rights. Plaintiff further alleges that consumers familiar with plaintiff will likely be confused as to the source or origin of defendants' goods, thereby causing plaintiff harm.

In September of 1998, defendants added a disclaimer to their Web site indicating that their products and franchise circulars were not available in Oregon.

II. JURISDICTIONAL STANDARDS

Determining whether personal jurisdiction exists over an out-of-state defendant involves two inquiries: whether the forum state's long-arm statute permits the assertion of jurisdiction and whether assertion of personal jurisdiction violates federal due process. Fireman's Fund Ins. Co. v. National Bank of Cooperatives, 103 F.3d 888, 893 (9th Cir. 1996); Chan v. Society Expeditions, Inc., 39 F.3d 1398, 1404-05 (9th Cir. 1994), cert. denied, 514 U.S. 1004 (1995). The relevant state statute applies even when the cause of action is purely federal. Fed. R. Civ. P. 4(k). Oregon's long-arm legislation is found in Rule 4 of the Oregon Rules of Civil Procedure. Plaintiff maintains that Rules 4C and 4D confer personal jurisdiction over defendants.1 However, Oregon's catch-all jurisdictional rule confers personal jurisdiction coextensive with due process. Or. R. Civ. P. 4L. Thus, the analysis collapses into a single framework and the court proceeds under federal due process standards.

Due process requires that a defendant, if not present in the state, "have certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." International Shoe Co. v. Washington, 326 U.S. 310, 315 (1945) (internal quotation marks omitted). Minimum contacts can be demonstrated through facts supporting either general or specific jurisdiction over the defendant. See Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414 (1984). Plaintiff bears the burden of establishing personal jurisdiction through a prima facie

A. General Jurisdiction

General jurisdiction refers to the authority of a court to hear any cause of action involving a defendant, regardless of whether the cause of action arose from the defendant's activities within the forum state. Helicopteros, 466 U.S. at 415. In order for a court to assert general jurisdiction, the defendant must have "continuous and systematic" contacts with the forum state. Id. at 416.

It is undisputed that defendants' business operations and retail outlets are located in South Carolina. Further, defendants have no physical presence within the state of Oregon. Defendants are not registered to conduct business in Oregon and have no registered agents, employees or sales representatives located in Oregon. No principles or personnel of defendants have ever traveled to Oregon. Defendants have never received a franchise inquiry from Oregon and have never offered a franchise to an Oregon resident or corporation. The only possible "contacts" defendant have had with Oregon include the sale of one compact disc to an Oregon resident, the purchase of inventory from an Oregon distributor and, according to plaintiff, the maintenance of an Internet Web site.

Plaintiff does not and cannot assert that any of these bases support general jurisdiction over defendants. Defendants' sale of one compact disc and sporadic purchases from a supplier are neither substantial nor "continuous and systematic" contacts with this forum. Further, the court is aware of no case in which a court asserted general jurisdiction based on the existence of an Internet Web site. In fact, a California district court declined to assert general jurisdiction on this ground. McDonough v. Fallon McElligott, Inc., 40 U.S.P.Q.2d 1826, 1996 WL 753991 (S.D. Cal. 1996). The court reasoned that "allowing computer interaction via the web to supply sufficient contacts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists." 1997 WL 753991 at *3; cf. Mieczkowski v. Mascot Corp., 997 F. Supp. 782, 785-86 (E.D. Tex. 1998) (Internet Web site plus traditional business contacts with forum created basis for general jurisdiction). Thus, the sole issue is whether the court may assert specific jurisdiction over defendants.

B. Specific Jurisdiction

Specific jurisdiction refers to a situation in which the cause of action arises directly from a defendant's contacts with the forum state. See Sher v. Johnson, 911 F.2d 1357, 1361 (1990). The Ninth Circuit employs a three-part test to determine whether the exercise of specific jurisdiction comports with due process. Ballard v. Savage, 65 F.3d 1495 (9th Cir. 1995); Roth v. Garcia Marquez, 942 F.2d 617, 620 (9th Cir. 1991). First, the defendant must perform some act or consummate some transaction within the forum by which it "purposefully avails" itself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of the forum and having "fair warning" that a particular activity may subject it to jurisdiction. See Burger King v. Rudzewicz, 471 U.S. 462, 472, 475 (1985). Second, the claim must be one which arises out of or results from the defendant's forum-related activities. Third, the court's exercise of jurisdiction must be reasonable. Ballard, 65 F.3d at 1498; Roth, 942 F.2d at 620-21.

Purposeful avowment is shown "if the defendant has taken deliberate action within the forum state or if he has created continuing obligations to forum residents." Ballard, 65 F.3d at 1498. Although contacts that are "isolated" or "sporadic" may support specific jurisdiction if they create a "substantial connection" with the forum, the contacts must be more than random, fortuitous, or attenuated. Burger King, 471 U.S. at 472-73, 475. Furthermore, it is not required that a defendant be physically present within the forum, provided its efforts are purposefully directed toward forum residents. Id. at 476. For example, jurisdiction may be properly asserted over a defendant who directs its tortious conduct toward the forum state, knowing the effects of the conduct will cause harm. Calder v. Jones, 465 U.S. 783, 789-90 (1984). However, contacts resulting from the "unilateral activity of another party or third person" are not attributable to a defendant. Burger King, 471 U.S. at 475 & n. 17. With these principles in mind, the court turns to the asserted conduct of defendants that plaintiff claims establishes minimum contacts.
with this forum.

1. Sale of Compact Disc

Plaintiff claims that defendants' sale of one compact disc to Ms. Lufkin constitutes purposeful availment of this forum, because the sale occurred after defendants "had solicited sales over the Internet in the state of Oregon." Plaintiff's Memorandum in Opposition to Defendants' Motion to Dismiss, p. 2. The court cannot agree.

During oral argument, plaintiff did not contest the fact that an acquaintance of plaintiff's counsel instructed Ms. Lufkin to purchase a compact disc from defendants. The court was gratified to learn that Ms. Lufkin, at least, was allowed to select the compact disc she was directed to purchase. Regardless, the court finds that the sale to Ms. Lufkin was nothing more than an attempt by plaintiff to manufacture a contact with this forum sufficient to establish personal jurisdiction.

Defendants cannot be said to have "purposely" availed themselves of the protections of this forum when it was an act of someone associated with plaintiff, rather than defendants' Web site advertising, that brought defendants' product into this forum. Moreover, plaintiff's claims of trademark infringement and unfair trade practices do not arise from the sale of the compact disc to Ms. Lufkin. "The gravamen of both an infringement and an unfair competition claims is whether the defendant has created a likelihood of confusion." Shakey's, Inc. v. Covalt, 704 F.2d 426, 430 (9th Cir. 1983) (citing 15 U.S.C. § 1125(a) and Or. Rev. Stat. § 646.608(1)(b)). Plaintiff can hardly argue that such action "caused a likelihood of confusion" regarding plaintiff's and defendants' trade names; Ms. Lufkin knew exactly with whom she was dealing and knew that defendants were not associated in any way with plaintiff.

The court is dismayed by plaintiff's counsel's lack of candor. In submissions to this court, including the complaint, counsel repeatedly asserted that defendants' sale of goods in Oregon had caused plaintiff harm and "ascertainable loss." Complaint, ¶ 25. However, it is clear to the court that no confusion and no harm or loss resulted from one commercial sale orchestrated by plaintiff through an acquaintance of counsel. Such questionable and unprofessional tactics cannot subject defendants to jurisdiction in this forum. "Only those contacts with the forum that were created by the defendant, rather than those manufactured by the unilateral acts of the plaintiff, should be considered for due process purposes." Edberg v. Neogen Corp., 17 F. Supp.2d 104, 112 (D. Conn. 1998).

2. Purchases from Oregon Supplier

Likewise, defendants purchases from Allegro do not suffice to establish the requisite minimum contacts. It is well-established that sporadic purchases within a forum cannot support the assertion of personal jurisdiction unless the cause of action arises from or relates to those purchases. Helicopteros, 466 U.S. at 414, 418. Plaintiff argues that its unlawful trade practices claim arises from the defendants' purchases, because confusion between plaintiff's and defendant trades' names resulted from defendants contacts with Allegro. See Or. Rev. Stat. § 646.608(1)(c). In support of this argument, plaintiff presents a credit document from Allegro that was intended for defendants but mailed to plaintiff.

Plaintiff's reliance on section § 646.608(1)(c) is misplaced. That statute defines an unlawful trade practice as including those which cause a "likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another." Or. Rev. Stat. § 646.608(c)(1). As defendants argue, the primary purpose of the Oregon Unlawful Trade Practices Act, which includes § 646.608, is to protect consumers from misleading representations regarding the source of products, thus creating a "likelihood of confusion." Shakey's, 704 F.2d at 430.

"Likelihood of confusion exists when consumers are likely to assume that a product or service is associated with a source other than its actual source because of similarities between the two sources' marks or marketing techniques." Id. (emphasis added); Kendall-Jackson Winery, Ltd. v. E. & J. Gallo Winery, 150 F.3d 1042, 1048 (9th Cir. 1998) (accord). For example, the Oregon Court of Appeals found a violation of § 646.608(1)(c) when a denturist made a misleading representation which could have led consumers to believe that the denturist was associated with a dentist. Terry v. Holden-Dhein Enterprises.
48 Or. App. 763, 767, 618 P.2d 7, 10 (1980). Under the facts presented to this court, the party allegedly confused by the parties' similar trade names is a supplier, not a consumer, of defendants' products.

Even if § 646.608(c) was intended to prohibit confusion among those other than consumers, § 646.608 does not confer a private cause of action. Or. Rev. Stat. § 646.638(1); Terry, 48 Or. App. at 768, 618 P.2d at 10. Rather, an individual action alleging a violation of 646.608(c) may only be brought if the plaintiff suffers an "ascertainable loss" as a result of the violation. Id. Here, plaintiff's assert no ascertainable loss caused by defendant's purchase of inventory from Allegro. In fact, plaintiff received a credit document, rather than an invoice, from Allegro. Accordingly, plaintiff's cause of action for unfair trade practices does not arise or relate to defendants' purchase of inventory from Allegro and cannot confer personal jurisdiction over defendants.

3. Effects of Defendants' Conduct

During oral argument, plaintiff argued that the effects of defendant's alleging infringing activities cause harm in Oregon, plaintiff's principle place of business, thus subjecting defendants to this court's jurisdiction. In support of its invocation of the "effects test," plaintiff cites Indianapolis Colts, Inc. v. Metropolitan Baltimore Football Club, 34 F.3d 410 (7th Cir. 1994). The court is not persuaded.

In Indianapolis Colts, the Canadian Football League ("CFL") team in Baltimore attempted to call itself the "Baltimore CFL Colts." 34 F.3d at 411. As anyone familiar with football knows, the "Baltimore Colts" of the National Football League ("NFL") was "one of the most illustrious teams in the history of professional football." Id. In 1984, the NFL team's owner moved the franchise to Indianapolis but kept the name "Colts." This action infuriated the city and citizens of Baltimore. Nine years later, the CFL granted a franchise in Baltimore, and the selection of the team's name, "Baltimore CFL Colts," led the Indianapolis Colts to file a lawsuit alleging trademark infringement against the Baltimore franchise and the CFL. Id.

The Seventh Circuit asserted personal jurisdiction over the defendants, because the allegedly infringing trademark would cause harm in Indiana, the home of the Indianapolis Colts. Id. at 411-412. The court further found that defendant had "entered" the state through broadcasts of football games within the state. Id. at 412.

The facts of Indianapolis Colts are distinguishable from those before this court. Given the history between the two teams, it is reasonable to assume that the defendants were directing their infringing action at Indiana, specifically at the owner of the Indianapolis Colts, knowing that their actions likely would cause harm. And, presumably, television broadcasts of football games are aired in specific market areas. Unlike Indianapolis Colts, plaintiff here offers no evidence that defendants intentionally directed its activities at Oregon knowing that plaintiff would be harmed.2

4. Defendants' Internet Web Site

Plaintiff's remaining ground asserted in support of specific jurisdiction is defendants' Internet Web site through which persons can purchase compact discs, request franchising information and join a discount club. According to plaintiff, the fact that defendants maintain an interactive, rather than passive, Web site is a sufficient contact with this forum to establish personal jurisdiction. In other words, plaintiff argues that purposeful availment is satisfied by an Internet Web site which allows for the exchange of information between the Web user and the Web site, regardless of whether an actual exchange of information occurred with residents of this forum.

The facts of this case coupled with plaintiff's argument raise questions that have yet to be answered in this Circuit. Because the answers to these questions will have far-reaching implications for those who utilize the Internet for commercial purposes, the court takes a comprehensive look at the current state of the law with respect to personal jurisdiction and Internet contacts.

III. THE INTERNET AND PERSONAL JURISDICTION
A. The Internet and the World Wide Web

The Internet is a "giant network which interconnects innumerable smaller groups of linked computer networks," American Civil Liberties Union v. Reno, 929 F. Supp. 824, 830 (E.D. Penn. 1996), aff'd 521 U.S. 844 (1997) ("ACLU v. Reno"). Some networks are "closed" to other networks, but many are connected to other computer networks so that each computer in every network can communicate with computers on any other network in the system. Id. at 831. "This global Web of linked networks and computers is referred to as the Internet." Id.

Computers and networks that comprise the system are owned by governmental and public institutions, non-profit organizations and private parties. Id. "The resulting whole is a decentralized, global medium of communications -- or 'cyberspace' -- that links people, institutions, corporations, and governments around the world." Id.

The two most common methods to connect with the Internet are the use of a computer or terminal that is directly connected to a computer network, which, in turn, is connected to the Internet, or the use of a personal computer with a modem to connect through telephone lines to a network that is connected to the Internet. ACLU v. Reno, 929 F. Supp. at 832. Students, faculty, and researchers can access the Internet through educational institutions. Id. Likewise, many corporations and other employers link their office networks to the Internet, thus providing their employees with direct or modem access to the Internet. Id. at 832-33. Those who lack access to the Internet through schools or employers often can gain access through libraries, community networks, "computer coffee shops" or commercial on-line service providers. Id. at 833.

The size of the Internet is difficult to estimate with accuracy at any given moment. ACLU v. Reno, 929 F. Supp. at 831. "It is indisputable, however, that the Internet has experienced extraordinary growth in recent years." Id. In 1989, approximately 90,000 computer were connected to the Internet; in 1996, over 9,400,000 computers worldwide were estimated to be connected. Id. These numbers do not include personal computers userd to access the Internet using modems. Id. By 1999, the number of Internet users is expected to grow to 200 million. Id.

The World Wide Web ("The Web") is the most well-known and advanced method of locating and retrieving information on the Internet. ACLU v. Reno, 929 F. Supp. at 835-36. The Web utilizes a specific formatting language so that programs which search the Web can display documents containing text, image, sound and video. Id. at 836. Any Web document can include links, known as "hyperlinks," to other types of information or resources, which can be used by clicking the computer mouse on the hyperlink which immediately connects the user to the other resource. Id. "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." Id.

Many organizations and businesses now have "home pages" or "sites" on the Web. ACLU v. Reno, 929 F. Supp. at 836. "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." Id. When an organization wants information made available, it is "published" on the Web. Id. at 837.

The Web contains information from a variety of sources and is accessible to Internet users around the world. Id. at 835-36. "Anyone with a personal computer, a telephone modem, and appropriate computer software may gain access to the Internet." Heroes, Inc. v. Heroes Foundation, 958 F. Supp. 1, 4 (D.D.C. 1996). Once connected to the Internet, the user may view Web pages "which provide information about almost anything one can imagine." Id. Likewise, the Internet "enables anyone with the right equipment and knowledge . . . to operate an international business cheaply, and from a desktop." Compuserve v. Patterson, 89 F.3d 1257, 1262 (6th Cir. 1996).

While the Internet allows businesses to engage in international communication and commerce, those businesses -- whether they be one-person operations or multi-national corporations -- remain "entitled to
the protection of the Due Process Clause, which mandates that potential defendants be able 'to structure their primary conduct with some minimum assurance as to where the conduct will and will not render them liable to suit.' Id., quoting World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980). As the Second Circuit has recognized, however, "attempting to apply established trademark law in the fast-developing world of the Internet is somewhat like trying to board a moving bus . . . ." Bensusan Restaurant Corp. v. King, 126 F.3d 25, 27 (2d Cir. 1997). The court finds the same is true when attempting to apply traditional notions of personal jurisdiction.

Unlike newspaper, mailing, radio, television and other media containing advertisements and solicitations, most Internet advertisements and solicitations are not directed at a specific geographic areas or markets; to the contrary, advertising on the Internet targets no one in particular and everyone in particular in any given geographic location. At first glance, the question of personal jurisdiction in such scenarios seems an all or nothing proposition. Nevertheless, district courts -- and to a lesser extent, circuit courts -- have attempted to develop guidelines in this novel area of the law, although "the development of the law concerning the permissible scope of personal jurisdiction is in its infant stages." Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123 (W.D. Penn. 1997).

B. Cases Interpreting Internet Contacts

One of the first cases to address the question of personal jurisdiction and the Internet was Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996). In that case, the plaintiff alleged trademark infringement as a result of the defendant's alleged use of plaintiff's trademark as its Internet domain address. 937 F. Supp at 163. The defendant did not have employees or offices or conduct business regularly within the forum state. Id. at 162-63. Rather, the plaintiff claimed that the defendant's Internet Web site, which contained advertising and a toll-free telephone number, constituted sufficient minimum contacts for purposes of federal due process. Id. at 164-65.

In discussing the defendant's Web site, the court remarked:

In the present case, [defendant] has directed its advertising activities via the Internet and its toll-free number toward not only the state of Connecticut, but to all states. The Internet as well as toll-free numbers are designed to communicate with people and their business in every state. Advertisements on the Internet can reach as many as 10,000 Internet users within Connecticut. Further, once posted on the Internet, unlike radio and television advertising, the advertisement is available continuously to any Internet user.

Id. at 165. Although these findings tend to show that the defendant did not target its Web site at the forum state in any particular manner, the court concluded that, through its Web site, defendant had "purposefully availed itself of the privilege of doing business within Connecticut." Id.

From this rather inauspicious beginning, the trend has shifted away from finding jurisdiction based solely on the existence of Web site advertising. Instead, "something more" is required to show that the defendant purposefully directed its activities at the forum. See Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 418 (9th Cir. 1997). After Inset, two district courts endeavored to set standards the majority of courts now have adopted.

In Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), affd 126 F.3d 25 (2d Cir. 1997), the operator of a New York jazz club, Bensusan, brought suit against the owner of a small Missouri jazz establishment, King, claiming that King infringed on Bensusan's right to the trademark "The Blue Note." Bensusan alleged that jurisdiction over King was properly asserted in New York, because King maintained a Web site that was accessible to New York residents. Id. at 299. The court disagreed: "The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York." Id.

The court further found that assertion of jurisdiction over King would violate the Due Process Clause, reasoning that King had not purposefully availed himself of the benefits of New York when he "simply
created a Web site and permitted anyone who could find it to access it." Id. at 301. "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." Id. Finally, the court found Bensunan's argument "that King 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" did not satisfy the requirements of due process. Id.

In Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123 (W.D. Penn. 1997) ("Zippo"), the plaintiff alleged trademark dilution and infringement based on the defendant's Web site domain names. 952 F. Supp. at 1121. In determining whether jurisdiction was proper, the court applied a "sliding scale" under which "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." Id. at 1124.

At one end of the scale are circumstances where a defendant "conducts business" over the Internet with residents of the forum, allowing for the assertion of personal jurisdiction in most cases. Zippo, 952 F. Supp. at 1124. In such situations, the assertion of jurisdiction is almost always proper. At the opposite end are situations where a defendant simply posts information on a Web site which is accessible to users in the forum state as well as others. "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 of personal jurisdiction." Id. In the middle are situations where a defendant operates an interactive Web site, allowing a user to exchange information with the host computer. In such a case, a court must review the "level of interactivity and commercial nature of the exchange of information" to determine whether jurisdiction should be exercised. Id.


Likewise, courts generally have exercised jurisdiction in cases at the other end of the scale, where the defendant "conducted business" over the Internet by engaging in repeated or ongoing business transactions with forum residents or by entering into a contract with the plaintiff through the Internet. See CompuServe v. Patterson, 89 F.3d 1257 (6th Cir. 1996); Thompson v. Handa-Lopez, Inc., 998 F. Supp. 738 (W.D. Tex. 1998) (defendant operated casino-type arcade game through its Web site and entered into contract with plaintiff to play the game); Zippo, 952 F. Supp. at 1125-26 (defendant contracted with approximately 3,000 individuals and several Internet access providers in the forum state).

Further, courts have found purposeful availment when the claim involves an intentional tort allegedly committed over the Internet, such that the defendant intentionally directed its tortious activities at the forum state. See Panavision v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) (tortious infringement of trademark where the defendant knew actions would cause plaintiff harm in forum state); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (defamatory statements on Internet site); Telco Communications
at forum). These cases are based on the "effects test" articulated in Calder v. Jones, 465 U.S. 783, 
788-90 (1984), where the Supreme Court found personal jurisdiction properly asserted over a defendant 
whose libelous actions were directed at the plaintiff resident of the forum state. See also Sinatra v. 
National Enquirer, Inc., 854 F.2d 1191, 1195-97 (9th Cir. 1988) (defendant fabricated elaborate story 
linking plaintiff's name with services).

Courts have reached differing conclusions with respect to those cases falling into the middle 
"interactive" category identified in Zippo. As declared by one commentator, the "current hodgepodge of 
this case law is inconsistent, irrational, and irreconcilable." Howard B. Stravitz, Personal Jurisdiction in 
Cyberspace: Something More is Required on the Electronic Stream of Commerce, 49 S.C. L. Rev. 925, 
939 (1998). In these cases, some courts find that an interactive Web site alone is sufficient to establish 
minimum contacts. Others find minimum contacts through additional non-Internet activity in the forum, 
regardless of whether the activity is related to the underlying claim. Finally, some courts require 
additional conduct in the forum that is related to the plaintiff's cause of action.

1. Interactive Web Site

a. Personal Jurisdiction Asserted

A case oft-cited for the proposition that interactive Web sites constitute minimum contacts is Maritz, 
Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996). In that case, the defendant maintained a 
Web site that invited users to a join mailing list in order to receive information about defendant's service. 
947 F. Supp at 1330. The court rejected the defendant's characterization of the Web site as "passive," 
noting that users could join the mailing list and receive information through the Web site. Id. at 1333. 
Indeed, the court rested jurisdiction on the fact that the defendant "consciously decided to transmit 
advertising information to all Internet users, knowing that such information will be transmitted 
globally." Id. at 1333. The court did not examine whether any resident of the forum actually had signed 
the mailing list or received information from the defendant as a result; rather, the court found that 
defendants' mailing list will "presumably includ[e] many residents of Missouri" and noted that forum 
residents had accessed the site 131 times. Id. at 1330. See also Superguide Corp. v. Kegan, 987 F. Supp. 
481 (W.D.N.C. 1997) (the court "assumed" residents of forum had accessed defendant's Web site and 
utilized defendant's commercial services).

In GTE New Media Services Inc. v. Americtech Corp., 21 F. Supp. 2d 27 (D.D.C. 1998), the court 
asserted jurisdiction over companies providing national "Yellow Pages" directory services over the 
Internet. The plaintiff alleged that the defendants formed agreements with Web browsers "to prevent 
users from accessing their competitors' websites through essential Internet access points." 21 F. Supp.2d 
at 37. The court found the Web sites highly interactive and the quality and nature significant so as to 
allow the assertion of personal jurisdiction. Id. at 38-39. The court also emphasized that the defendants 
derived substantial advertising revenues from the directory sites when residents of the forum accessed 
and utilized the defendants' Internet Yellow Pages. Id.

Finally, in Vitullo v. Velocity Powerboats, Inc., 1998 WL 246152 (N.D. Ill. 1998), the court found that 
the defendant's Internet Web site provided the contact necessary to assert specific jurisdiction under a 
stream of commerce theory in a products liability action. Defendants' Web site solicited residents to 
attend their "local boat show" and view defendants' boats and provided a hyperlink with information 
about a boat show within the forum state. Id. at *6. The court found that the Web site thus targeted local 
residents: "It is logical to say that a 'national advertisement' available to all persons with access to the 
Internet may take on a 'local' characteristic when it expressly solicits local residents, as does the Velocity 
web page." Id. at *7.

b. Personal Jurisdiction Declined

The following courts declined to assert personal jurisdiction over the defendant based solely on the 
defendant's interactive web site.
In Edberg v. Neogen, 17 F. Supp.2d 104 (D. Conn. 1998), the defendant's Web site allowed users to order product information and send electronic mail to defendant's representatives. The court found that no evidence suggested that any user in the forum state accessed the defendant's Web site or purchased products based on the Web site. Further, nothing suggested that the defendant directed its Web site at residents of the forum "anymore than anyplace else in the nation." Id. at 113-14.

A similar result occurred in E-Data Corp. v. Micropatent Corp., 989 F. Supp. 173 (D. Conn. 1997). In that case, the defendant operated a Web site where users could purchase, license, and download photography images. The defendant claimed it had no knowledge of the geographic location of any given customer. In response, the plaintiff failed to offer any evidence that defendant's advertising ever reached Connecticut, "i.e., that any Connecticut resident ever accessed" defendant's Web site. Id. 176 n.2. Rather, plaintiff simply showed the potential for the defendant to reach and solicit forum residents by its "offer to sell" photography images. The court rejected plaintiff's argument: "If such potentialities alone were sufficient to confer personal jurisdiction over a foreign defendant, any foreign corporation with the potential to reach to do business with Connecticut consumers by telephone, television or mail would be subject to suit in Connecticut." Id. at 177.

In Scherr v. Abrahams, 1998 WL 299678 (N.D. Ill. 1998), the court found that defendant's Web site was interactive because it allowed the user to type in an e-mail address and receive a copy of a publication in return. Id. *5. In contrast with Maritz, the court declined to assert jurisdiction, because the level of interactivity was low and the site was not targeted specifically at forum residents. Id.

Finally, in CD Solutions v. Tooker, 965 F. Supp. 17 (N.D. Tex. 1997), the court declined to assert specific jurisdiction on the grounds that the plaintiff's claims did not relate to the defendants' contacts with Texas. Id. at 20. The plaintiff sued the defendant over defendants' use of the domain name "cds.com" for their Web page on the Internet. Id. at 19. Both plaintiff and defendants advertised and sold their services over the Internet. Id. Nonetheless, the court found no connection between the defendants' asserted commercial efforts and the core question underlying the action, which was whether defendants' had infringed upon copyrights owned by the plaintiff. Id. at 20.

2. Interactive Web Site Plus Non-Internet Contacts

In Hasbro, Inc. v. Clue Computing, Inc., 994 F. Supp. 34 (D. Mass. 1997), the plaintiff sued the defendant, a small computer consulting company, for trademark infringement in connection with the defendant's use of the domain name "clue.com" for its Internet Web site. Initially, the court reasoned that "imposing traditional concepts on commercial Internet users might have dramatic implications, subjecting them to nationwide or even international jurisdiction." Id. at 39. Nevertheless, the court asserted specific jurisdiction over defendant based, in part, on defendant's Web site, which allowed users to send e-mail to the company, explaining, "Clue Computing's Web site is interactive, encouraging and enabling anyone who wishes, including Massachusetts residents, to send e-mail to the company." Id. at 45.

The court also deemed jurisdiction proper based on defendant's non-Internet activities, including services performed for a Massachusetts company. Id. In doing so, the court apparently took a "totality of the contacts" approach and considered contacts unrelated to plaintiff's claim. Although defendant's Web-related activities were related to the trademark action--indeed, were the nexus of the litigation--defendant's computer consulting work with a Massachusetts company was completely unrelated to the trademark action.

A different analysis was presented in Mieczkowski v. Masco Corp., 997 F. Supp. 782 (E.D. Tex 1998), where the court found defendant's minimal sales in the forum through traditional methods, along with its interactive Web site, constituted continuous and systematic contacts with the forum to support the assertion of general jurisdiction in a products liability case. Id. at 787. The court explicitly declined to decide "whether standing alone the Web site maintained by the defendant is sufficient to satisfy a finding of general jurisdiction." Id. at 788. But see Fernandez v. McDaniel Controls, Inc., 999 F. Supp. 1365, 1368 (D. Hawaii 1998) (refusing to assert specific jurisdiction in products liability case based on
defendant's passive Web site and shipments of product to forum at request of distributor).

3. Interactive Web Site Plus Related Contacts

In Park Inns International v. Pacific Plaza Hotels, Inc., the defendants operated an interactive Web site and accepted hotel reservations from residents of the forum through the Web site. 5 F. Supp.2d 762, 764-65 (D. Ariz. 1998). Reviewing a recent Ninth Circuit decision, the court found that purposeful availment is shown if the defendant transacted business with forum residents over the Internet. Id. at 763 (citing Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997). Thus, the court exercised specific jurisdiction over the defendants.

Similarly, in American Network, Inc. v. Access America/Connect Atlanta, Inc., 975 F. Supp. 494 (S.D.N.Y. 1997), the court found purposeful availment because the defendant sold subscriptions for Internet services to residents of the forum state and entered into contracts with those residents through its Web site. Id. at 499. In so ruling, the court questioned whether the mere existence of an interactive Web site may suffice for personal jurisdiction, reasoning that "arguably a defendant should not be subject to jurisdiction in New York simply because its home page could be viewed by users there." Id. at 498-99. Instead, the court relied on the fact that the defendant had entered into contracts with residents of New York that were related to plaintiff's cause of action for trademark infringement. Id.

In yet another case, the court asserted jurisdiction over a defendant accused of breaching a trademark licensing agreement with the plaintiff. Digital Equipment Corp. v. AltaVista Technology, Inc., 960 F. Supp. 456 (D. Mass. 1997). The plaintiff claimed that the defendant's Web site breached the licensing agreement between the parties, which governed the defendant's use of plaintiff's trademark on its Internet Web site. Id. at 459-61. Accordingly, the court found that the defendant had purposely availed itself of the benefits of the forum by entering into an agreement with the resident of the forum. Id. at 468-69. The court further noted that the defendant sold products to Massachusetts residents on at least three occasions through its Web site. Id. at 464. Finally, the defendant's alleged infringement was found analogous to intentional tortious conduct in that it was "purposefully directed" at plaintiff, whom defendant knew to reside in Massachusetts. Id. at 470. The court emphasized that "[t]here is no issue of parties being haled into the courts of a given jurisdiction solely by virtue of a Web-site, without meaningful notice that such an outcome was likely." Id. at 463.

C. Ninth Circuit Case Law

The Ninth Circuit is one of the few circuits which has jumped in the fray of Internet contacts and personal jurisdiction. Although the two cases decided by the Circuit are factually distinct from the one before this court, both rulings provide valuable guidance toward its resolution.

The Ninth Circuit has cited with approval the "sliding scale" approach articulated in Zippo. Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997). Arizona plaintiffs ("Cybersell AZ") and Florida defendants ("Cybersell FL") both formed corporations known as "Cybersell." Cybersell AZ provided Web advertising, marketing and consulting services. Cybersell FL provided business consulting services for strategic management and marketing on the Web. As part of its marketing effort, Cybersell FL created a Web page which included the "Cybersell" logo, a local phone number, an invitation to send electronic mail, and a hypertext link through which users could introduce themselves. Eventually, Cybersell AZ filed suit in the District of Arizona for trademark infringement. The district court dismissed the case for lack of personal jurisdiction. The Ninth Circuit affirmed.

In considering the purposeful availment factor, the court remarked:

[N]o court has ever held that an Internet advertisement alone is sufficient to subject the advertiser to jurisdiction in the plaintiff's home state... 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.

Cybersell, 130 F.3d at 418. The court found that Cybersell FL conducted no commercial activity over
the Internet in Arizona and that its Web page was "an essentially passive home page." Further, the court noted that Cybersell had no contact with Arizona over the Internet other than messages from Cybersell AZ. "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." Id. at 419.

Recently, the Ninth Circuit reiterated its reasoning set forth in Cybersell. Panavision International v. Toeppen, 141 F.3d 1316 (9th 1998). In Panavision, the defendant registered established trademark names as domain names for his Web sites, then attempted to "sell" the rights to the domain name to the holder of the trademark. 141 F.3d at 1319, 1322. The defendant argued that he had no contacts with the forum state, because he had not directed any activity toward or entered the state. The Ninth Circuit disagreed:

Toeppen engaged in a scheme to register Panavision's trademarks as his domain names for the purpose of extorting money from Panavision. His conduct, as he knew it likely would, had the effect of injuring Panavision in California where Panavision has its principle place of business and where the movie and television industry is centered.

Id. at 1322. With these principles in mind, the court turns to the facts of this case.

IV. ANALYSIS OF DEFENDANTS' INTERNET CONTACTS

The court first determines where defendants' Web site corresponds on the sliding scale of interactivity. Through defendants' Web site, Web users may purchase compact discs, join a discount club and request franchising information. Affidavit of Lawrence M. Verdun, Ex. A.

Arguably, the capability of selling compact discs through the Web site could constitute "doing business" over the Internet and confer personal jurisdiction almost as a matter of course. However, the court finds such designation intended for those businesses which conduct a significant portion of their business through ongoing Internet relationships; for example, by entering "into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet" Zippo, 952 F. Supp. at 1124; see also Thompson v. Handa-Lopez, 998 F. Supp. at 744.

An example of such business is found in Compuserve v. Patterson, 89 F.3d 1257 (6th Cir. 1996). In that case, the defendant was a subscriber of plaintiff's Internet provider services and entered into an agreement with plaintiff under which the defendant electronically transmitted 32 software files to plaintiff, a corporation located in Ohio. Id. at 1261. The Sixth Circuit found that the defendant "purposefully availed" himself of the privilege of doing business in Ohio by purposefully contracting with the plaintiff and utilizing the plaintiff's services to market his products. Id. at 1264.

Here, defendants have done nothing more than publish an interactive Web site. Defendants have not purposefully entered into contracts with Oregon residents through the Internet, other than Ms. Lufkin, nor have defendants otherwise exchanged files electronically with forum residents so as to create "repeated" or "ongoing obligations." See Burger King, 471 U.S. at 473 (defendants who "reach out beyond one state and create continuing relationships and obligations with citizens of another state" are subject to jurisdiction). Accordingly, defendants do not "conduct business" in Oregon over the Internet so as to fall under the first category in Zippo.

Neither is defendants' Web site at the other end of the spectrum, passively providing information for those interested. Rather, an exchange of information can occur between defendants and Web users. Thus, defendants' Web site falls into the middle category, requiring further inquiry into the "level of interactivity and commercial nature of the exchange of information" to determine whether jurisdiction should be exercised. Zippo, 952 F. Supp. at 1124.

Plaintiff contends that the nature of defendants' Web site confers jurisdiction; the crux of plaintiff's argument is that defendants' Web site solicits potential Oregon consumers and therefore constitutes purposeful availment of this forum. Thus, plaintiff urges the court to adopt the broad view of personal jurisdiction set forth in Inset and Maritz with respect to Internet Web sites. The court declines to do so.
On its face, defendants' Web site would appear to suffice for personal jurisdiction under the middle category in Zippo; the level of potential interactivity, while not necessarily high, is not insubstantial. Further, the potential exchange of information can be commercial in nature. However, the court finds that the middle interactive category as described in Zippo needs further refinement to include the fundamental requirement of personal jurisdiction: "deliberate action" within the forum state. Ballard, 65 F.3d at 1498. Such action could include transactions between the defendant and forum residents through the defendant's Web site or conduct of the defendant purposefully directed at residents of the forum state through the Web site. See Panavision, 141 F.3d at 1322; see also Calder, 465 U.S. at 788-90. This, in the court's view, is the "something more" that the Ninth Circuit intended in Cybersell and Panavision.

Although Cybersell involved an "essentially" passive home page, the court's reasoning easily applies in this case. In declining to assert jurisdiction, the court noted:

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. . . . 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.

Cybersell, 130 F.3d at 419. Although the court noted the lack of commercial activity associated with the defendant's Web site, the court concluded: "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." 1d. In other words, "simply registering someone else's trademark as a domain name and posting a web site on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another." Panavision, 141 F.3d at 1322.

Here, defendants have "consummated no transaction" and have made no "deliberate and repeated" contacts with Oregon through their Web site. Compserve v. Patterson, 89 F.3d at 1265. Defendants maintain a Web site which allows users to purchase products, thus rendering it foreseeable that residents of Oregon, or any other state or country for that matter, could purchase a product from defendants. However, it is well-established that foreseeability alone cannot serve as the constitutional benchmark for personal jurisdiction. "The foreseeability that is critical to due process analysis is not the mere likelihood that a product will find its way into the forum state. Rather, it is that the defendant's conduct and connection with the forum state are such that he should reasonably anticipate being haled into court there." World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

Defendants' Internet Web site, interactive though it may be, is not "conduct and connection" with Oregon giving defendants "fair warning" so that they would reasonably anticipate being "haled" into court here. Defendants have not taken action creating "a substantial connection" with Oregon, or deliberately engaged in "significant activities" within Oregon, or created "ongoing obligations" with residents of Oregon in a manner related to plaintiff's claims. See Burger King, 471 U.S. at 473, 475-76. Rather, defendants have published information on an Internet Web site that is accessible to whomever may find it. See Bensusan, 937 F. Supp. at 301. The fact that someone who accesses defendants' Web site can purchase a compact disc does not render defendants' actions "purposefully directed" at this forum. Id; see also Edberg, 17 F. Supp.2d at 133-14; Park Inns, 5 F. Supp.2d at 763 (interpreting and applying Cybersell); E-Data, 989 F. Supp. at 177. It is the conduct of the defendants, rather than the medium utilized by them, to which the parameters of specific jurisdiction apply. World-Wide Volkswagen, 444 U.S. at 297.

Furthermore, plaintiff offers no evidence that defendants targeted Oregon residents with the intent or knowledge that plaintiff could be harmed through their Web site. The Ninth Circuit rejected this notion with respect to the "effects test" in Cybersell, a case involving alleged trademark infringement. The Arizona plaintiff had argued that the effects of the defendants' infringing Internet caused injury in Arizona. The Ninth Circuit disagreed: "Cybersell FL's web page simply was not aimed intentionally at Arizona knowing that harm was likely to be caused there to Cybersell AZ." Cybersell, 130 F.3d at 420;
6

see also Panavision v. Toeppen, 143 F.3d 1316, 1322 (9th Cir. 1998) (comparing harm caused by intentional tortious conduct directed at forum to the harm alleged in Indianapolis Colts; Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328, 1331 (E.D. Mo. 1996) (alleged economic harm in forum state insufficient to establish minimum contacts absent additional conduct). Likewise, plaintiff makes no showing that defendants' Web page was "aimed intentionally" at Oregon.

A review of defendants' Web site furthers the conclusion that defendants did not intentionally or purposefully target its activities at Oregon. The site proclaims "Come Visit Us!" and provides a map of the location of defendants' stores. The maps are local in nature, providing little more than a showing of the cross-streets surrounding the stores. Nothing published on the Web site suggests that defendants intended to target Oregon residents, some 3,000 miles away, any more than they intended to target residents of other states. Rather, from defendants' invitation to visit their retail outlets, one could reasonably infer that defendants intended to target residents in their area. In sum, the court finds that this, too, is a case where "something more" is required. Cybersell, 130 F.3d at 418.

The court recognizes that its reasoning is at odds with some district courts addressing this new issue. Not surprisingly, plaintiff relies on Inset and Maritz for the proposition that jurisdiction over the operator of a Web site is proper if the site is interactive, i.e., capable of exchanging information with the computer user. However, the court finds lacking in Inset and Maritz the principle that a defendant must "purposefully direct" its activities at or take "deliberate action" in or create "substantial connection" with the forum state so as to provide "fair warning" that such activities may subject defendant to jurisdiction in a distant forum. See Burger King, 471 U.S. at 472.

The existence of a Web site, whether passive or interactive, does not rise to the requisite level of conduct. Publishing a Web site requires no "deliberate" action within the forum state. Furthermore, a Web site is not automatically projected to a user's computer without invitation as are advertisements in a newspaper or on the television and radio. Rather, the user must take affirmative action to access either a passive or interactive Web Site. The user must turn on a computer, access the Internet and the Web, and browse the Web for a particular site. Thus, contrary to the scenario described in Inset, information published on Web sites is not thrust upon users indiscriminately.

Likewise, the court declines to adopt the reasoning in cases like Hasbro v. Clue Computing, where contacts unrelated to the plaintiff's claim are considered in conjunction with a Web site in order to assert specific jurisdiction. Hasbro, 994 F. Supp. at 45. Specific jurisdiction is not proper unless the forum-related contacts give rise or relate to the plaintiff's cause of action. Ballard, 65 F.3d at 1498. Accordingly, the court does not consider defendants' purchases from Allegro in conjunction with their Internet site for purposes of personal jurisdiction analysis. Those purchases do not give rise or relate to plaintiff's claims of trademark infringement and unfair competition.9

Rather, the court views the better approach as that taken by the courts which refused to assert jurisdiction on the sole basis of an interactive Web site, see E-Data, 989 F. Supp. at 177, and finds most persuasive the reasoning of those which required contacts with forum residents relating to the plaintiff's claim. See Park Inns, 5 F. Supp. at 764-65; American Network, 975 F. Supp. at 498-99; Digital Equipment, 960 F. Supp. at 468-69. The court also agrees with the reasoning of those courts which have asserted jurisdiction on the basis that the defendant's Internet conduct was intended to reach residents of the forum. See Panavision, 141 F.2d at 1322; Vitullo, 1998 WL 246152 at *6-7 (Web site targeted at local residents); cf. Scherr, 1998 WL 299678 at *5 (declining to assert jurisdiction because Web site not targeted at forum residents).

* * * * * * * *

Absent actual exchanges or transactions with residents of the forum or evidence that local residents were targeted, the distinctions between specific and general jurisdiction become blurred. As the courts in Inset and Maritz point out, Web sites are accessible day and night to all who possess the necessary technological know-how and equipment. Thus, if an interactive Web site can constitute "purposeful availment" of a forum simply by being continuously accessible to residents of that forum, surely that contact can be considered "continuous and systematic" for purposes of general jurisdiction. Taking this reasoning to its logical conclusion, a plaintiff could sue a foreign defendant in any forum and claim jurisdiction based on the defendant's interactive Web site, even if the cause of action is unrelated to the
Web site. Such results hardly conform with notions of "fair play and substantial justice." International Shoe, 326 U.S. at 320. The grasp of personal jurisdiction was never intended to reach so far and so wide.

Moreover, the imposition of broad territorial concepts of personal jurisdiction on the commercial uses of the Internet has dramatic implications, "opening the Web user up to inconsistent regulations throughout fifty states, indeed, throughout the globe." Digital Equipment, 960 F. Supp. at 463 (internal quotation marks and citations omitted); see also Hearst, 1997 WL 9709 at *20. The possibility of such overreaching jurisdiction raises the specter of "dramatically chilling what may well be the most participatory marketplace of mass speech that this country--and indeed the world--has yet seen." Id. Businesses offering products through the Internet, particularly small businesses, might forego this efficient and accessible avenue of commerce if faced with the "litigious nightmare of being subject to suit" in every jurisdiction in this country. See Donnie L. Kidd, Jr., Casting the Net: Another Confusing Analysis of Personal Jurisdiction and Internet Contacts in Telco Communications v. An Apple a Day, 32 U. Rich. L. Rev. 505, 541 (1998).

For all of these reasons, this court will not abandon the basic principle that defendants must have taken some action to direct their activities in the forum so as to "purposely avail" themselves of the privilege of doing business within Oregon. The timeless and fundamental bedrock of personal jurisdiction assures us all that a defendant will not be "haled" into a court of a foreign jurisdiction based on nothing more than the foreseeability or potentiality of commercial activity with the forum state. World-Wide Volkswagen, 444 U.S. at 297. Until transactions with Oregon residents are consummated through defendants' Web site, defendants cannot reasonably anticipate that they will be brought before this court, simply because they advertise their products through a global medium which provides the capability of engaging in commercial transactions. It is therefore "presumptively . . . unreasonable to require [them] to submit to the burdens of litigations" in this forum. Burger King, 471 U.S. at 476.

CONCLUSION

Due process requires that personal jurisdiction be based first and foremost on fairness. If defendants do not have "fair warning" that their Internet activities would render them subject to jurisdiction in this forum, personal jurisdiction may not be had, regardless of other considerations:

Even if the defendant would suffer minimal or no inconvenience from being forced to litigate before the tribunals of another State; even if the forum State has a strong interest in applying its law to the controversy; even if the forum State is the most convenient location for litigation, the Due Process Clause, acting as an instrument of interstate federalism, may sometimes act to divest the State of its power to render a valid judgment.

World-Wide Volkswagen Corp., 444 U.S. at 294.

Plaintiff fails to show that defendants have sufficient minimum contacts with this forum to allow the exercise of personal jurisdiction in accordance with federal due process. Therefore, defendants' Motion to Dismiss (doc. 21) is GRANTED and all pending motions are DENIED as moot. Plaintiff's Complaint is HEREBY DISMISSED.

IT IS SO ORDERED.

Dated this ___ day of January, 1999.

Ann Aiken
United States District Judge

---

1Rules 4C and 4D authorize personal jurisdiction as follows: 4C Local act or omission: In any action claiming injury to person or property within or without this state arising out of an act or omission within this state by the defendant. 4D Local injury; foreign act: In any action claiming injury to person or property within this state arising out of an act or omission outside this state by the defendant, provided in addition that at the time of the injury, either:
D(1) Solicitation or service activities were carried on within this state by or on behalf of the defendant; or

D(2) Products, materials, or things distributed, processed, serviced, or manufactured by the defendant were used or consumed within this state in the ordinary course of trade.

2 Plaintiff urges the court to infer that defendants' knew of plaintiff's existence in Oregon for the purposes of this motion. Even assuming that is true, plaintiff offers no evidence that defendants directed their conduct at this forum.

The "something more" identified in Cybersell apparently is a reference to the plurality opinion in Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102 (1992), where the Supreme Court split over the requirements for application of the stream of commerce theory. In an opinion written by Justice O'Connor, four justices endorsed the view that the "placement of a product in the stream of commerce, without more, is not an act the defendant purposefully directed toward the forum State." Id. at 112 (emphasis added).

The Ninth Circuit tentatively has adopted the plurality opinion in Asahi, noting that "[a]t least a majority and perhaps all the justices agreed in Asahi that jurisdiction cannot be founded on the mere presence of a product in the forum . . . ." Omeluk v. Lansten Slip & Batbyggeri A/S, 52 F.3d 267, 271 (9th Cir. 1995).

Many cases find the "stream of commerce" theory of specific jurisdiction analogous to Web-site advertising, in that the person or business operating the site creates it for use and viewing on the Internet with the hope, if not the expectation, that users will access the site and learn about the company's products or services. See Smith v. Hobby Lobby Stores, Inc., 968 F. Supp. 1356, 1362-65 (W.D. Ark. 1997); Bensusan Restaurant Corp., 937 F. Supp. 295, 301 (S.D.N.Y. 1996).

4 It is unclear whether the court exercised specific or general jurisdiction over the defendants. The court found that "the continuous contact the defendants' interactive website have with the [forum] demonstrate the defendants purposefully established minimum contacts by invoking the benefits and privileges of conducting activities in the forum district." 21 F. Supp.2d at 39. Thus, it appears that the court found "purposeful availment" to establish specific jurisdiction through "continuous" activity, normally a basis for general jurisdiction.

The court is not convinced that plaintiff's claims arise from or relate to defendants' Internet Web site. It seems to the court that plaintiff's claims for trademark infringement and unfair competition do not depend on defendants' Web site. See CD Solutions v. Tooker, 965 F. Supp. 17 (N.D. Tex. 1997). However, the court need not reach this question because it finds that defendants' Web site does not constitute purposeful availment of this forum.

---

PERKINS COIE LLP

Home | About Perkins Coie | Attorney Directory | Practice Areas | Recruiting
Resource Center | New Content | WebReleases | Webmaster | Search Our Web Site

Last Updated 1/13/99
©1999 Perkins Coie LLP
Legal Notice
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.;
BIBLIODYTES, 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,

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
the majority 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). This
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
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 Int'l 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." Fucker Anthony Realty Corp. v. Schlesinger, 888 F.2d 569, 975 (2d Cir. 1989). Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury. C & A Carbone, 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 Youncer 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. Rv. 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 sado masochistic 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 the challenged 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). 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 Newfound, 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, 32 S. 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, "exceeded 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. . . . [B]ooksellers 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 noncensored materials 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.

(Teicher 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 "extraterritoriality" 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 quoting 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 refinshed 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 refinshed 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 
wellfare 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 
executing 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 
("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. 
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. denied, 340 U.S. 929 (1951).

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.

Wabash, St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557, 574-75 (1886). The Court in Wabash 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 transmission 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 York10 -- 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 Hershler Aff't ("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 Hershler Aff't ("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 siced 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. 93).

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 Commission, 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 unsupportable 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 sadomasochistic 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.")
NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION
SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION

STEVEN J. CASPI, RONALD W. JONAS, ARDEN JEFFREY CONE III, and
LAUREL BARRIE, On Behalf of Themselves and All Others Similarly Situated,
Plaintiffs-Appellants,
v.
THE MICROSOFT NETWORK, L.L.C., and MICROSOFT CORPORATION,
Defendants-Respondents.

A-2182-97T5

Argued: January 5, 1999 -- Decided: July 2, 1999

Before Judges Long, Kestin and Weing.

On appeal from the Superior Court of New Jersey, Law Division, Civil Part, Bergen County.

The opinion of the court was delivered by

KESTIN, J.A.D.

We are here called upon to determine the validity and enforceability of a forum selection clause contained in an online subscriber agreement of the Microsoft Network (MSN), an online computer service. The trial court granted defendants' motion to dismiss the complaint on the ground that the forum selection clause in the parties' contracts called for plaintiffs' claims to be litigated in the State of Washington. Plaintiffs appeal. We affirm.

The amended class action complaint[1] The "first amended complaint" was filed on March 5, 1997. in eighteen counts sought diverse relief against two related corporate entities, The Microsoft Network, L.L.C. and Microsoft Corporation (collectively, Microsoft).[2] Plaintiffs asserted various theories including breach of contract, common law fraud, and consumer fraud in the way Microsoft had "rolled over" MSN membership into more expensive plans. Among the claims was an accusation that Microsoft had engaged in "unilateral negative option billing," a practice condemned by the attorneys general of twenty-one states, including New Jersey's, with regard to a Microsoft competitor, America Online, Inc. Under the practice as alleged, Microsoft, without notice to or permission from MSN members, unilaterally charged them increased membership fees attributable to a change in service plans.

The four named plaintiffs are members of MSN. Two reside in New Jersey; the others in Ohio and New York. Purporting to represent a nationwide class of 1.5 million similarly aggrieved MSN members,

Shortly thereafter, defendants moved to dismiss the amended complaint for lack of jurisdiction and improper venue by reason of the forum selection clause which, defendants contended, was in every MSN membership agreement and bound all the named plaintiffs and all members of the class they purported to represent. That clause, paragraph 15.1 of the MSN membership agreement, provided:

This agreement is governed by the laws of the State of Washington, USA, and you consent to the exclusive jurisdiction and venue of courts in King County, Washington in all disputes arising out of or relating to your use of MSN or your MSN membership.

Plaintiffs cross-moved, *inter alia*, to strike a certification submitted in support of defendants’ motion to dismiss and to compel the deposition of the certificant.

On November 13, 1997, Judge Fitzpatrick, in a written opinion, expressed his reasons for dismissing the complaint based upon the forum selection clause. Given that conclusion, plaintiffs’ cross-motions were denied perforce, and plaintiffs’ motion to certify the class was denied as moot. Conforming orders were entered on the same date. On December 19, 1997, Judge Fitzpatrick entered an order modifying a passage in his November 13 opinion.

The background of the matter was depicted in the amended opinion:

Before becoming an MSN member, a prospective subscriber is prompted by MSN software to view multiple computer screens of information, including a membership agreement which contains the above clause. MSN’s membership agreement appears on the computer screen in a scrollable window next to blocks providing the choices "I Agree" and "I Don't Agree." Prospective members assent to the terms of the agreement by clicking on "I Agree" using a computer mouse. Prospective members have the option to click "I Agree" or "I Don't Agree" at any point while scrolling through the agreement. Registration may proceed only after the potential subscriber has had the opportunity to view and has assented to the membership agreement, including MSN's forum selection clause. No charges are incurred until after the membership agreement review is completed and a subscriber has clicked on "I Agree."

The trial court observed:

Generally, forum selection clauses are prima facie valid and enforceable in New Jersey. See *McNeill v. Zoref*, 297 N.J. Super. 213 (App. Div. 1997). New Jersey courts will decline to enforce a clause only if it fits into one of three exceptions to the general rule: (1) the clause is a result of fraud or "overweening" bargaining power; (2) enforcement would violate the strong public policy of New Jersey; or (3) enforcement would seriously inconvenience trial. *Wilfred McDonald, Inc. v. Cushman, Inc.*, 256 N.J. Super. 58 (App. Div.), *certif. denied*, 130 N.J. 17 (1992). The burden falls on the party objecting to enforcement to show that the clause in question fits within one of these exceptions. *Id.* Plaintiffs have failed to meet that burden here.

Judge Fitzpatrick correctly discerned that

New Jersey follows the logic of the United States Supreme Court decision in *Carnival Cruise Lines v. Shute*, 499 U.S. 585, 111 S. Ct. 1522, 113 L. Ed. 2d 622 (1991). * * * In *Carnival*, cruise ship passengers were held to a forum selection clause which appeared in their travel contract. The clause enforced in *Carnival* was very similar in nature to the clause in question here, the primary difference being that the *Carnival* clause was placed in small print in a travel contract while the clause in the case *sub judice* was placed on-line on scrolled computer screens.

The trial court opinion went on to analyze plaintiffs' contentions:

Plaintiffs' consent to MSN's clause does not appear to be the result of fraud or overweening bargaining power. In New Jersey, fraud consists of (1) material misrepresentation of a past or present fact; (2) knowledge or belief by the declarant of its falsity; (3) an intention that the recipient rely on it; (4)
reasonable reliance by the recipient; and (5) resulting damages. *Gennari v. Weichert Co. Realtors*, 148 N.J. 582 (1997). Plaintiffs have not shown that MSN's forum selection clause constitutes fraud. The clause is reasonable, clear and contains no material misrepresentation.

Further, plaintiffs were not subjected to overweening bargaining power in dealing with Microsoft and MSN. The Supreme Court has held that a corporate vendor's inclusion of a forum selection clause in a consumer contract does not in itself constitute overweening bargaining power. *Carnival*, 499 U.S. 585. In order to invalidate a forum selection clause, something more than merely size difference must be shown. *Id*. A court's focus must be whether such an imbalance in size resulted in an inequality of bargaining power that was unfairly exploited by the more powerful party. See, e.g., *Hodes v. S.N.C. Achille Lauro ed Altri-Gestione*, 858 F.2d 905 (3d Cir. 1988), *cert. denied*, 490 U.S. 1001, 109 S. Ct. 1633, 104 L. Ed. 2d 149 (1989).

Plaintiffs have shown little more than a size difference here. The on-line computer service industry is not one without competition, and therefore consumers are left with choices as to which service they select for Internet access, e-mail and other information services. Plaintiffs were not forced into a situation where MSN was the only available server. Additionally, plaintiffs and the class which they purport to represent were given ample opportunity to affirmatively assent to the forum selection clause. Like *Carnival*, plaintiffs here "retained the option of rejecting the contract with impunity." 499 U.S. 585. In such a case, this court finds it impossible to perceive an overwhelming bargaining situation.


Finally, Judge Fitzpatrick held that enforcement of the forum selection clause would not inconvenience a trial. Given the fact that the named plaintiffs reside in several jurisdictions and that, if the class were to be certified, many different domestic and international domiciles would also be involved, "the inconvenience to all parties is no greater in Washington than anywhere else in the country."

After reviewing the record in the light of the arguments advanced by the parties, we are in substantial agreement with the reasons for decision articulated by Judge Fitzpatrick. We reject as meritless plaintiffs' arguments on appeal that the terms of the forum selection clause do not prevent plaintiffs from suing Microsoft outside of Washington or, alternatively, that the forum selection clause lacks adequate clarity. The meaning of the clause is plain and its effect as a limiting provision is clear. Furthermore, New Jersey's interest in assuring consumer fraud protection will not be frustrated by requiring plaintiffs to proceed with a lawsuit in Washington as prescribed by the plain language of the forum selection clause. As a general matter, none of the inherent characteristics of forum selection clauses implicate consumer fraud concepts in any special way. If a forum selection clause is clear in its purport and has been presented to the party to be bound in a fair and forthright fashion, no consumer fraud policies or principles have been violated. Cf. *id.* at 63-64. Moreover, as a matter of policy interest and apart from considerations bearing upon the choice-of-law provision in the forum selection clause, plaintiffs have given us no reason to apprehend that the nature and scope of consumer fraud protections afforded by the State of Washington are materially different or less broad in scope than those available in this State.

The only viable issues that remain bear upon the argument that plaintiffs did not receive adequate notice of the forum selection clause, and therefore that the clause never became part of the membership contract which bound them. A related, alternative argument is that the question of notice is a factual matter that should be submitted to a jury. Defendants respond by arguing that 1) in the absence of fraud, a contracting party is bound by the provisions of a form contract even if he or she never reads them; 2) this clause met all reasonable standards of conspicuousness; and 3) the sign-up process gave plaintiffs
ample opportunity to review and reject the agreement. Defendants also contend that notice is a question of law, decidable by a court, not a jury.

The holding in *Carnival Cruise Lines v. Shute*, 499 U.S. 585, 111 S. Ct. 1522, 113 L. Ed. 2d 622 (1991), does not dispose of the notice question because the plaintiffs there had "essentially ... conceded that they had notice of the forum-selection provision[,]" by stating that they "'[did] not contest ... that the forum selection clause was reasonably communicated to [them], as much as three pages of fine print can be communicated." *Id.* at 590, 111 S. Ct. at 1525, 113 L. Ed. 2d at 630. The dissenting justices described the format in which the forum selection clause had been presented as "in the fine print on the back of the [cruise] ticket." *Id.* at 597, 111 S. Ct. at 1529, 113 L. Ed. 2d at 634 (Stevens, J., dissenting).

The scenario presented here is different because of the medium used, electronic versus printed; but, in any sense that matters, there is no significant distinction. The plaintiffs in *Carnival* could have perused all the fine-print provisions of their travel contract if they wished before accepting the terms by purchasing their cruise ticket. The plaintiffs in this case were free to scroll through the various computer screens that presented the terms of their contracts before clicking their agreement.

Also, it seems clear that there was nothing extraordinary about the size or placement of the forum selection clause text. By every indication we have,[3] the clause was presented in exactly the same format as most other provisions of the contract. It was the first item in the last paragraph of the electronic document. We note that a few paragraphs in the contract were presented in upper case typeface, presumably for emphasis, but most provisions, including the forum selection clause, were presented in lower case typeface. We discern nothing about the style or mode of presentation, or the placement of the provision, that can be taken as a basis for concluding that the forum selection clause was preferred unfairly, or with a design to conceal or de-emphasize its provisions. To conclude that plaintiffs are not bound by that clause would be equivalent to holding that they were bound by no other clause either, since all provisions were identically presented. Plaintiffs must be taken to have known that they were entering into a contract; and no good purpose, consonant with the dictates of reasonable reliability in commerce, would be served by permitting them to disavow particular provisions or the contracts as a whole. See *Rudbart v. North Jersey Dist. Water Supply Comm'n*, 127 N.J. 344, 351-53 (referring to the principle that a contracting party may be bound by the terms of a form contract even if he or she has never read them), *cert. denied*, 506 U.S. 871, 113 S. Ct. 203, 121 L. Ed. 2d 145 (1992).

The issue of reasonable notice regarding a forum selection clause is a question of law for the court to determine. See *Effron v. Sun Line Cruises, Inc.*, 67 F.3d 7, 9 (2d Cir. 1995); *Hodes v. S.N.C. Achille Lauro ed Altri-Gestione*, 858 F.2d 905, 908 (3d Cir. 1988), *petition for cert. dismissed*, 490 U.S. 1001, 109 S. Ct. 1633, 104 L. Ed. 2d 149 (1989), *abrogated on other grounds*, *Lauro Lines, S.R.L. v. Chasser*, 490 U.S. 495, 109 S. Ct. 1976, 104 L. Ed. 2d 548 (1989). We agree with the trial court that, in the absence of a better showing than has been made, plaintiffs must be seen to have had adequate notice of the forum selection clause. The resolution of this notice issue, at this stage of the litigation between plaintiffs and defendants must, of course, be seen to be without prejudice to any showing either party may have the opportunity to make in another jurisdiction in a plenary proceeding on the contract regarding issues apart from the validity and enforceability of the forum selection clause.

Affirmed.

FOOTNOTES

1. [Return to Text] The complaint was initially filed on February 24, 1997.

2. [Return to Text] Defendants' March 26, 1997 petition to remove the matter to the U.S. District Court for the District of New Jersey was withdrawn on April 24, 1997.

3. [Return to Text] We have not considered the CD-ROM version of the contract, presented in the record on appeal, since none of the present plaintiffs used that means in joining MSN.
## State-by-State Analysis of Anti-Spam Laws

by Max Ochoa, Cooley Godward

### Exhibit B - DRAFT (last updated 10/21/99)

<table>
<thead>
<tr>
<th>“Commercial” Only</th>
<th>Unsolicited Email Statute</th>
<th>Unsolicited Safe Harbors</th>
<th>ISP Safe Harbors</th>
<th>Civil Damages</th>
<th>Consumer Protection Statute</th>
<th>No violation of ISP policies</th>
<th>Long arm</th>
<th>Criminal Penalty</th>
<th>Bulk email</th>
<th>SOL</th>
<th>Special Damages, punis, lost profits, etc</th>
</tr>
</thead>
<tbody>
<tr>
<td>NV (NRS 41.705 et seq.)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>WA (RCW 19.190 et seq.)</td>
<td>Y</td>
<td>N</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>CA (B&amp;P Code § 17538.4)</td>
<td>Y*</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>CA (B&amp;P Code § 17538.45)</td>
<td>Y*</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>VA (1999 HB 1714, §§ 8.01-328.1, 18.2-152.2, -152.4,-152.12)</td>
<td>N</td>
<td>N</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>WV (1999 HB 2627, Code § 46A, 6G)</td>
<td>N</td>
<td>Y</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y (2 years)</td>
</tr>
<tr>
<td>IA (Title XVI, §§ 714D.1, 714D.2)</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>OK (Title 15, § 776.1 et seq., Title 74, § 5060.52)</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N/A</td>
<td>Y</td>
<td>N/N/A</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>TN (1999 HB 530, Title 47, Chap. 18)</td>
<td>Y*</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Private AG?</td>
<td>N/A</td>
<td>N</td>
<td>N/N/A</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>CT (1999 HB 5028, Public Act No. 99-160)</td>
<td>N</td>
<td>N</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y/N/A</td>
<td>Y</td>
<td>Y/N/A</td>
<td>Y</td>
<td>Y</td>
<td>Y (2 years)</td>
</tr>
<tr>
<td>State</td>
<td>&quot;Commercial&quot; Only</td>
<td>Unsolicited Email Statute</td>
<td>Unsolicited Safe Harbors</td>
<td>ISP Safe Harbors</td>
<td>Civil Damages</td>
<td>Consumer Protection Statute</td>
<td>No violation of ISP policies</td>
<td>Long arm</td>
<td>Criminal Penalty</td>
<td>Bulk email</td>
<td>SOL</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
<td>------------------</td>
<td>--------------</td>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>------------</td>
<td>-----</td>
</tr>
<tr>
<td>NC (1999 SB 288, G.S. §§ 1-75.4, 14-453, 14-458, 1-539.2A)</td>
<td>Y</td>
<td>Y</td>
<td>N/A</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>?</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>DE (Title 11, §§ 936-941, as amended by 1999 HB 242)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>?</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RI (1999 HB 5641, General Laws 6-47)</td>
<td>Y*</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>RI (General Laws § 11-52-1, 6, 41, as amended by 1999 HB 5644)</td>
<td>N</td>
<td>N</td>
<td>N/A</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>?</td>
<td>Y</td>
<td>N/A</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>LA (1999 HB 2228, R.S. 14:73.1(5), (8), (12), (13), 14:73.6)</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>?</td>
<td>Y</td>
<td>N</td>
<td>Y &gt;1000</td>
<td>N</td>
</tr>
<tr>
<td>IL (1999 HB 2616, Public Act 91-0233)</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
§ 17538.4. (Operative term contingent) Unsolicited fax or e-mail

(a) No person or entity conducting business in this state shall facsimile (fax) or cause to be faxed, or electronically mail (e-mail) or cause to be e-mailed, documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit unless:

(1) In the case of a fax, that person or entity establishes a toll-free telephone number that a recipient of the unsolicited faxed documents may call to notify the sender not to fax the recipient any further unsolicited documents.

(2) In the case of e-mail, that person or entity establishes a toll-free telephone number or valid sender operated return e-mail address that the recipient of the unsolicited documents may call or e-mail to notify the sender not to e-mail any further unsolicited documents.

(b) All unsolicited faxed or e-mailed documents subject to this section shall include a statement informing the recipient of the toll-free telephone number that the recipient may call, or a valid return address to which the recipient may write or e-mail, as the case may be, notifying the sender not to fax or e-mail the recipient any further unsolicited documents to the fax number, or numbers, or e-mail address, or addresses, specified by the recipient.

In the case of faxed material, the statement shall be in at least nine-point type. In the case of e-mail, the statement shall be the first text in the body of the message and shall be of the same size as the majority of the text of the message.

(c) Upon notification by a recipient of his or her request not to receive any further unsolicited faxed or e-mailed documents, no person or entity conducting business in this state shall fax or cause to be faxed or e-mail or cause to be e-mailed any unsolicited documents to that recipient.
CAL BUS & PROF CODE § 17538.4

(d) In the case of e-mail, this section shall apply when the unsolicited e-mailed documents are delivered to a California resident via an electronic mail service provider's service or equipment located in this state. For these purposes "electronic mail service provider" means any business or organization qualified to do business in this state that provides individuals, corporations, or other entities the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(e) As used in this section, "unsolicited e-mailed documents" means any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit that meet both of the following requirements:

(1) The documents are addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(2) The documents are not sent at the request of, or with the express consent of, the recipient.

(f) As used in this section, "fax" or "cause to be faxed" or "e-mail" or "cause to be e-mailed" does not include or refer to the transmission of any documents by a telecommunications utility or Internet service provider to the extent that the telecommunications utility or Internet service provider merely carries that transmission over its network.

(g) In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, the subject line of each and every message shall include "ADV:" as the first four characters. If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include "ADV:ADLT" as the first eight characters.

(h) An employer who is the registered owner of more than one e-mail address may notify the person or entity conducting business in this state e-mailing or causing to be e-mailed, documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit of the desire to cease e-mailing on behalf of all of the employees who may use employer-provided and employer-controlled e-mail addresses.

(i) This section, or any part of this section, shall become inoperative on and after the date that federal law is enacted that prohibits or otherwise regulates the transmission of unsolicited advertising by electronic mail (e-mail).

HISTORY:
Added Stats 1992 ch 564 § 1 (AB 2438).
Amended Stats 1998 ch 865 § 1 (AB 1676).
§ 17538.45. Unsolicited electronic mail advertisement

(a) For purposes of this section, the following words have the following meanings:

(1) "Electronic mail advertisement" means any electronic mail message, the principal purpose of which is to promote, directly or indirectly, the sale or other distribution of goods or services to the recipient.

(2) "Unsolicited electronic mail advertisement" means any electronic mail advertisement that meets both of the following requirements:

(A) It is addressed to a recipient with whom the initiator does not have an existing business or personal relationship.

(B) It is not sent at the request of or with the express consent of the recipient.

(3) "Electronic mail service provider" means any business or organization qualified to do business in California that provides registered users the ability to send or receive electronic mail through equipment located in this state and that is an intermediary in sending or receiving electronic mail.

(4) "Initiation" of an unsolicited electronic mail advertisement refers to the action by the initial sender of the electronic mail advertisement. It does not refer to the actions of any intervening electronic mail service provider that may handle or retransmit the electronic message.

(5) "Registered user" means any individual, corporation, or other entity that maintains an electronic mail address with an electronic mail service provider.

(b) No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy
prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.

(c) No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.

(d) An electronic mail service provider shall not be required to create a policy prohibiting or restricting the use of its equipment for the initiation or delivery of unsolicited electronic mail advertisements.

(e) Nothing in this section shall be construed to limit or restrict the rights of an electronic mail service provider under Section 230(c)(1) of Title 47 of the United States Code, or any decision of an electronic mail service provider to permit or to restrict access to or use of its system, or any exercise of its editorial function.

(f) (1) In addition to any other action available under law, any electronic mail service provider whose policy on unsolicited electronic mail advertisements is violated as provided in this section may bring a civil action to recover the actual monetary loss suffered by that provider by reason of that violation, or liquidated damages of fifty dollars ($50) for each electronic mail message initiated or delivered in violation of this section, up to a maximum of twenty-five thousand dollars ($25,000) per day, whichever amount is greater.

(2) In any action brought pursuant to paragraph (1), the court may award reasonable attorney's fees to a prevailing party.

(3) (A) In any action brought pursuant to paragraph (1), the electronic mail service provider shall be required to establish as an element of its cause of action that prior to the alleged violation, the defendant had actual notice of both of the following:

(i) The electronic mail service provider's policy on unsolicited electronic mail advertising.

(ii) The fact that the defendant's unsolicited electronic mail advertisements would use or cause to be used the electronic mail service provider's equipment located in this state.

(B) In this regard, the Legislature finds that with rapid advances in Internet technology, and electronic mail technology in particular, Internet service providers are already experimenting with embedding policy statements directly into the software running on the computers used to provide electronic mail services in a manner that displays the policy statements every time an electronic mail delivery is requested. While the state of the technology does not support such a finding at present, the Legislature believes that, in a given case at some future date, a showing that notice was supplied via electronic means between the sending and receiving computers could be held to constitute actual notice to the sender for purposes of this paragraph.
(4) A violation of this section shall not be subject to Section 17534.

HISTORY:
Added Stats 1998 ch 863 § 2 (AB 1629).

EDITOR'S NOTES:
§ In the 1999 Deering's Supplement, this section was erroneously placed to follow B & P C § 17539.4. It should, in fact, follow B & P C § 17538.4.
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
JUDGE GRAHAM

February 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 in addition prevent defendant 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.

I.

The Court will begin its analysis of the issues by acknowledging, for the purpose of providing a 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 innumerous 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 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 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

1 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 a restaurant menu.

CompuServe subscribers use CompuServe's domain name "CompuServe.com" together with their own unique alphanumeric 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 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. CompuServe 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 a 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 account or 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 prescribed 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 prescribed 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 prescribing 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 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.B. 591 (1929); Great American Mut. Indem. 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); Klienbriel 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 intentionally using or intermeddling 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.]

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. Bezenecik, 56 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 massages are affirmatively directed to their destination.

Defendants, citing Restatement (Second) of Torts §221, which defines "disposition", 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 dispossessed 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 dispossession is in just one circumstance under which a defendant can be found liable. Defendants suggest that "[u]nless 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 chattels 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. Szybiak, 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 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 Zaalow 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 by 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 computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. (Mangino Supp. Dec. at ¶¶7-8). To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's 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 has 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 chattel, 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, defendant's 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).

2 That consent is apparently subject to express limitations. See Kolehmainen Dec. at ¶2 and discussion *infra*.

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 of express restriction or limitation on invitation turns business invitee into trespasser). 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 systems by denying unauthorized parties the use of CompuServe equipment to 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 in 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 determination 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 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 the same 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 oligopolistic 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 necessary to provide Internet access services on a smaller 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*, --- U.S. ---, ---, 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 a 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. 991, 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 private 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*, --- 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), protestors 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 may 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 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. An 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 unresponsive 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. 1974); see generally Wright, Miller & Kane, Federal Practice and Procedure §2949, at 218-220 (West 1995). Defendants 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 in not appropriate where an ultimate award of monetary damages will suffice. Montgomery v. Carr, 848 F. Supp. 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. Supp. 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 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 had 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
HOTMAIL CORPORATION, Plaintiff,

v.

VAN$ MONEY PIE INC.; ALS Enterprises, Inc.; LCGM, Inc.; Christopher Moss d/b/a the Genesis Network, Inc.; Claremont Holdings Ltd.; Consumer Connections; Palmer & Associates; and Financial Research Group; and Darlene Snow d/b/a Visionary Web Creations and/or d/b/a Maximum Impact Marketing, Defendants.

No. C-98 JW PVT ENE, C 98-20064 JW.

United States District Court, N.D. California.


Nicole A. Wong, Hosie, Wes, Sacks & Brelsford, LLP, Menlo Park, CA, for Plaintiff.


ORDER GRANTING PRELIMINARY INJUNCTION

WARE, J.

THIS MATTER was submitted on the papers by the Court on the Motion of plaintiff Hotmail Corporation ("Hotmail") for Preliminary Injunction to enjoin defendants ALS Enterprises, Inc. ("ALS"); LCGM, Inc. ("LCGM"); Christopher Moss d/b/a Genesis Network ("Moss"); Palmer & Associates ("Palmer"); Financial Research Group ("Financial") and Darlene Snow d/b/a Visionary Web Creations and/or d/b/a Maximum Impact Marketing ("Snow") from infringing Hotmail's HOTMAIL trade name and service mark, diluting this mark, engaging in acts of unfair competition, violating the Computer Fraud and Abuse Act, breaching a contract, and violating California law. 15 U.S.C. §§ 1125(a) & (c); 18 U.S.C. § 1030; Cal. Bus. & Prof.Code §§ 14330, 17200; Cal. Civ.Code §§ 1709-10; and 3420-22. Having reviewed the entire court record pertaining to this Motion, and having considered the evidence and argument of counsel in support of Hotmail's Motion, the Court enters the following Findings of Fact and Conclusions of Law:

FINDINGS OF FACT

1. Plaintiff Hotmail is a Silicon Valley company that provides free electronic mail ("e-mail") on the World Wide Web. Hotmail's online services allow its over ten million registered subscribers to exchange e-mail messages over the Internet with any other e-mail user who has an Internet e-mail address throughout the world. Every e-mail sent by a Hotmail subscriber automatically displays a header depicting Hotmail's domain name "hotmail.com" and a footer depicting Hotmail's "signature" at the bottom of the e-mail which reads "Get Your Private, Free Email at http://www.hotmail.com." Every e-mail received by a Hotmail subscriber also automatically displays a header depicting Hotmail's domain name. Thus, plaintiff's HOTMAIL mark--contained within its domain name and signature--appears on millions of e-mails transmitted worldwide daily.

2. In or about 1996, Hotmail developed the mark HOTMAIL and obtained the Internet domain name "hotmail.com" which incorporates its mark. Hotmail is the sole and exclusive holder of that domain name.

3. In or about 1996, Hotmail began using its HOTMAIL mark in various forms and styles, continuously in commerce in association with its online services as a means of identifying and distinguishing Hotmail's online services from those of others. Thus Hotmail's mark has appeared in the headers and footers of e-mail sent from and received by Hotmail subscribers, on Hotmail's homepage and on nearly every page of its Website, on letterhead and envelopes, on business cards, in promotional materials and in press releases.
4. Hotmail has spent approximately $10 million marketing, promoting, and distributing its services in association with its HOTMAIL mark. Hotmail does not authorize any other e-mail service provider to use its HOTMAIL mark, or Hotmail's domain name or signature.

5. "Spam" is unsolicited commercial bulk e-mail akin to "junk mail" sent through the postal mail. The transmission of spam is a practice widely condemned in the Internet Community and is of significant concern to Hotmail.

6. Hotmail has invested substantial time and money in efforts to disassociate itself from spam and to protect e-mail users worldwide from receiving spam associated in any way with Hotmail.

7. To become a Hotmail subscriber, one must agree to abide by a Service Agreement ("Terms of Service") which specifically prohibits subscribers from using Hotmail's services to send unsolicited commercial bulk e-mail or "spam," or to send obscene or pornographic messages. Hotmail can terminate the account of any Hotmail subscriber who violates the Terms of Service.

8. In or about the Fall of 1997, Hotmail learned that defendants were sending "spam" e-mails to thousands of Internet e-mail users, which were intentionally falsified in that they contained return addresses bearing Hotmail account return addresses including Hotmail's domain name and thus its mark, when in fact such messages did not originate from Hotmail or a Hotmail account. Such spam messages advertised pornography, bulk e-mailing software, and "get-rich-quick" schemes, among other things.

9. In addition, Hotmail learned that defendants had created a number of Hotmail accounts for the specific purpose of facilitating their spamming operations. Such accounts were used to collect responses to defendants' e-mails and "bounced back" messages in what amounted to a "drop box" whose contents were never opened, read or responded to. It was these Hotmail accounts that were used as return addresses by defendants in lieu of defendants' actual return addresses when defendants sent their spam e-mail.

10. As a result of the falsified return addresses described above, Hotmail was inundated with hundreds of thousands of misdirected responses to defendants' spam, including complaints from Hotmail subscribers regarding the spam and "bounced back" e-mails which had been sent by defendants to nonexistent or incorrect e-mail addresses. This overwhelming number of e-mails took up a substantial amount of Hotmail's finite computer space, threatened to delay and otherwise adversely affect Hotmail's subscribers in sending and receiving e-mail, resulted in significant costs to Hotmail in terms of increased personnel necessary to sort and respond to the misdirected complaints, and damaged Hotmail's reputation and goodwill.

11. In particular, Hotmail discovered a spam e-mail message advertising pornographic material that was sent by ALS. While this spam originated from ALS and was transmitted through an E-mail Provider other than Hotmail, ALS falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "geri748@hotmail.com."

12. Hotmail also discovered a number of spam e-mail messages advertising pornographic material that were sent by LCGM. While these spam e-mails originated from LCGM and were transmitted through an E-mail Provider other than Hotmail, LCGM falsely designated a number of real Hotmail e-mail address as the points of origin. The e-mail addresses chosen for this purpose were "becky167@hotmail.com;" "deena54@hotmail.com;" "marisa104@hotmail.com;" "shelly345@hotmail.com;" "sonnie67@hotmail.com;" "ashley_113@hotmail.com;" "grace44@hotmail.com;" "jess_59@hotmail.com;" "kristina17@hotmail.com;" "nellie24@hotmail.com;" and, "tyriona56@hotmail.com."

13. Hotmail also discovered a spam e-mail message advertising pornographic material that was sent by Moss. While this spam originated from Moss and was transmitted through an E-mail Provider other than Hotmail, Moss falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "rebecca_h19@hotmail.com."
14. Hotmail also discovered a spam e-mail message advertising a cable descrambler kit that was sent by Palmer. While this spam originated from Palmer and was transmitted through an E-mail Provider other than Hotmail, Palmer falsely designated two real Hotmail e-mail addresses as the points of origin. The e-mail addresses chosen for this purpose were "kelCA@hotmail.com" and "angiCA@hotmail.com."

15. Hotmail also discovered a spam e-mail message advertising a service that matches people seeking cash grants that was sent by Financial. While this spam originated from Financial and was transmitted through an E-mail Provider other than Hotmail, Financial falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "order_desk66@hotmail.com."

16. Hotmail also discovered a number of spam e-mail messages advertising pornography that were sent by Snow. While this spam originated from Snow and was transmitted through an E-mail Provider other than Hotmail, Snow falsely designated several real Hotmail e-mail address as the point of origin. The e-mail addresses chosen for this purpose were "bettyharriss123@hotmail.com;" "annharriss123@hotmail.com;" "cindyharriss123@hotmail.com;" "wilmasimpson@hotmail.com;" "rw3570@hotmail.com;" "rw3560@hotmail.com;" and, "jw2244@hotmail.com."

CONCLUSIONS OF LAW

Jurisdiction and Venue

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367. This Court has personal jurisdiction over the defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, who have engaged in business activities in or directed in California.

18. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because a substantial portion of the events giving rise to the claims pled herein occurred in this judicial district and defendants do business in this judicial district.

Standard For Granting Preliminary Injunction

19. The standard for preliminary injunction relief in trademark infringement cases and related actions is well-settled. Hotmail must show either: (a) a likelihood of success on the merits and the possibility of irreparable injury; or (b) the existence of serious questions going to the merits and the balance of hardships tips in Hotmail's favor. Apple Computer, Inc. v. Formula Int'l, Inc., 725 F.2d 521, 523 (9th Cir.1984).

Plaintiff's Legal Claims


Plaintiff's Likelihood Of Success On Its Claims

False Designation Of Origin And Unfair Competition

21. The core element of a cause of action for false designation of origin under 15 U.S.C. § 1125(a) as well as other unfair competition is "likelihood of confusion, i.e., whether the similarity of the marks is likely to confuse customers about the source of the products." E. & J. Gallo Winery v. Gallo Cattle Co., 967 F.2d 1280, 1290 (9th Cir.1992); Academy of Motion Picture Arts & Sciences v. Creative House Promotions, Inc., 944 F.2d 1446, 1454 (9th Cir.1991).
22. Courts will consider the following factors, among others, as relevant to a determination of the likelihood of confusion for claims under 15 U.S.C. § 1125(a) and related other unfair competition claims: (a) strength or weakness of plaintiff's mark; (b) the degree of similarity with defendant's mark; (c) class of goods; (d) marketing channels used; (e) evidence of actual confusion; and (f) intent of the defendant. Americana Trading Inc. v. Russ Berrie & Co., 966 F.2d 1284, 1287 (9th Cir.1992). However, there is not a mandated test for likelihood of confusion applied by the courts in this Circuit, and the appropriate time for full consideration of all relevant factors is when the merits of the case are tried. Apple Computer, 725 F.2d at 526.

23. The majority of these factors supports a finding that Hotmail is likely to succeed on the merits of its claims that defendants' use of the HOTMAIL mark is likely to cause consumer confusion or mistake as to the origin, sponsorship, or approval of defendants' spam e-mails and spam e-mail business, and that there are at least serious questions going to the merits of plaintiff's claims.

24. Plaintiff's mark is strong. The "strength" of a mark depends in part on whether it is arbitrary or fanciful, suggestive, merely descriptive, or generic. Chronicle Pub. Co. v. Chronicle Publications, Inc., 733 F.Supp. 1371, 1375 (N.D.Cal.1989). In addition, a company's "extensive advertising, length of time in business, public recognition, and uniqueness" all strengthen its trademarks. Century 21 Real Estate Corp. v. Sandlin, 846 F.2d 1175, 1179 (9th Cir.1988). While the second part of the mark--"mail"--may be suggestive by conveying some aspect of the e-mail process, the mark as a whole is arbitrary and fanciful because it neither describes nor suggests that Hotmail is a provider of electronic mail as a Web-based service on the Internet. Moreover, plaintiff has spent substantial sums of money to advertise and market its services in association with the mark and has extensively featured the mark in its promotions.

25. Defendants' "mark" is not only confusingly similar to plaintiff's mark, it is identical to it. A comparison of defendants' and plaintiff's uses shows such striking similarity that a jury could not help but find that defendants' use is confusing. Indeed, there has been actual confusion among consumers regarding the marks. This factor alone may be determinative. See E. Remy Martin & Co., S.A. v. Shaw-Ross International Imports, Inc., 756 F.2d 1525, 1529, 1530 (11th Cir.1985) (it is "well-settled" that "evidence of actual confusion is not necessary to a finding of likelihood of confusion, although it is the best such evidence;" indeed, "a sufficiently strong showing of likelihood of confusion may be itself constitute a showing of substantial likelihood of prevailing on the merits and/or a substantial threat of irreparable harm"); World Carpets, Inc. v. Dick Littrell's New World Carpets, 438 F.2d 482, 489 (5th Cir.1971) ("[t]here can be no more positive or substantial proof of likelihood of confusion than proof of actual confusion").

26. The class of goods and services distributed by defendants--e-mails--which bear a mark identical to plaintiff's, are the same as the class of goods and services distributed by plaintiff--e-mails.

27. The marketing channels through which the parties sell their goods and services are the same--via e-mail over the Internet. Their consumer audience is likewise the same. Moreover, because e-mail is specifically designed for the rapid exchange of information, consumers are unlikely to exercise a great deal of care in distinguishing between marks on e-mails they receive.

28. Defendants' intent further supports possible confusion. Levi Strauss & Co. v. Blue Bell, 632 F.2d 817, 822 (9th Cir.1981); Pacific Telesis Group v. International Telesis Communications, 994 F.2d 1364, 1369 (9th Cir.1993). Here, the evidence supports an inference that defendants intended to emulate plaintiff's trademark, given their knowing falsification of e-mail return addresses, their fraudulent creation of Hotmail mailboxes, as well as their attempts to circumvent plaintiff's efforts to prevent its subscribers from receiving spam.

Dilution

29. The core elements of a cause of action under the federal dilution statute are plaintiff's ownership of a famous mark and dilution of the distinctive quality of plaintiff's mark, regardless of whether consumers
are confused about the parties' goods. 15 U.S.C. § 1125(c)(1). Under the California dilution statute as well, actual injury or likelihood of confusion need not be shown; plaintiff need only show its business reputation is likely to be injured or the distinctive value of its mark is likely to be diluted. Cal. Bus. & Prof.Code § 14330; Academy, 944 F.2d at 1457.

30. In determining whether a mark is distinctive and famous so as to support a claim for federal dilution, the Court has considered the following factors: (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 or 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 mark's owner and the person against whom the injunction is sought; and (g) the nature and extent of use of the same or similar marks by third parties. 15 U.S.C. § 1125(c)(1).


32. Here, the evidence supports a finding that plaintiff will likely prevail on its federal and state dilution claims and that there are at least serious questions going to the merits of these claims. First, there is sufficient evidence to lead to a finding that plaintiff's trademark is "famous" within the meaning of 15 U.S.C. § 1125(c)(1) and also that it is entitled to state dilution protection. Plaintiff's mark is distinctive, has been advertised and used extensively both nationally and internationally in connection with plaintiff's services, and has established considerable consumer recognition. Moreover, the use of identical marks by defendants who are sending e-mails to thousands of e-mail users across the country and the world through identical trade channels threatens to dilute the distinctiveness of plaintiff's trademark and threatens to harm plaintiff's business reputation.

Violation Of Computer Fraud And Abuse Act

33. The Computer Fraud and Abuse Act prohibits any person from knowingly causing the transmission of information which intentionally causes damage, without authorization, to a protected computer. 18 U.S.C. § 1030.

34. The evidence supports a finding that plaintiff will likely prevail on its Computer Fraud and Abuse Act claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants knowingly falsified return e-mail addresses so that they included, in place of the actual sender's return address, a number of Hotmail addresses; that such addresses were tied to Hotmail accounts set up by defendants with the intention of collecting never-to-be-read consumer complaints and "bounced back" e-mails; that defendants knowingly caused this false information to be transmitted to thousands of e-mail recipients; that defendants took this action knowing such recipients would use the "reply to" feature to transmit numerous responses to the fraudulently created Hotmail accounts, knowing thousands of messages would be "bounced back" to Hotmail instead of to defendants, and knowing that numerous recipients of defendants' spam would e-mail complaints to Hotmail; that defendants took such actions knowing the risks caused thereby to Hotmail's computer system and online services, which include risks that Hotmail would be forced to withhold or delay the use of computer services to its legitimate subscribers; that defendants' actions caused damage to Hotmail; and that such actions were done by defendants without Hotmail's authorization.

Breach Of Contract

35. The evidence supports a finding that plaintiff will likely prevail on its breach of contract claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants obtained a number of Hotmail mailboxes and access to Hotmail's services; that in so doing defendants agreed to abide by Hotmail's Terms of Service which prohibit using a Hotmail account for purposes of sending spam and/or pornography; that defendants breached their contract with Hotmail by using Hotmail's services to facilitate sending spam and/or
pornography; that Hotmail complied with the conditions of the contract except those from which its performance was excused; and that if defendants are not enjoined they will continue to create such accounts in violation of the Terms of Service.

Fraud And Misrepresentation

36. The cause of action for fraud includes willfully deceiving another with intent to induce him to alter his position to his injury or risk by asserting, as a fact, that which is not true, by one who has no reasonable ground for believing it to be true; or by suppressing a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or by making a promise without any intention of performing it. Civ.Code §§ 1709-10.

37. The evidence supports a finding that plaintiff will likely prevail on its fraud and misrepresentation claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants fraudulently obtained a number of Hotmail accounts, promising to abide by the Terms of Service without any intention of doing so and suppressing the fact that such accounts were created for the purpose of facilitating a spamming operation, and that defendants’ fraud and misrepresentation caused Hotmail to allow defendants to create and use Hotmail’s accounts to Hotmail’s injury. In addition, the evidence supports a finding that defendants’ falsification of e-mails to make it appear that such messages and the responses thereto were authorized to be transmitted via Hotmail’s computers and stored on Hotmail’s computer system--when defendants knew that sending such spam was unauthorized by Hotmail--constitutes fraud and misrepresentation, and that Hotmail relied on such misrepresentations to allow the e-mails to be transmitted over Hotmail’s services and to take up storage space on Hotmail’s computers, to Hotmail’s injury.

Trespass To Chattel

38. "Trespass to chattel ... lies where an intentional interference with the possession of personal property has proximately caused injury." Thrifty-Tel, Inc. v. Bezenek, 46 Cal.App.4th 1559, 1566, 54 Cal.Rptr.2d 468 (1996).

39. The evidence supports a finding that plaintiff will likely prevail on its trespass to chattel claim and that there are serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that the computers, computer networks and computer services that comprise Hotmail’s e-mail system are the personal property of Hotmail; that defendants obtained consent to create Hotmail accounts within the limitations set forth in the Terms of Service: no spamming and no pornography; that defendants intentionally trespassed on Hotmail’s property by knowingly and without authorization creating Hotmail accounts that were used for purposes exceeding the limits of the Terms of Service; that defendants trespassed on Hotmail’s computer space by causing tens of thousands of misdirected e-mail messages to be transmitted to Hotmail without Hotmail’s authorization, thereby filling up Hotmail’s computer storage space and threatening to damage Hotmail’s ability to service its legitimate customers; and that defendants’ acts of trespass have damaged Hotmail in terms of added costs for personnel to sort through and respond to the misdirected e-mails, and in terms of harm to Hotmail’s business reputation and goodwill.

Irreparable Harm To Plaintiff

40. In cases where trademark infringement is shown, irreparable harm is presumed. Apple Computer, 725 F.2d at 525; Charles Schwab & Co. v. Hibernia Bank, 665 F.Supp. 800, 812 (N.D.Cal.1987).

41. Plaintiff has suffered and, if defendants are not enjoined, will continue to suffer irreparable harm from the distribution, promotion and use of e-mails bearing plaintiff’s mark--particularly spam e-mails, some of which advertise pornography--because of the loss of goodwill and reputation arising from customer confusion about the source of defendants’ spam e-mails and/or plaintiff’s affiliation or sponsorship of them. This kind of harm is not easily quantified and not adequately compensated with money damages. Plaintiff thus has no adequate remedy at law.
Balance Of Hardships

42. The Court finds that the irreparable harm to plaintiff should injunctive relief not be granted outweighs any injury to defendants resulting from a temporary injunction. Plaintiff has introduced evidence that it has been involved in extensive distribution and promotion of its online services in association with its mark for years and has expended vast amounts of time and money developing and promoting its mark. Plaintiff also is a service mark owner entitled to avoid having its reputation and goodwill placed in jeopardy. In contrast, if enjoined, defendants would not suffer harm in that they would be free to continue advertising by means of e-mail so long as they did not use Hotmail's mark or services to facilitate such advertising. Thus, the balance of hardships strongly tips in favor of plaintiff.

Conclusion

43. The Court therefore concludes that plaintiff is entitled to a preliminary injunction on the grounds that plaintiff is likely to succeed on the merits, that there is a possibility of irreparable injury, that there are serious questions going to the merits, and that the balance of hardships tips sharply in plaintiff's favor. It is therefore,

ORDERED AND ADJUDGED:

That defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, their officers, agents, co-conspirators, servants, affiliates, employees, parent and subsidiary corporations, attorneys and representatives, and all those in privity or acting in concert with defendants are temporarily and preliminarily enjoined and restrained during the pendency of this action from directly or indirectly:

1. Using any images, designs, logos or marks which copy, imitate or simulate Hotmail's HOTMAIL mark, and/or Hotmail's "hotmail.com" domain name for any purpose, including but not limited to any advertisement, promotion, sale or use of any products or services;

2. Performing any action or using any images, designs, logos or marks that are likely to cause confusion, to cause mistake, to deceive, or to otherwise mislead the trade or public into believing that Hotmail and defendants, or any of them, are in any way connected, or that Hotmail sponsors defendants; or that defendants, or any of them, are in any manner affiliated or associated with or under the supervision or control of Hotmail, or that defendants and Hotmail or Hotmail's services are associated in any way.

3. Using any images, designs, logos or marks or engaging in any other conduct that creates a likelihood of injury to the business reputation of Hotmail or a likelihood of misappropriation and/or dilution of Hotmail's distinctive mark and the goodwill associated therewith;

4. Using any trade practices whatsoever, including those complained of herein, which tend to unfairly compete with or injure Hotmail, its business and/or the goodwill appertaining thereto;

5. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, electronic mail or messages bearing any false, fraudulent, anonymous, inactive, deceptive, or invalid return information, or containing the domain "hotmail.com," or otherwise using any other artifice, scheme or method of transmission that would prevent the automatic return of undeliverable electronic mail to its original and true point of origin or that would cause the e-mail return address to be that of anyone other than the actual sender;

6. Using, or directing, aiding, or conspiring with others to use, Hotmail's computers or computer networks in any manner in connection with the transmission or transfer of any form of electronic information across the Internet, including, but not limited to, creating any Hotmail e-mail account, or becoming a Hotmail subscriber, for purposes other than those permitted by Hotmail's Terms of Services, including but not limited to, for purposes of participating in any way in sending spam e-mail or operating a spamming business, or sending or advertising or promoting pornography and/or sending e-mails for any commercial purpose.
7. Opening, creating, obtaining and/or using, or directing, aiding, or conspiring with others to open, create, obtain and/or use, any Hotmail account or mailbox;

8. Acquiring or compiling Hotmail member addresses for use in the transmission of unsolicited promotional messages to those Hotmail members; and,

9. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, any unsolicited electronic mail message, or any electronic communication of any kind, to or through Hotmail or its members without prior written authorization.

IT IS FURTHER ORDERED AND ADJUDGED:

That plaintiff shall provide a bond in the amount of only $100.
H.R. 4328--OMNIBUS APPROPRIATIONS BILL FY99

TITLE XIII--CHILDREN'S ONLINE PRIVACY PROTECTION

SEC. 1301. SHORT TITLE.

This title may be cited as the "Children's Online Privacy Protection Act of 1998".

SEC. 1302. DEFINITIONS.

In this title:
(1) Child.--The term "child" means an individual under the age of 13.
(2) Operator.--The term "operator"--
(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce--
(i) among the several States or with 1 or more foreign nations;
(ii) in any territory of the United States or in the District of Columbia, or between any such territory and--
(I) another such territory; or
(II) any State or foreign nation; or
(iii) between the District of Columbia and any State, territory, or foreign nation; but
(B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).
(4) Disclosure.--The term "disclosure" means, with respect to personal information--
(A) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and
(B) making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting, through the Internet, or through--
(i) a home page of a website;
(ii) a pen pal service;
(iii) an electronic mail service;
(iv) a message board; or
(v) a chat room.
(5) Federal agency.--The term "Federal agency" means an agency, as that term is defined in section 551(1) of title 5, United States Code.
(6) Internet.--The term "Internet" means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any
predecessor or successor protocols to such protocol, to
communicate information of all kinds by wire or radio.
(7) Parent.--The term "parent" includes a legal guardian.
(8) Personal information.--The term "personal
information" means individually identifiable information
about an individual collected online, including--
(A) a first and last name;
(B) a home or other physical address including street name
and name of a city or town;
(C) an e-mail address;
(D) a telephone number;
(E) a Social Security number;
(F) any other identifier that the Commission determines
permits the physical or online contacting of a specific
individual; or
(G) information concerning the child or the parents of that
child that the website collects online from the child and
combines with an identifier described in this paragraph.
(9) Verifiable parental consent.--The term "verifiable
parental consent" means any reasonable effort (taking into
consideration available technology), including a request for
authorization for future collection, use, and disclosure
described in the notice, to ensure that a parent of a child
receives notice of the operator's personal information
collection, use, and disclosure practices, and authorizes the
collection, use, and disclosure, as applicable, of personal
information and the subsequent use of that information before
that information is collected from that child.
(10) Website or online service directed to children.--
(A) In general.--The term "website or online service
directed to children" means--
(1)i a commercial website or online service that is targeted
to children; or
(ii) that portion of a commercial website or online service
that is targeted to children.
(B) Limitation.--A commercial website or online service, or
a portion of a commercial website or online service, shall
not be deemed directed to children solely for referring or
linking to a commercial website or online service directed to
children by using information location tools, including a
directory, index, reference, pointer, or hypertext link.
(11) Person.--The term "person" means any individual,
partnership, corporation, trust, estate, cooperative,
association, or other entity.
(12) Online contact information.--The term "online contact
information" means an e-mail address or another
substantially similar identifier that permits direct contact
with a person online.

SEC. 1303. REGULATION OF UNFAIR AND DECEPTIVE ACTS AND
PRACTICES IN CONNECTION WITH THE COLLECTION AND
USE OF PERSONAL INFORMATION FROM AND ABOUT
CHILDREN ON THE INTERNET.

(a) Acts Prohibited.--
(1) In general.--It is unlawful for an operator of a
website or online service directed to children, or any
operator that has actual knowledge that it is collecting
personal information from a child, to collect personal
information from a child in a manner that violates the
regulations prescribed under subsection (b).
(2) Disclosure to parent protected.--Notwithstanding
paragraph (1), neither an operator of such a website or
online service nor the operator's agent shall be held to be
liable under any Federal or State law for any disclosure made
in good faith and following reasonable procedures in responding to a request for disclosure of personal information under subsection (b)(1)(B)(iii) to the parent of a child.

(b) Regulations.--
(1) In general.--Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate under section 553 of title 5, United States Code, regulations that--
(A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child--

[(Page H11241)]

(i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and
(ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;
(B) require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent--
(i) a description of the specific types of personal information collected from the child by that operator;
(ii) the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and
(iii) notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;
(C) prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.
(2) When consent not required.--The regulations shall provide that verifiable parental consent under paragraph (1)(A)(ii) is not required in the case of--
(A) online contact information collected from a child that is used only to respond directly on a one-time basis to a specific request from the child and is not used to recontact the child and is not maintained in retrievable form by the operator;
(B) a request for the name or online contact information of a parent or child that is used for the sole purpose of obtaining parental consent or providing notice under this section and where such information is not maintained in retrievable form by the operator if parental consent is not obtained after a reasonable time;
(C) online contact information collected from a child that is used only to respond more than once directly to a specific request from the child and is not used to recontact the child beyond the scope of that request--
(i) if, before any additional response after the initial response to the child, the operator uses reasonable efforts
to provide a parent notice of the online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(ii) without notice to the parent in such circumstances as the Commission may determine are appropriate, taking into consideration the benefits to the child of access to information and services, and risks to the security and privacy of the child, in regulations promulgated under this subsection;

(B) the name of the child and online contact information (to the extent reasonably necessary to protect the safety of a child participant on the site)--

(i) used only for the purpose of protecting such safety;

(ii) not used to recontact the child or for any other purpose; and

(iii) not disclosed on the site,

if the operator uses reasonable efforts to provide a parent notice of the name and online contact information collected from the child, the purposes for which it is to be used, and an opportunity for the parent to request that the operator make no further use of the information and that it not be maintained in retrievable form; or

(E) the collection, use, or dissemination of such information by the operator of such a website or online service necessary--

(i) to protect the security or integrity of its website;

(ii) to take precautions against liability;

(iii) to respond to judicial process; or

(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

(3) Termination of service.--The regulations shall permit the operator of a website or an online service to terminate service provided to a child whose parent has refused, under the regulations prescribed under paragraph (1)(B)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.

(c) Enforcement.--Subject to sections 1304 and 1306, a violation of a regulation prescribed under subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(d) Inconsistent State Law.--No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this title that is inconsistent with the treatment of those activities or actions under this section.

SEC. 1304. SAFE HARBORS.

(a) Guidelines.--An operator may satisfy the requirements of regulations issued under section 1303(b) by following a set of self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, approved under subsection (b).

(b) Incentives.--

(1) Self-regulatory incentives.--In prescribing regulations under section 1303, the Commission shall provide incentives for self-regulation by operators to implement the protections afforded children under the regulatory requirements described
in subsection (b) of that section.

(2) Deemed compliance.--Such incentives shall include provisions for ensuring that a person will be deemed to be in compliance with the requirements of the regulations under section 1303 if that person complies with guidelines that, after notice and comment, are approved by the Commission upon making a determination that the guidelines meet the requirements of the regulations issued under section 1303.

(3) Expedited response to requests.--The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.

(c) Appeals.--Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

SEC. 1305. ACTIONS BY STATES.

(a) In General.--

(1) Civil actions.--In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 1303(b), the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to--

(A) enjoin that practice;

(B) enforce compliance with the regulation;

(C) obtain damage, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider to be appropriate.

(2) Notice.--

(A) In general.--Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Commission--

(i) written notice of that action; and

(ii) a copy of the complaint for that action.

(B) Exemption.--

(i) In general.--Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(ii) Notification.--In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(b) Intervention.--

(1) In general.--On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) Effect of intervention.--If the Commission intervenes in an action under subsection (a), it shall have the right--

(A) to be heard with respect to any matter that arises in that action; and

(B) to file a petition for appeal.

(3) Amicus curiae.--Upon application to the court, a person whose self-regulatory guidelines have been approved by the
Commission and are relied upon as a defense by any defendant to a proceeding under this section may file amicus curiae in that proceeding.

(c) Construction.--For purposes of bringing any civil action under subsection (a), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to--
   (1) conduct investigations;
   (2) administer oaths or affirmations; or
   (3) compel the attendance of witnesses or the production of documentary and other evidence.

(d) Actions by the Commission.--In any case in which an action is instituted by or on behalf of the Commission for violation of any regulation prescribed under section 1303, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that regulation.

(e) Venue; Service of Process.--
   (1) Venue.--Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.
   (2) Service of process.--In an action brought under subsection (a), process may be served in any district in which the defendant--
      (A) is an inhabitant; or
      (B) may be found.

SEC. 1306. ADMINISTRATION AND APPLICABILITY OF ACT.

(a) In General.--Except as otherwise provided, this title shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(b) Provisions.--Compliance with the requirements imposed under this title shall be enforced under--
   (1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of--
      (A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;
      (B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a) of the Federal Reserve Act (12 U.S.C. 601 et seq. and 611 et seq.), by the Board; and
   (C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;
   (2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;
   (3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.)
by the National Credit Union Administration Board with respect to any Federal credit union;
(4) part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;
(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and
(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.
(c) Exercise of Certain Powers.--For the purpose of the exercise by any agency referred to in subsection (a) of its powers under any Act referred to in that subsection, a violation of any requirement imposed under this title shall be deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (a), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this title, any other authority conferred on it by law.
(d) Actions by the Commission.--The Commission shall prevent any person from violating a rule of the Commission under section 1303 in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title. Any entity that violates such rule shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this title.
(e) Effect on Other Laws.--Nothing contained in the Act shall be construed to limit the authority of the Commission under any other provisions of law.

SEC. 1307. REVIEW.

Not later than 5 years after the effective date of the regulations initially issued under section 1303, the Commission shall--
(1) review the implementation of this title, including the effect of the implementation of this title on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and
(2) prepare and submit to Congress a report on the results of the review under paragraph (1).

SEC. 1308. EFFECTIVE DATE.

Sections 1303(a), 1305, and 1306 of this title take effect on the later of--
(1) the date that is 18 months after the date of enactment of this Act; or
(2) the date on which the Commission rules on the first application filed for safe harbor treatment under section 1304 if the Commission does not rule on the first such application within one year after the date of enactment of
this Act, but in no case later than the date that is 30 months after the date of enactment of this Act.
Final Rule

List of Subjects in 16 CFR Part 312

Children, Children's online privacy protection, Communications, Computer technology, Consumer protection, Data protection, Electronic mail, E-mail, Information practices, Internet, Online service, Privacy, Record retention, Safety, Trade practices, Website, Youth.

Accordingly, the Federal Trade Commission amends 16 CFR chapter I by adding a new Part 312 to read as follows:

PART 312 -- CHILDREN'S ONLINE PRIVACY PROTECTION RULE

Sec.
312.1 Scope of regulations in this part.
312.2 Definitions.
312.3 Unfair or deceptive acts or practices.
312.4 Notice to parents.
312.5 Parental consent.
312.6 Right of parent to review personal information provided by a child.
312.7 Prohibition against conditioning a child's participation on collection of personal information.
312.8 Confidentiality, security, and integrity.
312.9 Enforcement.
312.10 Safe harbors.
312.11 Rulemaking review.

Authority: Secs. 15 U.S.C. 6501 et seq.

§312.1 Scope of regulations in this part.

This Rule implements the Children's Online Privacy Protection Act of 1998, to be codified at 15 U.S.C. 6501, et seq., which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. The effective date of the Rule is April 21, 2000.
§ 312.2 Definitions.

Child means an individual under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:
(a) requesting that children submit personal information online;
(b) enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator’s records; or
(c) the passive tracking or use of any identifying code linked to an individual, such as a cookie.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclosure means, with respect to personal information:
(a) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this subparagraph:
(1) release of personal information means the sharing, selling, renting, or any other means of providing personal information to any third party, and
(2) support for the internal operations of the website or online service means those activities necessary to maintain the technical functioning of the website or online service, or to fulfill a request of a child as permitted by §§ 312.5(c)(2) and (3).

or
(b) making personal information collected from a child by an operator publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-
wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

*Online contact information* means an e-mail address or any other substantially similar identifier that permits direct contact with a person online.

*Operator* means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

(a) among the several States or with 1 or more foreign nations;
(b) in any territory of the United States or in the District of Columbia, or between any such territory and
   (1) another such territory, or
   (2) any State or foreign nation; or
(c) between the District of Columbia and any State, territory, or foreign nation.

This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

*Parent* includes a legal guardian.

*Person* means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

*Personal information* means individually identifiable information about an individual collected online, including:

(a) a first and last name;
(b) a home or other physical address including street name and name of a city or town;
(c) an e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual’s e-mail address;
(d) a telephone number;
(e) a Social Security number;
(f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or
(g) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this paragraph.

Third party means any person who is not (1) an operator with respect to the collection or maintenance of personal information on the website or online service or (2) a person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this Rule for any other purpose.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) receives notice of the operator’s personal information collection, use, and disclosure practices; and
(b) authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children. Provided, however, that a commercial website or online service, or a portion thereof, shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link. In determining whether a commercial website or online service, or a portion thereof, is targeted to children, the Commission will consider its subject matter, visual or audio content, age of models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities and incentives.

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

General requirements. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this Rule. Generally, under this Rule, an operator must:

(a) provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b));
(b) obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5); (c) provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§ 312.6); (d) not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity (§ 312.7); and (e) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

(a) General principles of notice.

All notices under §§ 312.3(a) and 312.5 must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.

(b) Notice on the website or online service.

Under § 312.3(a), an operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children. An operator of a general audience website or online service that has a separate children's area or site must post a link to a notice of its information practices with regard to children on the home page of the children's area.

(1) Placement of the notice.

(i) The link to the notice must be clearly labeled as a notice of the website or online service's information practices with regard to children;
(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and
(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.
(2) **Content of the notice.**

To be complete, the notice of the website or online service’s information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service. **Provided that:** the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators’ privacy policies and use of children’s information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;
(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;
(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means;
(iv) Whether personal information is disclosed to third parties, and if so, the types of business in which such third parties are engaged, and the general purposes for which such information is used; whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator; and that the parent has the option to consent to the collection and use of their child’s personal information without consenting to the disclosure of that information to third parties;
(v) That the operator is prohibited from conditioning a child’s participation in an activity on the child’s disclosing more personal information than is reasonably necessary to participate in such activity; and
(vi) That the parent can review and have deleted the child’s personal information, and refuse to permit further collection or use of the child’s information, and state the procedures for doing so.

(c) **Notice to a parent.**

Under § 312.5, an operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of the
operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(1) Content of the notice to the parent.

(i) All notices must state the following:
   (A) that the operator wishes to collect personal information from the child;
   (B) the information set forth in paragraph 312.4(b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under § 312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such information, and state the means by which the parent can provide verifiable consent to the collection of information.

(iii) In the case of a notice under the exception in § 312.5(c)(3), the notice must also state the following:
   (A) that the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;
   (B) that the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and
   (C) that if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in § 312.5(c)(4), the notice must also state the following:
   (A) that the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;
   (B) that the parent may refuse to permit the use of the information and require the deletion of the information, and how the parent can do so; and
   (C) that if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.
§ 312.5 Parental consent.

(a) General requirements.

(1) An operator is required to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

(b) Mechanisms for verifiable parental consent.

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this provision include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using e-mail accompanied by a PIN or password obtained through one of the verification methods listed above.

Provided that: For the period until April 21, 2002, methods to obtain verifiable parental consent for uses of information other than the "disclosures" covered by § 312.2 of this Rule may also include use of e-mail coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory e-mail to the parent following receipt of consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Operators who use such methods must provide notice that the parent can revoke any consent given in response to the earlier e-mail.
(c) Exceptions to prior parental consent

Verifiable parental consent is required prior to any collection, use and/or disclosure of personal information from a child except as set forth in this paragraph. The exceptions to prior parental consent are as follows:

(1) where the operator collects the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent or providing notice under § 312.4. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;

(2) where the operator collects online contact information from a child for the sole purpose of responding directly on a one-time basis to a specific request from the child, and where such information is not used to recontact the child and is deleted by the operator from its records;

(3) where the operator collects online contact information from a child to be used to respond directly more than once to a specific request from the child, and where such information is not used for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that a parent receives notice and has the opportunity to request that the operator make no further use of the information, as described in § 312.4(c), immediately after the initial response and before making any additional response to the child. Mechanisms to provide such notice include, but are not limited to, sending the notice by postal mail or sending the notice to the parent’s e-mail address, but do not include asking a child to print a notice form or sending an e-mail to the child;

(4) where the operator collects a child’s name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website or online service, where such information is

(i) used for the sole purpose of protecting the child’s safety;
(ii) not used to recontact the child or for any other purpose;
(iii) not disclosed on the website or online service;

and the operator uses reasonable efforts to provide a parent notice as described in § 312.4(c); and
(5) where the operator collects a child’s name and online contact information to the extent reasonably necessary
(i) to protect the security or integrity of its website or online service;
(ii) to take precautions against liability;
(iii) to respond to judicial process; or
(iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety;
and such information is not used for any other purpose.

§ 312.6 Right of parent to review personal information provided by child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:
(1) a description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;
(2) the opportunity at any time to refuse to permit the operator’s further use or future online collection of personal information from that child, and to direct the operator to delete the child’s personal information; and
(3) notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:
(i) ensure that the requestor is a parent of that child, taking into account available technology; and
(ii) not be unduly burdensome to the parent.

(b) Neither an operator nor the operator’s agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator’s further use or collection of personal information from his or her child or has directed the operator to delete the child’s personal information.
§ 312.7 Prohibition against conditioning a child’s participation on collection of personal information.

An operator is prohibited from conditioning a child’s participation in a game, the offering of a prize, or another activity on the child’s disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

§ 312.9 Enforcement.

Subject to §§ 6503 and 6505 of the Children’s Online Privacy Protection Act of 1998, a violation of a regulation prescribed under § 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Safe harbors.

(a) In general.

An operator will be deemed to be in compliance with the requirements of this Rule if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and comment, are approved by the Commission.

(b) Criteria for approval of self-regulatory guidelines.

To be approved by the Commission, guidelines must include the following:

(1) a requirement that operators subject to the guidelines ("subject operators") implement substantially similar requirements that provide the same or greater protections for children as those contained in §§ 312.2-312.9 of this Rule;

(2) an effective, mandatory mechanism for the independent assessment of subject operators’ compliance with the guidelines.

This performance standard may be satisfied by:

(i) periodic reviews of subject operators’ information practices conducted on a random basis either by the industry group promulgating the guidelines or by an independent entity;
(ii) periodic reviews of all subject operators' information practices, conducted either by the industry group promulgating the guidelines or by an independent entity;
(iii) seeding of subject operators' databases, if accompanied by either (i) or (ii); or
(iv) any other equally effective independent assessment mechanism; and
(3) effective incentives for subject operators' compliance with the guidelines. This performance standard may be satisfied by:
(i) mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;
(ii) consumer redress;
(iii) voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines;
(iv) referral to the Commission of operators who engage in a pattern or practice of violating the guidelines; or
(v) any other equally effective incentive.

The assessment mechanism required under paragraph (b)(2) of this section can be provided by an independent enforcement program, such as a seal program. In considering whether to initiate an investigation or to bring an enforcement action for violations of this Rule, and in considering appropriate remedies for such violations, the Commission will take into account whether an operator has been subject to self-regulatory guidelines approved under this section and whether the operator has taken remedial action pursuant to such guidelines, including but not limited to actions set forth in paragraphs (b)(3)(i) through (iii) of this section.

(c) Request for Commission approval of self-regulatory guidelines.

(1) To obtain Commission approval of self-regulatory guidelines, industry groups or other persons must file a request for such approval. A request shall be accompanied by the following:
(i) a copy of the full text of the guidelines for which approval is sought and any accompanying commentary;
(ii) a comparison of each provision of §§ 312.3 through 312.8 of this Rule with the corresponding provisions of the guidelines; and
(iii) a statement explaining:
(A) how the guidelines, including the applicable assessment mechanism, meet the requirements of this Rule; and
(B) how the assessment mechanism and compliance incentives required under paragraphs (b)(2) and (3) of this
section provide effective enforcement of the requirements of this Rule.

(2) The Commission shall act upon a request under this section within 180 days of the filing of such request and shall set forth its conclusions in writing.

(3) Industry groups or other persons whose guidelines have been approved by the Commission must submit proposed changes in those guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under subsection (1). The statement required under subsection (1)(iii) must describe how the proposed changes affect existing provisions of the guidelines.

(d) Records.

Industry groups or other persons who seek safe harbor treatment by compliance with guidelines that have been approved under this Rule shall maintain for a period not less than three years and upon request make available to the Commission for inspection and copying:

(1) consumer complaints alleging violations of the guidelines by subject operators;
(2) records of disciplinary actions taken against subject operators; and
(3) results of the independent assessments of subject operators’ compliance required under paragraph (b)(2) of this section.

(c) Revocation of approval.

The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory guidelines and their implementation do not, in fact, meet the requirements of this Rule.

§ 312.11 Rulemaking review.

No later than five years after the effective date of this Rule, the Commission shall initiate a rulemaking review proceeding to evaluate the implementation of this rule, including the effect of the implementation of this Rule on practices relating to the collection and disclosure of information relating to children, children’s ability to obtain access to information of their choice online, and on the availability of websites directed to children; and report to Congress on the results of this review.
§ 312.12 Severability.

The provisions of this Rule are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

By direction of the Commission.

Donald S. Clark
Secretary
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

GEOCITIES, a corporation.

FILE NO. 9823015

AGREEMENT CONTAINING CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of GeoCities, a corporation ("proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between GeoCities, by its duly authorized officer, and counsel for the Federal Trade Commission that:

1. Proposed respondent GeoCities is a California corporation with its principal office or place of business at 1918 Main Street, Suite 300, Santa Monica, California 90405.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

(a) Any further procedural steps;

(b) The requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

(c) All rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of sixty (60) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may
have to any other manner of service. The complaint may be used in construing the terms of
the order. No agreement, understanding, representation, or interpretation not contained in the
order or the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it
may be liable for civil penalties in the amount provided by law and other appropriate relief
for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Child" or "children" shall mean a person of age twelve (12) or under.

2. "Parents" or "parental" shall mean a legal guardian, including, but not limited to, a
biological or adoptive parent.

3. "Personal identifying information" shall include, but is not limited to, first and last
name, home or other physical address (e.g., school), e-mail address, telephone
number, or any information that identifies a specific individual, or any information
which when tied to the above becomes identifiable to a specific individual.

4. "Disclosure" or "disclosed to third party(ies)" shall mean (a) the release of
information in personally identifiable form to any other individual, firm, or
organization for any purpose or (b) making publicly available such information by any
means including, but not limited to, public posting on or through home pages, pen pal
services, e-mail services, message boards, or chat rooms.

5. "Clearly and prominently" shall mean in a type size and location that are not
obscured by any distracting elements and are sufficiently noticeable for an ordinary
consumer to read and comprehend, and in a typeface that contrasts with the
background against which it appears.

6. "Archived" database shall mean respondent's off-site "back-up" computer tapes
containing member profile information and GeoCities Web site information.

7. "Electronically verifiable signature" shall mean a digital signature or other
electronic means that ensures a valid consent by requiring: (1) authentication
(guarantee that the message has come from the person who claims to have sent it); (2)
integrity (proof that the message contents have not been altered, deliberately or
accidentally, during transmission); and (3) non-repudiation (certainty that the sender
of the message cannot later deny sending it).

8. "Express parental consent" shall mean a parent's affirmative agreement that is
obtained by any of the following means: (1) a signed statement transmitted by postal
mail or facsimile; (2) authorizing a charge to a credit card via a secure server; (3)
e-mail accompanied by an electronically verifiable signature; (4) a procedure that is
specifically authorized by statute, regulation, or guideline issued by the Commission;
or (5) such other procedure that ensures verified parental consent and ensures the
identity of the parent, such as the use of a reliable certifying authority.

9. Unless otherwise specified, "respondent" shall mean GeoCities, its successors and
assigns and its officers, agents, representatives, and employees.

10. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not make any misrepresentation, in any manner, expressly or by implication, about its collection or use of such information from or about consumers, including, but not limited to, what information will be disclosed to third parties and how the information will be used.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with any online collection of personal identifying information from consumers, in or affecting commerce, shall not misrepresent, in any manner, expressly or by implication, the identity of the party collecting any such information or the sponsorship of any activity on its Web site.

III.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall not collect personal identifying information from any child if respondent has actual knowledge that such child does not have his or her parent's permission to provide the information to respondent. Respondent shall not be deemed to have actual knowledge if the child has falsely represented that (s)he is not a child and respondent does not knowingly possess information that such representation is false.

IV.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information, in or affecting commerce, shall provide clear and prominent notice to consumers, including the parents of children, with respect to respondent's practices with regard to its collection and use of personal identifying information. Such notice shall include, but is not limited to, disclosure of:

A. what information is being collected (e.g., "name," "home address," "e-mail address," "age," "interests");

B. its intended use(s);

C. the third parties to whom it will be disclosed (e.g., "advertisers of consumer products," "mailing list companies," "the general public");

D. the consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;

E. the consumer's ability to remove directly or have the information removed from respondent's databases and the means by which (s)he may do so; and

F. the procedures to delete personal identifying information from respondent's databases and any limitations related to such deletion.

Such notice shall appear on the home page of respondent's Web site(s) and at each location
on the site(s) at which such information is collected.

Provided that, respondent shall not be required to include the notice at the locations at which information is collected if such information is limited to tracking information and the collection of such information is described in the notice required by this Part.

Provided further that, for purposes of this Part, compliance with all of the following shall be deemed adequate notice: (a) placement of a clear and prominent hyperlink or button labeled PRIVACY NOTICE on the home page(s), which directly links to the privacy notice screen(s); (b) placement of the information required in this Part clearly and prominently on the privacy notice screen(s), followed on the same screen(s) with a button that must be clicked on to make it disappear; and (c) at each location on the site at which any personal identifying information is collected, placement of a clear and prominent hyperlink on the initial screen on which the collection takes place, which links directly to the privacy notice and which is accompanied by the following statement in bold typeface:

NOTICE: We collect personal information on this site. To learn more about how we use your information click here.

V.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online collection of personal identifying information from children, in or affecting commerce, shall maintain a procedure by which it obtains express parental consent prior to collecting and using such information.

Provided that, respondent may implement the following screening procedure that shall be deemed to be in compliance with this Part. Respondent shall collect and retain certain personal identifying information from a child, including birth date and the child's and parent's e-mail addresses (hereafter "screening information"), enabling respondent to identify the site visitor as a child and to block the child's attempt to register with respondent without express parental consent. If respondent elects to have the child register with it, respondent shall: (1) give notice to the child to have his/her parent provide express parental consent to register; and/or (2) send a notice to the parent's e-mail address for the purpose of obtaining express parental consent. The notice to the child or parent shall provide instructions for the parent to: (1) go to a specific URL on the Web site to receive information on respondent's practices regarding its collection and use of personal identifying information from children and (2) provide express parental consent for the collection and use of such information. Respondent's collection of screening information shall be by a manner that discourages children from providing personal identifying information in addition to the screening information. All personal identifying information collected from a child shall be held by respondent in a secure manner and shall not be used in any manner other than to effectuate the notice to the child or parent, or to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent. The personal identifying information collected shall not be disclosed to any third party prior to the receipt of express parental consent. If express parental consent is not received by twenty (20) days after respondent's collection of the information from the child, respondent shall remove all such personal identifying information from its databases, except such screening information necessary to block the child from further attempts to register or otherwise provide personal identifying information to respondent without express parental consent.

VI.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall provide a reasonable means for consumers, including the parents of children, to obtain removal of their or their children's personal identifying information collected and retained
by respondent and/or disclosed to third parties, prior to the date of service of this order, as follows:

A. Respondent shall provide a clear and prominent notice to each consumer over the age of twelve (12) from whom it collected personal identifying information and disclosed that information to CMG Information Services, Inc., describing such consumer's options as stated in Part VI.C and the manner in which (s)he may exercise them.

B. Respondent shall provide a clear and prominent notice to the parent of each child from whom it collected personal identifying information prior to May 20, 1998, describing the parent's options as stated in Part VI.C and the manner in which (s)he may exercise them.

C. Respondent shall provide the notice within thirty (30) days after the date of service of this order by e-mail, postal mail, or facsimile. Notice to the parent of a child may be to the e-mail address of the parent and, if not known by respondent, to the e-mail address of the child. The notice shall include the following information:

   1. the information that was collected (e.g., "name," "home address," "e-mail address," "age," "interests"); its use(s) and/or intended use(s); and the third parties to whom it was or will be disclosed (e.g., "advertisers of consumer products," "mailing list companies," "the general public") and with respect to children, that the child's personal identifying information may have been made public through various means, such as by publicly posting on the child's personal home page or disclosure by the child through the use of an e-mail account;

   2. the consumer's and child's parents right to obtain access to such information and the means by which (s)he may do so;

   3. the consumer's and child's parent's right to have the information removed from respondent's or a third party's databases and the means by which (s)he may do so;

   4. a statement that children's information will not be disclosed to third parties, including public posting, without express parental consent to the disclosure or public posting;

   5. the means by which express parental consent may be communicated to the respondent permitting disclosure to third parties of a child's information; and

   6. a statement that the failure of a consumer over the age of twelve (12) to request removal of the information from respondent's databases will be deemed as approval to its continued retention and/or disclosure to third parties by respondent.

D. Respondent shall provide to consumers, including the parents of children, a reasonable and secure means to request access to or directly access their or their children's personal identifying information. Such means may include direct access through password protected personal profile, return e-mail bearing an electronically verifiable signature, postal mail, or facsimile.

E. Respondent shall provide to consumers, including the parents of children, a reasonable means to request removal of their or their children's personal identifying information from respondent's and/or the applicable third party's databases or an
assurance that such information has been removed. Such means may include e-mail, postal mail, or facsimile.

F. The failure of a consumer over the age of twelve (12) to request the actions specified above within twenty (20) days after his/her receipt of the notice required in Part VI.A shall be deemed to be consent to the information's continued retention and use by respondent and any third party.

G. Respondent shall provide to the parent of a child a reasonable means to communicate express parental consent to the retention and/or disclosure to third parties of his/her child's personal identifying information. Respondent shall not use any such information or disclose it to any third party unless and until it receives express parental consent.

H. If, in response to the notice required in Part VI.A, respondent has received a request by a consumer over the age of twelve (12) that respondent should remove from its databases the consumer's personal identifying information or has not received the express consent of a parent of a child to the continued retention and/or disclosure to third parties of a child's personal identifying information by respondent within twenty (20) days after the parent's receipt of the notice required in Part VI.B, respondent shall within ten (10) days:

1. Discontinue its retention and/or disclosure to third parties of such information, including but not limited to (a) removing from its databases all such information, (b) removing all personal home pages created by the child, and (c) terminating all e-mail accounts for the child; and

2. Contact all third parties to whom respondent has disclosed the information, requesting that they discontinue using or disclosing that information to other third parties, and remove the information from their databases.

With respect to any consumer over the age of twelve (12) or any parent of a child who has consented to respondent's continued retention and use of personal identifying information pursuant to this Part, such consumer's or parent's continuing right to obtain access to his/her or a child's personal identifying information or removal of such information from respondent's databases shall be as specified in the notice required by Part IV of this order.

I. Within thirty (30) days after the date of service of this order, respondent shall obtain from a responsible official of each third party to whom it has disclosed personal identifying information and from each GeoCities Community Leader a statement stating that (s)he has been advised of the terms of this order and of respondent's obligations under this Part, and that (s)he agrees, upon notification from respondent, to discontinue using or disclosing a consumer's or child's personal identifying information to other third parties and to remove any such information from its databases.

J. As may be permitted by law, respondent shall cease to do business with any third party that fails within thirty (30) days of the date of service of this order to provide the statement set forth in Part VI.I or whom respondent knows or has reason to know has failed at any time to (a) discontinue using or disclosing a child's personal identifying information to other third parties, or (b) remove any such information from their databases. With respect to any GeoCities Community Leader, the respondent shall cease the Community Leader status of any person who fails to provide the statement set forth in Part VI.I or whom respondent knows or has reason to know has failed at
any time to (a) discontinue using or disclosing a child's personal identifying information to other third parties, or (b) remove any such information from their databases.

For purposes of this Part: "third party(ies)" shall mean each GeoCities Community Leader, CMG Information Services, Inc., Surplus Software, Inc. (Surplus Direct/Egghead Computer), Sage Enterprises, Inc. (GeoPlanet/Planetall), Netopia, Inc. (Netopia), and InfoBeat/Mercury Mail (InfoBeat).

VII.

IT IS FURTHER ORDERED that for the purposes of this order, respondent shall not be required to remove personal identifying information from its archived database if such information is retained solely for the purposes of Web site system maintenance, computer file back-up, to block a child's attempt to register with or otherwise provide personal identifying information to respondent without express parental consent, or to respond to requests for such information from law enforcement agencies or pursuant to judicial process. Except as necessary to respond to requests from law enforcement agencies or pursuant to judicial process, respondent shall not disclose to any third party any information retained in its archived database. In any notice required by this order, respondent shall include information, clearly and prominently, about its policies for retaining information in its archived database.

VIII.

IT IS FURTHER ORDERED that for five (5) years after the date of this order, respondent GeoCities, and its successors and assigns, shall place a clear and prominent hyperlink within its privacy statement which states as follows in bold typeface:

NOTICE: Click here for important information about safe surfing from the Federal Trade Commission.

The hyperlink shall directly link to a hyperlink/URL to be provided to respondent by the Commission. The Commission may change the hyperlink/URL upon thirty (30) days prior written notice to respondent.

IX.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall maintain and upon request make available to the Federal Trade Commission for inspection and copying the following:

A. For five (5) years after the last date of dissemination of a notice required by this order, a print or electronic copy in HTML format of all documents relating to compliance with Parts IV through VIII of this order, including, but not limited to, a sample copy of every information collection form, Web page, screen, or document containing any representation regarding respondent's information collection and use practices, the notice required by Parts IV through VI, any communication to third parties required by Part VI, and every Web page or screen linking to the Federal Trade Commission Web site. Each Web page copy shall be accompanied by the URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting information on the World Wide Web; and

Provided that, after creation of any Web page or screen in compliance with this order, respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect respondent's
compliance obligations under this order.

B. For five (5) years after the last collection of personal identifying information from a child, all materials evidencing the express parental consent given to respondent.

X.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities with respect to the subject matter of this order. Respondent shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

XI.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall establish an "information practices training program" for any employee or GeoCities Community Leader engaged in the collection or disclosure to third parties of consumers' personal identifying information. The program shall include training about respondent's privacy policies, information security procedures, and disciplinary procedures for violations of its privacy policies. Respondent shall provide each such current employee and GeoCities Community Leader with information practices training materials within thirty (30) days after the date of service of this order, and each such future employee or GeoCities Community Leader such materials and training within thirty (30) days after (s)he assumes his/her position or responsibilities.

XII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

XIII.

IT IS FURTHER ORDERED that respondent GeoCities, and its successors and assigns, shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.

XIV.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a
complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order's application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this ___________ day of ________________________ 1998.

GEOCITIES

By:

DAVID C. BOHNETT
Chairman

BART A. LAZAR
Seyfarth, Shaw, Fairweather & Geraldson
Counsel for Respondent

RONALD L. PLESSER
Piper & Marbury L.L.P.
Counsel for Respondent

MICHAEL F. BROCKMEYER
Piper & Marbury L.L.P.
Counsel for Respondent

TOBY MILGROM LEVIN
Counsel for the Federal Trade Commission

MARTHA K. LANDSBERG
Counsel for the Federal Trade Commission

DEAN C. FORBES
Counsel for the Federal Trade Commission

CAROLINE G. CURTIN
Counsel for the Federal Trade Commission

APPROVED:
Criminal Law and Procedure Decisions of the 1998-99 Supreme Court Term - Summary and analysis from Solomon L. Wisenberg of Ross, Dixon & Bell, L.L.P.

FindLaw: Laws: Cases and Codes: Supreme Court Opinions


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.

U.S. Supreme Court

Syllabus

RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al. v. AMERICAN CIVIL LIBERTIES UNION et al.

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 "knowin[g]" 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)(3)(B). A
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.

U.S. Supreme Court

No. 96-511

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v. AMERICAN CIVIL LIBERTIES UNION et al.

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

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 "listservs"), "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 addressess. The message is generally stored electronically, sometimes 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." 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." 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. 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." 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 impure search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community." 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." Some of the communications over the Internet that originate in foreign countries are also sexually explicit.

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 the site's content before he or she needs to take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content." For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident. 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."

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, or 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." 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."

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." 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."

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 averrification 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).

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;

...

"(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 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).

On February 8, 1996, immediately after the President signed the statute, 20 plaintiffs 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, and 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)(1) 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.

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 cabin'd 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 abridgement 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 because 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 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.

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 vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry. 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." Ibid.

We distinguished Pacifica in Sable, 492 U.S., at 128, on just this basis. In 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 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 Pacifica because it did not involve a complete ban and because it involved a different medium of communication, id., at 127. We explained that "the dial it medium requires the listener to take affirmative steps to receive the communication." 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." 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." 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.

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, this difference in language will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean. Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our 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. See, e.g., 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 its 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 one of those limitations, standing by itself, is not vague. 38 Each of Miller's additional two prongs--(1) taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lac[k] 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. 39

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.
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 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 "overarching 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 communications. 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 private 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.

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 exploders--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 discoursers 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.

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.

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 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. Jacksonville, 422 U.S. 205, 216 (1975) ("readily subject" to narrowing construction). The open ended character of the CDA provides no guidance whatever 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.

______________________________

U.S. Supreme Court

No. 96-511

JANET RENO, ATTORNEY GENERAL OF THE UNITED STATES, et al., APPELLANTS v.
AMERICAN CIVIL LIBERTIES UNION et al.

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 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 a[n]y 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 Stateshave 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, 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.

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 "tend[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 (ED 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 her 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 (SDNY 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. A. § 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.

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 "invad[e] the area of freedom of expression constitutionally secured to minors." Id., 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 therights 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

[Footnote 1] "Congress shall make no law . . . abridging the freedom of speech." U. S. Const., Amdt. 1.

[Footnote 2] 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.

[Footnote 3] An acronym for the network developed by the Advanced Research Project Agency.

[Footnote 4] Id., at 844 (finding 81).

[Footnote 5] Id., at 831 (finding 3).

[Footnote 6] Id., at 835 (finding 27).

[Footnote 7] Id., at 842 (finding 74).

[Footnote 8] Id., at 836 (finding 36).

[Footnote 9] "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).

[Footnote 10] Id., at 838 (finding 46).

[Footnote 11] Id., at 844 (finding 82).

[Footnote 12] Ibid. (finding 86).

[Footnote 13] Ibid. (finding 85).

[Footnote 14] Id., at 848 (finding 117).

[Footnote 15] Id., at 844-845 (finding 88).

[Footnote 16] Ibid.
[Footnote 17] Id., at 845 (finding 89).

[Footnote 18] Id., at 842 (finding 72).

[Footnote 19] Ibid. (finding 73).

[Footnote 20] 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 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."

[Footnote 21] Ibid. (finding 93).

[Footnote 22] Id., at 846 (finding 102).

[Footnote 23] 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."

[Footnote 24] See Exxon 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 Exxon 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 Exxon 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 Exxon 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).

[Footnote 25] 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.

[Footnote 26] 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 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."

[Footnote 27] 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; Bibliobyytes; 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.

[Footnote 28] 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.


[Footnote 30] 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.

[Footnote 31] 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."

[Footnote 32] 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 lawwe sustained in Ginsberg." Post, at 8.

[Footnote 33] Cf. Pacifica Foundation v. FCC, 556 F. 2d 9, 36 (CADC 1977) (Levánhthal, 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.
[Footnote 34] Juris. Statement 3 (citing 929 F. Supp., at 831 (finding 3)).

[Footnote 35] "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."

[Footnote 36] See Gozlon 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).


[Footnote 38] 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.

[Footnote 39] 413 U.S., at 30 (Determimations 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 Conformers' own assertion that the CDA was intended "to establish a uniform national standard of content regulation." S. Conf. Rep., at 191.


[Footnote 41] 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.

[Footnote 42] 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.

[Footnote 43] 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.

[Footnote 44] 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 authorized its ongoing efforts to prosecute obscenity, child pornography, and child solicitation. See 141 Cong. Rec. S8342 (June 14, 1995) (letter from Kent Markus, Acting Assistant Attorney General, U. S. Department of Justice, to Sen. Leahy).

[Footnote 45] 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.

[Footnote 46] For the full text of §223(e)(5), see n. 26, supra.

[Footnote 47] 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.


[Footnote 49] 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 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).

[Footnote 50] 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").


Cyberspace Communications, Inc., et al. v. Engler

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

Cyberspace, Communications, Inc., Arbornet, Marty Klein, Aids Partnership of Michigan, Art on The Net, Mark Amerika of Alt-X, Web Del Sal, Glad Day Bookshop, Inc., Litline, American Civil Liberties Union, Plaintiffs,

v.

John Engler, Governor of the State of Michigan, and Jennifer M. Granholm, Attorney General of the State of Michigan, Defendants.

No. 99-cv-73 150

Hon. Arthur J. Tarnow

FINDINGS OF FACT AND CONCLUSIONS OF LAW REGARDING PLAINTIFFS' MOTION FOR INJUNCTIVE RELIEF [1]

In 1978, the Michigan Legislature enacted a statute to protect children by prohibiting the distribution of obscene materials to children of this state. 1978 Public Act 33, M.C.L. 722.671 et seq.; M.S.A. 25.254(1) et. seq. In an effort to modernize the statute in light of current technology (and in an effort to make other improvements in the operation of the statute), the Legislature amended the statute by means of 1999 Public Act 33 (hereinafter referred to as the "Act"). The Act primarily attempts to do two things: 1) it adds criminal prohibitions against using computers or the Internet to disseminate sexually explicit materials to minors, and, 2) it changed the language of the statute so that the statute prohibits the dissemination of "sexually explicit" materials to minors rather than "obscene" materials.

The Act, amendments to M.C.L. 722.671 et seq., was signed by Defendant, John Engler, the Governor of Michigan on June 1, 1999. It is set to take effect August 1, 1999. Plaintiffs represent a broad spectrum of organizations and individuals who use the Internet to communicate, disseminate, display and access a broad range of speech and ideas. Plaintiffs include speakers, content providers, and/or Internet service providers (ISPs).

Plaintiffs claim that the Act will adversely impact them because it is unconstitutionally vague or overbroad. They maintain it will have a chilling effect on their freedom of speech under the First Amendment. Plaintiffs communicate online both within and outside of the state of Michigan. Their speech is accessible within and outside of the state of Michigan. For this reason, Plaintiffs further argue that the Act violates the Commerce Clause of the United States Constitution. They have requested this Court issue a preliminary injunction to enjoin the amendments to the statute.

I. The Amended Statute

The central prohibition contained in the amended act is found in M.C.L. 722.675(1); M.S.A. 25.254(5)(1):

A person is guilty of disseminating sexually explicit matter to a minor if that person does either of the following:

(a) Knowingly disseminates to a minor sexually explicit visual or verbal material that is harmful to minors;
(b) Knowingly exhibits to a minor a sexually explicit performance that is harmful to minors.

The Act redefines obscenity as "sexually explicit matter[2]. The Act makes it unlawful to communicate, transmit, display, or otherwise make available by means of the Internet or a computer, computer program, computer system, or computer network this sexually explicit matter. M.C.L. 722.673; M.S.A. 25.254(3). Violation of the statute is a felony punishable by up to two years in prison and a fine of $10,000. 722.675(5); M.S.A. 25.254(5)(5)[3]. Finally, the Act threatens criminal sanctions "if the violation originates, terminates, or both originates and terminates" in the State of Michigan. (M.C.L. 722.675(8), M.S.A. 25.254(5)(8)).

The 1999 P.A. 33 amendments were specifically intended to apply the pre-existing statute's prohibition on the dissemination of sexually explicit matter to communication over the Internet. Because of the anonymous and borderless nature of the Internet, Plaintiffs fear the amendments will subject them to criminal prosecution for the expression of protected speech. They filed suit challenging the Act. Plaintiffs then asked to enjoin the Act's enforcement scheduled to begin August 1, 1999.

A hearing was held on the Motion for a Preliminary Injunction on July 22, 1999. The Court wishes to thank the parties for the thoroughness and quality of the arguments presented.

The following constitutes the Court's findings of fact and conclusions of law:

II. The Internet

Based on the testimony presented at the hearing on the preliminary injunction motion, based on the parties' stipulation of facts, and based on the factual findings of other federal courts, including the United States Supreme Court, [4] the Court finds the following to accurately describe the Internet:

The Nature of the Internet

1. The Internet is a decentralized, global communications medium that links people, institutions, corporations and governments around the world. ACLU 929 F. Supp. at 831; Pataki, 969 F. Supp at 164; Johnson, 4 F. Supp. 2d at 1031.

2. The Internet is a giant computer "network of networks" which interconnects innumerable smaller groups of linked computer networks and individual computers offering a range of digital information including text, images, sound and video, Reno I, 117 S. Ct. at 2334; Pataki, 969 F. Supp. at 164; Johnson, 4 F. Supp. 2d at 1031; Reno II, 31 F. Supp. 2d at 481.

3. While estimates are difficult due to its constant and rapid growth, the Internet is currently believed to connect more than 159 countries, and over 100 million users. ACLU v. Reno, 929 F. Supp. at 831; Johnson, 4 F. Supp. 2d at 1031. The amount of traffic on the Internet is doubling approximately every 100 days.

4. Content ranges from academic writings, to art, to humor, to literature, to medical information, to music, to news, to sexually oriented material. Pataki, 969 F. Supp. at 164; Reno I, 117 S. Ct. at 2335.

5. Sexually explicit material is available on the Internet; however, it is not "the primary type of content on this new medium." ACLU v. Reno, 929 F. Supp. at 844; Pataki, 969 F. Supp. at 164; Reno II, 31 F. Supp. 2d at 484.

6. In addition, at any one time, the Internet serves as the communication medium for tens of thousands of global conversations, political debates, and social dialogues. Pataki, 969 F. Supp. at 165-166.

7. The Internet is distinguishable in important ways from traditional media. It is a revolutionary medium that is dramatically altering traditional views of
communications and community. See ACLU v. Reno, 929 F. Supp. at 843-844. 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. Reno I, 117 S. Ct. at 2336; Reno II, 31 F. Supp. 2d at 484.

8. The Internet is a global medium. Reno II, 31 F. Supp. 2d at 482. At least 40% of the content of the Internet originates abroad. Reno I, 117 S. Ct. at 2334; Reno II, 31 F. Supp. 2d at 484.

9. The Internet also differs from traditional media in that it provides users with an ability to interact with other users and with content. ACLU v. Reno, 929 F. Supp. at 843-44. Unlike radio or television, communications on the Internet do not "invade" an individual's home or appear on one's computer screen unbidden. Id. at 844. Rather, the receipt of information on the Internet "requires a series of affirmative steps more deliberate and directed than merely turning a dial." Reno I, 117 S. Ct. at 2336 (quoting ACLU v. Reno, 929 F. Supp. at 845).

10. Because the Internet presents extremely low entry barriers to publishers and distributors of information, it is an especially attractive method of communicating for non-profit and public interest groups. ACLU v. Reno, 929 F. Supp. at 843; Reno II, 31 F. Supp. 2d at 482.

11. Any person or organization with a computer connected to the Internet can "publish" information. Reno I, 117 S. Ct. at 2335.

12. Also, unlike radio, television, newspapers and books, the Internet is not exclusively, or even primarily, a means of commercial communication. Reno v. ACLU, 929 F. Supp. at 842. In sum, the Internet is "a unique and wholly new medium of worldwide human communication." Reno I, 117 S. Ct. at 2334 (quoting ACLU v. Reno, 929 F. Supp. at 844).

How Individuals Access the Internet

13. Individuals may obtain easy access to the Internet in particular through many educational institutions, businesses, libraries, and individual communities who maintain computer networks linked directly to the Internet and provide account numbers and passwords enabling users to gain access to the network. Reno I, 117 S. Ct. at 2334; Pataki, 969 F. Supp. at 164-165.

14. Internet service providers ("ISPs"), such as plaintiffs Cyberspace Communications and ArborNet.org, offer their subscribers modem access to computers or networks maintained by the ISP which are linked directly to the Internet. ACLU v. Reno, 929 F. Supp. at 832-33; Reno I, 117 S. Ct. at 2334; Pataki, 969 F. Supp. at 165; Reno II, 31 F. Supp. 2d at 482.

Ways of Communicating and Exchanging Information on the Internet

15. Most users of the Internet are provided with a username, password and electronic mail (or "e-mail") address that allow them to sign on to the Internet and to communicate with other users. Pataki, 969 F. Supp. at 165.

16. Many usernames are pseudonyms or pen names that often provide users with a distinct online identity and help to preserve their anonymity. An e-mail sender directs his or her message to a "logical rather than geographic address." Id.

17. The username and e-mail address are the only indicators of the user's identity. Persons communicating with the user will know them only by their username and e-mail address (unless the user reveals other information about herself through her messages). Id. Anonymity of the communicant is both important and valuable to the free exchange of ideas and information on the Internet.

18. Once an individual signs on to the Internet, there are a wide variety of methods for communicating and exchanging information with other users. See generally Reno I, 117 S. Ct. at 2334-35; ACLU v. Reno, 929 F. Supp. at 834-38; Shea, 929 F. Supp. at 927-30; Pataki, 969 F. Supp. at 165; Reno II,
31 F. Supp. 2d at 482-483. The primary methods are:

**E-Mail:** "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." Reno I, 117 5. Ct. at 2335; Pataki, 969 F. Supp. at 165.

**Online Discussion Groups:** Thousands of discussion groups have been organized by individuals, institutions, and organizations on many different computer networks and cover virtually every topic imaginable -- creating a new, global version of the village green. The three most common methods for online discussion are mail exploders, USENET newsgroups, and chat rooms.

**Mail Exploders:** Mail exploders, also called mailing lists, 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. Subscribers can reply to the message by sending a response to the list. Reno I, 117 5. Ct. at 2335. Users of mailing lists typically can add or remove their names from the list automatically, with no direct human involvement. ACLU v. Reno, 929 F. Supp. at 834; Pataki, 969 F. Supp. at 165-166.

**USENET Newsgroups:** "USENET" newsgroups are a 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." Reno I, 117 5. Ct. at 2335 (quoting ACLU v. Reno, 929 F. Supp. at 834-35); see also Pataki, 969 F. Supp. at 166. Users may read or send messages to most newsgroups without a prior "subscription," and there is no way for a speaker who posts an article to most newsgroups to know who is reading her message. Id.

**Chat Rooms:** "Chat rooms" provide additional online discussion forums that allow users to engage in real time dialogue with one or many other users by typing messages and reading the messages typed by others participating in the chat, analogous to a telephone party line. Reno, 929 F. Supp. at 835. 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." Reno I, 117 5. Ct. at 2335 (quoting ACLU v. Reno, 929 F. Supp. at 835); Pataki, 969 F. Supp. at 166.

**The World Wide Web:** The Web allows users to publish documents, also called "Web pages," that can then be accessed by anyone in the world. See generally Reno I, 117 5. Ct. at 2335, and 929 F. Supp. at 836-38; Shea, 930 F. Supp. at 929-30; Pataki, 969 F. Supp. at 166; Reno II, 31 F. Supp. 2d at 484. The Web comprises 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 her own 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. Pataki, 969 F. Supp. at 166. There are Web sites now by large corporations, banks, brokerage houses, newspapers and magazines, and government agencies and courts. Id.

19. There are a number of different ways that Internet users can browse or search for content on the Web: by specific address ("URL") or by "search engines," which are available free of charge to help users navigate the Web, Reno I, 117 5. Ct. at 2335; Pataki, 969 F. Supp. at 166; or by "linking" from one Web page to another. Reno II, 31 F. Supp. 2d at 483. Almost all Web documents contain "links," which are short sections of text or image that refer and link to another Web document. Reno I, 117 5. Ct. at 2335; Pataki, 969 F. Supp. at 166-167; Reno II, 31 F. Supp. 2d at 484. When selected by the user, the "linked" document is automatically displayed, wherever in the world it is actually stored. Reno I, 117 5. Ct. at 2335; 969 F. Supp. at 166; Reno II, 31 F. Supp. 2d at 484. "The Web is thus comparable... to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services." Reno I, 117 5. Ct. at
2335.

20. "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." Reno I, 117 5. Ct. at 2334-35.

21. Once a provider posts content on the Internet, it is available to most other Internet users worldwide. ACLU v. Reno, 929 F. Supp. at 844; Pataki 969 F. Supp. at 167; Johnson, 4 F. Supp. 2d at 1032.

22. For the vast majority of communications over the Internet, including all communications over the Web, by e-mail, newsgroups, mail exploders, and chat rooms, it is not technologically possible for a speaker to determine the age of a user who is accessing such communications. See Reno I 117 S. Ct. at 2336-37 (quoting ACLU v. Reno, 929 F. Supp. at 845) ("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."); Shea, 930 F. Supp. at 941 ("for the vast majority of applications and services available on the Internet, a user has no way of communicating . . . with certainty that the content will not reach a person under eighteen . . . ."); Reno II, 31 F. Supp. 2d at 495 ("the nature of the Web and the Internet is such that Web site operators and content providers cannot know who is accessing their sites, or from where, or how old the users are, unless they take affirmative steps to gather information from the user, and the user is willing to give them truthful responses.").

Thus, these categories of speakers either must make their information available to all users of the Internet, including users who may be minors, or not make it available at all. This is also true for non-Web-based communications by e-mail, newsgroups, mail exploders, and chat rooms.

For Web speakers, the vast majority cannot now determine the age of people accessing their speech and many could not technologically change their site even to request information on age. Also, even for those Web sites, or other Internet speakers, who ask readers to state their age, there is no reasonable method by which the speaker can determine the reliability of that information.

The Availability of User-Based Filtering Programs

24. There are a variety of options available to parents and other users who wish to restrict access to online communications that they might consider unsuitable for minors. See generally-Reno I, 117 5. Ct. at 2337, and ACLU v. Reno, 929 F. Supp. at 838-42; Shea, 930 F. Supp. at 93 1-34.

25. First, there are a variety of user-based software products that allow users to block access to sexually explicit materials on the Web, to prevent minors from giving personal information to strangers by e-mail or in chat rooms, and to keep a log of all online activity that occurs on the home computer. Reno I, 117 5. Ct. at 2337. "The market for this type of [user-based] software is growing, and there is increasing competition among software providers to provide products." AClu v. RENO, 929 F. Supp. at 839.

26. Second, large commercial online services such as America Online provide features to prevent minors from accessing chat rooms and to block access to certain newsgroups based on keywords, subject matter, or specific newsgroup. Reno I, 117 5. Ct. at 2336; Johnson, 4 F. Supp. 2d at 1033; Reno II, 31 F. Supp. 2d at 492.

27. Third, the large online services such as America Online also offer parental control options free of charge to their members. America Online has established an online area designed specifically for children. The "Kids Only" parental control feature allows parents to establish an America Online account for their children that accesses only the "Kids Only" channel on America Online. ACLU v. RENO, 929 F. Supp. at 842.
The Interstate Nature of Online Communication

28. The Internet is wholly insensitive to geographic distinctions, and Internet protocols were designed to ignore rather than document geographic location. Pataki, 969 F. Supp. at 167, 170; Johnson, 4 F. Supp. 2d at 1032.

29. While computers on the network do have "addresses," they are digital addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic indicators. Pataki, 969 F. Supp. at 170.

30. Like the nation's railways and highways, the Internet is by nature an instrument of interstate commerce. Pataki, 969 F. Supp. at 173; Johnson, 4 F. Supp. 2d at 1032. Just as goods and services travel over state borders by truck and train, information flows freely across state borders on the Internet. Pataki, 969 F. Supp. at 173.

31. It is this characteristic which has earned the Internet the nickname, "the information superhighway." 969 F. Sup p. at 161.

32. In fact, no aspect of the Internet can feasibly be closed to users from another state. Pataki, 969 F. Supp. at 171; Johnson, 4 F. Supp. 2d at 1032. There is no way to stop or bar speech at Michigan's border.

33. An Internet user who posts a Web page cannot prevent Michiganders or Oklahomans or Iowans from accessing that page. They will not even know the state residency of any visitors to that site, unless the information is voluntarily (and accurately) given by the visitor. Pataki, 969 F. Supp. at 171; Reno II, 31 F. Supp. 2d at 495; Johnson, 4 F. Supp. 2d at 1032.

34. Participants in chat rooms and online discussion groups also have no way of knowing when participants from a particular state have joined the conversation Id; Johnson, 4 F. Supp. 2d at 1032.

35. Because most e-mail accounts allow users to download their mail from anywhere, it is impossible for someone who sends an e-mail to know with certainty where the recipient is located geographically. Pataki 969 F. Supp. at 171.

36. In addition, the Internet is a redundant series of linked computers over which information often travels randomly. Pataki, 969 F. Supp. at 164, 171. Thus, a message from an Internet user sitting at a computer in New York may travel via one or more other states -- including Michigan -- before reaching a recipient who is also sitting at a computer in New York. Id; Johnson, 4 F. Supp. 2d at 1032.

37. There is no way for an Internet user to prevent his or her message from reaching residents of any particular state. Pataki, 969 F. Supp. at 171; Johnson, 4 F. Supp. 2d at 1032. Similarly, "[o]nce a provider posts its content on the Internet, it cannot prevent that content from entering any community." I, 117 S. Ct. at 2338 (quoting ACLU v. Reno, 929 F. Supp. at 844).

III. Standing

Defendants argue that the threshold issue before the court is that the Plaintiffs lack standing to bring this request for injunctive relief. A plaintiff must have standing to bring or pursue a claim in federal court. Arizonans for Official English v. Arizona, 520 U.S. 43, 117 S.Ct. 1055, 137 L.Ed.2d 170 (1997). Standing is a question of judicial power, and it is the threshold question in every federal case. Warth v. Seldin, 422 U.S. 490, 95 S. Ct. 2205, 45 L.Ed.2d 343 (1975).

Standing encompasses at least three factors:

1) an injury in fact - i.e., an injury which is concrete and actual or imminent, not merely speculative or hypothetical;
which visitors may obtain information about Glad Day Bookshop and the books it makes available. Its Web site is located at www.tiac.net/users/gladday..

- Litline a nonprofit web site set up by the Counsel for Literary Magazines and Presses (CLMP) to provide Internet content for independent literary presses, journals, and organizations. Its Web address is www.litline.org. Litline mainly provides free design and hosting services to eleven independent literary journals and six independent presses, none of which could otherwise afford to go online.

- 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.

All the Plaintiffs justifiably fear prosecution. They have stated that they disseminate on the Internet sexually explicit material which arguably could be deemed "harmful to minors". Absent an injunction they must self-censor their speech on the Internet or else risk prosecution under the Act. These allegations of harm are sufficient to confer standing in this action for declaratory and injunctive relief. "In the context of threats to the right of free expression," it is not necessary "that an individual first be exposed to prosecution in order to have standing to challenge a statute which is claimed to deter the exercise of constitutional rights." Briggs v. Ohio Elections Comm'n, 61 F.3d 487, 492 (6th Cir. 1995) (citations omitted). These allegations of harm also sufficiently support a request for a preliminary injunction. G & V Lounge, Inc. v. Michigan Liquor Control Comm'n, 23 F.3d 1071, 1078-79 (6th Cir. 1994). See also Dombrowski v. Pfister, 380 U.S. 479 (1965); Steffel v. Thompson, 415 U.S. 452 (1974). The Plaintiffs in this case have standing and are entitled to a preliminary injunction, because the Act poses a threat to their rights under the U.S. Constitution. See also, ACLU v. Johnson, 4 F. Supp. 2d at 1027; ALA v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

IV. First Amendment Challenge

The First Amendment to the United States Constitution provides in pertinent part that "Congress shall make no law ... abridging freedom of speech." The prohibitions of the First Amendment extend to the several States through the Fourteenth Amendment.

Defendants argue Ginsberg v. New York 390 U.S. 629, 88 S.Ct. 1274, 20 L.Ed.2d 195 (1968) and Miller v California, 413 U.S. 15, 93 S.Ct. 2607, 37 L.Ed. 2419 (1973), for the proposition that "obscenity" is not protected by the First Amendment. In Ginsberg, the Supreme Court held that a state could prohibit the dissemination to minors of sexually explicit materials which would not be legally obscene with regard to an adult. In Miller, the Supreme Court stated:

This much has been categorically settled by the Court, that obscene material is unprotected by the First Amendment. Kois v. Wisconsin, 408 U.S. 229, 92 S.Ct. 2245, 33 L.Ed.2d 312 (1972); (citations omitted). We acknowledge, however, the inherent dangers of undertaking to regulate any form of expression. State statutes designed to regulate obscene materials must be carefully limited. See Interstate Circuit, Inc. v. Dallas, supra, 390 U.S., at 682-685, 88 S.Ct., at 1302-1305. As a result, we now confine the permissible scope of such regulation to works which depict or describe sexual conduct. That conduct must be specifically defined by the applicable state law, as written or authoritatively construed. A state offense must also be limited to works which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value.

Id. at 23-24, S.Ct. at 26 14-15.
Defendants argue that the Act comports to the specifications of Ginsberg and Miller; therefore, the Act is constitutional. Yet in these cases, the "materials" referenced were magazines and brochures, respectively. Magazines or brochures can be brown bagged or hidden in the backroom of purveyors. With the Internet, you would have to "close the bookstore" because the disseminator and the recipient are not face to face. A magazine can be regulated or censored by the county in which it is located. A person's age can be verified because that person is physically there, and the disseminator can logically be held responsible for conveying "sexually explicit material" to a minor. The Internet does not distinguish between minors and adults in their audience. To comply with the Act, a communicant must speak only in language suitable for children. Even under the guise of protecting minors, the government may not justify the complete suppression of constitutionally protected speech because to do so would "burn the house to roast the pig." Butler v. Michigan, 352 U.S. 380, 383, 77 S.Ct. 524, 525, 1 L.Ed.2d 412 (1957).

The Internet is cyberspace, or an international network of computers. It is virtually impossible to prevent the content of messages from being read by someone under 18. The only way to ascertain an individual's age would be to require submission of a driver's license, birth certificate or some other form of identification. Considering a website may receive ten to a million plus "hits" a day, and many of these websites are established and maintained by even just one publisher, the impossibility of identification checking is understood. With the imposition of the government policing speech and deciding what is acceptable; a user, publisher, disseminator or communicant is faced with a Hobson's choice [6] of shutting down their website (or whatever vehicle of information exchange), or risk prosecution for exercising protected speech.

The Act itself may in fact pass constitutional muster as a permitted regulation of obscenity, as it is quite similarly worded as those statutes upheld by the Supreme Court in Miller and Ginsberg. Defendant argues that a state does have the police power to regulate obscenity within their borders. This is true, but proper focus centers on this Public Act's impact on the Internet. The Internet is an international free flow of ideas and information. Enforcement of this Act would stifle one of the cornerstones of American Society - what Thomas Jefferson called "The Marketplace of Ideas."

The amended statute at issue limits the receipt and communication of information through the Internet based on the content of that information. A content-based limitation on speech will be upheld only where the state demonstrates that the limitation is necessary to serve a compelling state interest and that the narrowly drawn to achieve that end." Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45, 103 S.Ct. 948, 74 L.Ed.2d 794 (1983) (citing Carey v. Brown, 447 U.S. 455, 461, 100 S.Ct. 2286, 65 L.Ed.2d 263 (1980)).

This test involves three distinct inquiries: [7] (1) whether the interests asserted by the state are compelling; (2) whether the limitation is necessary to further those interests; and (3) whether the limitation is narrowly drawn to achieve those interests. Mainstream Loudoun v Board of Trustees of Loudoun County Library. 24 F. Supp. 2d 552, 564-65 (E.D. Va. 1998).

(1). Whether the Defendant's Interests Are Compelling

The Internet offers users quick and relatively simple access to a wide variety of information resources, products and services, and opportunities for interactive communication with millions of people through the use of a computer... Despite the beneficial and education advantages of the Internet's growing network of information, the Internet is not without its problems. One common concern, particularly in light of the number of children who use the Internet, is the relative ease with which children can access materials that their parents might find offensive. House Legislative Analysis, Senate Bill 117 (March 18, 1999)
The Court is quite sympathetic to the attempt of the Michigan legislature to protect minors. Society has a compelling interest in preserving the innocence of their children. Although Defendants have failed to address this prong, there is arguably a compelling state interest to shelter our children from sexually explicit material until maturity. The Supreme Court has recognized such an interest:

"We have recognized that there 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." Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126, 109 S.Ct. 2829, 2836, 106 L.Ed.2d 93 (1989), quoting Ginsberg v. New York, 390 U.S. 629, 639-640, 88 S.Ct. 1274, 1280-81, 20 L.Ed.2d 195 (1968); and New York v. Ferber, 458 U.S. 747, 756-757, 102 S.Ct. 3348, 3354-55, 73 L.Ed.2d 1113 (1982).

(2) Whether the Act is Necessary to Further Those Interests

To satisfy strict scrutiny, defendants must do more than demonstrate that it has a compelling interest; they must also demonstrate that the Act is necessary to further that interest. Defendants "must demonstrate that the recited harms are real, not merely conjectural, and that the regulation will in fact alleviate those harms in a direct and material way." Turner Broadcasting Systems, Inc. v. FCC, 512 U.S. 622, 664, 114 S.Ct. 2445, 2479 L.Ed.2d 497 (1994); see also Johnson, 865 F.Supp. at 1439 ("[S]imply alleging the need to avoid sexual harassment is not enough [;] ... the defendant[] must show that the threat of disruption is actual, material, and substantial."). The defendant bears this burden because "[t]he interest in encouraging freedom of expression in a democratic society outweighs any theoretical but un proven benefit of censorship." Reno v. ACLU, 521 U.S. 844, 117 S.Ct. 2329, 2351, 136 L.Ed.2d 874 (1997).

The Defendants failed to satisfy that the Act will further a compelling interest of the State. Plaintiffs though did submit testimony and documentation that such an Act could produce a result contrary to the desires of society. The free flow of information on the Internet enables a teenager to ask about premarital sex or sexually transmitted diseases with anonymity. Plaintiffs at the hearing read into the record an example of a teenager asking Dr. Marty Klein, a sex therapist in California and plaintiff in this case, who operates a website entitled "Ask Me Anything", about an encounter with her boyfriend that she incorrectly reasoned was not sexual intercourse. Other examples offered at the hearing include submitted transcripts of chat room discussions concerning contraceptives and abstention. Sometimes words were utilized in these discussions which could be construed as "sexually explicit" and "harmful to a minor", which theoretically could subject the disseminator to criminal prosecution.

This would have an adverse affect on public policy. With all Internet participants fearful of criminal prosecution if certain terminology is utilized, the discussions would be stifled to the point that a teenager seeking answers to curious questions concerning a subject foremost on their mind, could not find answers via this medium. Without open discussion of how to prevent being raped or birth control or abstention, there would quite possibly be greater numbers of teenage pregnancy or sexually transmitted diseases. This would be contrary to the interests of the State.

(3) Whether the Act is Narrowly Tailored to Achieve the Compelling Government Interests.

Even if defendants could demonstrate that the Act was reasonably necessary to further compelling state interests, it would still have to show that the Act is narrowly tailored to achieve those interests. The government may effectuate even a compelling interest only "by narrowly drawn regulations designed to serve those interests without unnecessarily interfering with First Amendment freedoms." Sable, 492 U.S. at 126, 109 S.Ct. at 2836. The government must "choose[s] the least restrictive means to further the articulated interest." Id.
Whether Less Restrictive Means Are Available

In Sable, the Court declared unconstitutional a statute banning all "indecent" commercial telephone communications. The Court found that the government could not justify a total ban on communication that is harmful to minors, but not obscene, by arguing that only a total ban could completely prevent children from accessing indecent messages. Id. at 128, 109 S.Ct. 2829. The Court held that without evidence that less restrictive means had "been tested over time," the government had not carried its burden of proving that they would not be sufficiently effective. Id. at 128-29, 109 S.Ct. 2829.

Testimony was offered by Plaintiffs through a qualified Internet expert. Dr. Lorrie Faith Cranor is Senior Technical Staff Member for Secure Systems Research for AT&T Labs-Research in Florham Park, New Jersey. She testified at the hearing that there are many less intrusive, more effective ways to screen harmful material to minors. Some of the ways or methods that this can be accomplished is through the use of currently marketed software that restrict content received. This safe and child-friendly software works off of either a 'white list' or a 'black list' theory. A white list enables a parent to program what areas of the Internet their child will be allowed to enter. A black list prevents a child from venturing into certain pre-programmed areas. Dr. Cranor explained that there is software available to allow parents to filter certain words that may be offensive. Some of these are smart programs that read the context in which the word is presented, e.g. differentiating between a woman's thigh and a chicken thigh. All of these software programs have settings that allow a parent to expand vocabulary words as a child matures. These programs are reasonably priced, usually between $20 to $30.

Many Internet Service Providers (ISPs) allow parents to regulate content with different levels of restriction. The ISP allows parents to establish separate accounts for their children depending on their ages restricting entry to only child-friendly, fun and educational places on the Internet. These areas are usually monitored by employees of the ISP and a communicant that shares offensive language will be blocked when discovered.

It was also noted at the hearing that Internet users have an unwritten code of decency and curiosity. If a communicant is being offensive to other chat room participants, (s)he will be told to stop. If the communicant persists, the offensive communicant will be ‘flamed’ by the group. A flame is a continuous barrage of warnings from others. The warnings can be so continuous and overwhelming that flaming can render the black-listed recipient’s computer unusable online [8].

Dr. Cranor began her list of available methods or ways for which a parent can monitor the content of material to which a child receives, as having a parent sit down and explore with the child. Parental control is the most effective method in overseeing where the child ventures. This can be as simple as placing the computer in a common area of your home, like the living room, so the child can anticipate the presence of an adult. She suggested not placing the computer in the children’s bedroom where they have the exclusion for unbounded exploration. A parent could also place a lock on the computer until such time as a parent can supervise the child. If the parent cannot directly supervise the child’s computer usage, then set limits, much like what shows a child can and cannot watch on television. There are software programs that log all the websites so that a parent can have a record and the child knows that they have to adhere to limits. Finally, the Court takes judicial notice of the fact that every computer is equipped with an on/off switch.

The Court finds that the Act is not narrowly tailored, because less restrictive means are available to further Defendants’ interests. As in Sable, there is no evidence that Defendants has tested any of these means over time.

In summary, Defendants have asserted a broad right to censor the expressive activity of the receipt and communication of information through the Internet with an Act that (1) addresses a compelling government interest...
but is not necessary to further that interest; (2) is not narrowly tailored; and (3) fails to employ the least restrictive means available to further that interest. The Act offends the guarantee of free speech in the First Amendment and is, therefore, unconstitutional.

V. Violation of the Commerce Clause

The Commerce Clause, U.S. Const. Art. I, § 8, cl. 3, contains an express authorization for Congress to "regulate Commerce with foreign Nations, and among the several States ...". A "dormant" or "negative" aspect of this grant of power is that a state's power to impinge on interstate commerce may be limited in some situations. Quill Corp. v. North Dakota, 504 U.S. 298, 112 S.Ct. 1904, 119 L.Ed.2d91 (1992).

Defendants do not dispute that the Act reaches interstate commerce. Rather, they contend that the Act does not discriminate against out-of-state businesses in favor of Michigan businesses. Further, the government argues, any balancing of burdens on interstate commerce with local interests must tip in favor of the local interests asserted in the Act. These contentions fail for the reasons explained in ACLU v. Pataki 969 F. Supp. 160 (S.D.N.Y. 1997).

First, Defendants focus solely on the line of cases which prohibit a state's discrimination against out-of-state businesses. The Commerce Clause reaches further than such discrimination alone. The Commerce Clause also operates to preclude "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." Pataki, 160 F. Supp. at 175 (quoting Healy v. The Beer Institute, 491 U.S. 324, 336 (1989)). Although the Act by its terms regulates speech that "originates" or "terminates" in Michigan, virtually all Internet speech is, as stipulated by Defendants available everywhere including Michigan. A New York speaker must comply with the Act in order to avoid the risk of prosecution in Michigan even though (s) he does not intend his message to be read in Michigan. A publisher of a web page cannot limit the viewing of his site to everyone in the country except for those in Michigan. The Internet has no geographic boundaries. The Act is, as a direct regulation of interstate commerce, aperse violation of the Commerce Clause.

Moreover, even if this Court reaches the balancing of burdens on interstate commerce with local interests asserted in the Act, the Commerce Clause still requires the injunction of this Act. Assuming arguendo the validity of Michigan's interest in the Act, the Act will be wholly ineffective in achieving the asserted goal because nearly half of all Internet communications originate overseas. Pataki, 969 F. Supp. at 177. Just as in Martin-Marietta Corp. v. Bendix Corp., 690 F.2d 558, 566 (6th Cir. 1982), where the Sixth Circuit said: "[W]hile protecting local investors is plainly a legitimate state objective, the state has no legitimate interest in protecting non-resident shareholders"; so to Michigan has no interest in regulating out-of-state communications.

As further explained in Pataki, the chilling effect on Internet communications outside of Michigan greatly outweighs any putative benefit inside Michigan. The Act, and other state statutes like it, would subject the Internet to inconsistent regulations across the nation. Information is a commodity and must flow freely. On this basis alone, the Act may be preliminarily enjoined as a violation of the Commerce Clause.

VI. Fundamental Right of Child Rearing

Although Plaintiffs did not raise the argument that parents have a liberty interest in how their own children are raised [9], nor is the Court's decision today based on that sound principal, the Court believes that there is a good argument to be considered.

As Mr. Justice Harlan wrote, dissenting in Poe v. Ullman, 367 U.S. 497, 55 1-552, 81 S.Ct. 1752, 1781, 6 L.Ed.2d 989 (1951):
Here we have not an intrusion into the home so much as on the life which characteristically has its place in the home. . . . The home derives its pre-eminence as the seat of family life. And the integrity of that life is something so fundamental that it has been found to draw to its protection the principles of more than one explicitly granted Constitutional right.

The full scope of the liberty guaranteed by the Due Process Clause cannot be found in or limited by the precise terms of the specific guarantees elsewhere provided in the Constitution. This 'liberty' is not a series of isolated points picked out in terms of the taking of property; the freedom of speech, press, and religion; the right to keep and bear arms; the freedom from unreasonable searches and seizures; and so on. It is a rational continuum which, broadly speaking, includes a freedom from all substantial arbitrary impositions and purposeless restraints, . . . and which also recognizes, what a reasonable and sensitive judgment must, that certain interests require particularly careful scrutiny of the state needs asserted to justify their abridgment.

Id. at 542-543, 81 S.Ct., at 1776-1777.

Further, the Supreme Court explained in Moore v City of Cleveland, Ohio, 431 U.S. 494, 97 S. Ct. 1932, 52 L.Ed.2d 531 (1977):

But unless we close our eyes to the basic reasons why certain rights associated with the family have been accorded shelter under the Fourteenth Amendment's Due Process Clause, we cannot avoid applying the force and rationale of these precedents to the family choice involved in this case.

Id. at 502, S.Ct. at 1936.

Our decisions establish that the Constitution protects the sanctity of the family precisely because the institution of the family is deeply rooted in this Nation's history and tradition. [footnote omitted]. It is through the family that we inculcate and pass down many of our most cherished values,-moral and cultural.

Id. at 503-504, S.Ct. at 1938.

Although it is difficult in today's society to constantly monitor the activities of children, it is still the right, and duty, of every parent to teach and mold children's concepts of good and bad, right and wrong. This right is no greater than in the confines of one's own home. A family with values will supervise their children. This includes setting limits, and either being there to enforce those limits, or utilizing the available technology to do so. With such less restrictive means to monitor the online activities of children, the government need not restrict the right of free speech guaranteed to adults.

VII. Preliminary Injunction Standard

The district courts must consider the following four factors in determining whether or not to issue a preliminary injunction:

1. whether the movant has a "strong" likelihood of success on the merits;

2. whether the movant would otherwise suffer irreparable injury;

3. whether issuance of a preliminary injunction would cause substantial harm to others; and


The purpose of a preliminary injunction is always to prevent irreparable
(b) Absent an injunction, as the Act violates the Commerce Clause of the United States Constitution.

3. Finally, the Court concludes that the preliminary injunction will not cause substantial harm to others, but rather will serve the public interest, because it will protect the free expression of the millions of Internet users both within and outside of the State of Michigan.

Having reached these findings of fact and conclusions of law, the Court concludes that the Plaintiffs have met their burden for a motion for a preliminary injunction. The threatened injury to Plaintiffs' constitutionally protected speech outweighs any claimed damage to the Defendants. Consequently, the Court grants the Plaintiffs' Motion for a Preliminary Injunction.

NOW, THEREFORE, IT IS HEREBY ORDERED THAT, pursuant to Fed. R. Civ. P. 65(d), the Defendants - as well as their officers, agents, servants, employees, and attorneys, and those persons

in active concert or participation with Defendants - are hereby preliminarily enjoined from enforcing or threatening to enforce 1999 Public Act 33, which amends Sections 3, 5, 6 and 7 (Mich. Comp. Laws §§ 722.673, 722.675, 722.676, and 722.677) of 1978 Public Act 33, M.C.L. §§ 722.671-722.684

Author J. Tarnow
United States District Judge

Date: 7/29/99

1. Law Clerk Philip M. Cavanaugh provided quality research assistance.

2. As defined in M.C.L. 722.673; M.S.A. 25.254(3), as amended.

3. Plaintiffs here do not challenge the Act to the extent that it applies to obscenity. This would allow the Court to enjoin the amendments without nullifying the original statute.


5. Defendants do not challenge that Plaintiffs satisfy the 2nd and 3rd criteria needed for standing as set forth Lujan.

6. Hobson's choice: [After Thomas Hobson (1544-1631), English liveryman, from his requirement that customers take either the horse nearest the stable door or none.] An apparently free choice that offers no actual alternative. Webster's II, New College Dictionary 526 (1995).

7. Defendants' sole argument was that the State of Michigan, by its police powers, could enact this statute as a constitutional ban on obscenity. Therefore, Defendants refused to recognize that the Act regulates free speech and must overcome strict scrutiny.

8. Dr. Cranor also stated that she had done extensive research on solutions to curb unsolicited, unwanted e-mail. She labeled this junk e-mail problem as SPAM - a computer term which is not an acronym, but rather is named after a Monty Python comedy skit.
(1) an analysis of the extent to which local signals are being provided by direct-to-home satellite television providers and by other multichannel video program distributors;

(2) an enumeration of the technical, economic, and other impediments each type of multichannel video programming distributor has encountered; and

(3) recommendations for specific measures to facilitate the provision of local signals to subscribers in unserved and underserved markets by direct-to-home satellite television providers and by other distributors of multichannel video programming service.

TITLE III—TRADEMARK
CYBERPIRACY PREVENTION

SEC. 3001. SHORT TITLE; REFERENCES.

(a) Short Title.—This title may be cited as the “Anticybersquatting Consumer Protection Act”.

(b) References to the Trademark Act of 1946.—Any reference in this title to the Trademark Act of 1946 shall be a reference to the Act entitled “An Act to provide for the registration and protection of trademarks 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 et seq.).
SEC. 3002. CYBERPIRACY PREVENTION.

(a) IN GENERAL.—Section 43 of the Trademark Act
of 1946 (15 U.S.C. 1125) is amended by inserting at the
end the following:

"(d)(1)(A) A person shall be liable in a civil action
by the owner of a mark, including a personal name which
is protected as a mark under this section, if, without re-
gard to the goods or services of the parties, that person—

"(i) has a bad faith intent to profit from that
mark, including a personal name which is protected
as a mark under this section; and

"(ii) registers, traffics in, or uses a domain
name that—

"(I) in the case of a mark that is distinc-
tive at the time of registration of the domain
name, is identical or confusingly similar to that
mark;

"(II) in the case of a famous mark that is
famous at the time of registration of the do-
main name, is identical or confusingly similar
to or dilutive of that mark; or

"(III) is a trademark, word, or name pro-
tected by reason of section 706 of title 18,
United States Code, or section 220506 of title
36, United States Code."
"(B)(i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to—

"(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

"(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

"(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

"(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

"(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

"(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner
or any third party for financial gain without having
used, or having an intent to use, the domain name
in the bona fide offering of any goods or services, or
the person’s prior conduct indicating a pattern of
such conduct;

“(VII) the person’s provision of material and
misleading false contact information when applying
for the registration of the domain name, the per-
son’s intentional failure to maintain accurate contact
information, or the person’s prior conduct indicating
a pattern of such conduct;

“(VIII) the person’s registration or acquisition
of multiple domain names which the person knows
are identical or confusingly similar to marks of oth-
ers that are distinctive at the time of registration of
such domain names, or dilutive of famous marks of
others that are famous at the time of registration of
such domain names, without regard to the goods or
services of the parties; and

“(IX) the extent to which the mark incor-
porated in the person’s domain name registration is
or is not distinctive and famous within the meaning
of subsection (e)(1) of section 43.

“(ii) Bad faith intent described under subparagraph
(A) shall not be found in any case in which the court de-
termines that the person believed and had reasonable
grounds to believe that the use of the domain name was
a fair use or otherwise lawful.

"(C) In any civil action involving the registration,
trafficking, or use of a domain name under this para-
graph, a court may order the forfeiture or cancellation of
the domain name or the transfer of the domain name to
the owner of the mark.

"(D) A person shall be liable for using a domain
name under subparagraph (A) only if that person is the
domain name registrant or that registrant's authorized li-
censee.

"(E) As used in this paragraph, the term 'traffics in'
refers to transactions that include, but are not limited to,
sales, purchases, loans, pledges, licenses, exchanges of cur-
rency, and any other transfer for consideration or receipt
in exchange for consideration.

"(2)(A) The owner of a mark may file an in rem civil
action against a domain name in the judicial district in
which the domain name registrar, domain name registry,
or other domain name authority that registered or as-
signed the domain name is located if—

"(i) the domain name violates any right of the
owner of a mark registered in the Patent and Trade-
mark Office, or protected under subsection (a) or (c); and

"(ii) the court finds that the owner—

"(I) is not able to obtain in personam juris-

(j) diction over a person who would have been a
defendant in a civil action under paragraph (1);

or"

"(II) through due diligence was not able to
find a person who would have been a defendant
in a civil action under paragraph (1) by—

"(aa) sending a notice of the alleged
violation and intent to proceed under this
paragraph to the registrant of the domain
name at the postal and e-mail address pro-
vided by the registrant to the registrar;

and

"(bb) publishing notice of the action
as the court may direct promptly after fil-
ing the action.

"(B) The actions under subparagraph (A)(ii) shall
constitute service of process.

"(C) In an in rem action under this paragraph, a do-
main name shall be deemed to have its situs in the judicial
district in which—
“(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

“(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

“(D)(i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall—

“(I) expeditiously deposit with the court documents sufficient to establish the court’s control and authority regarding the disposition of the registration and use of the domain name to the court; and

“(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

“(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive
or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

"(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.

"(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam."

(b) CYBERPIRACY PROTECTIONS FOR INDIVIDUALS.—

(1) IN GENERAL.—

(A) CIVIL LIABILITY.—Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person’s consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person.

(B) EXCEPTION.—A person who in good faith registers a domain name consisting of the
name of another living person, or a name sub-
stantially and confusingly similar thereto, shall
not be liable under this paragraph if such name
is used in, affiliated with, or related to a work
of authorship protected under title 17, United
States Code, including a work made for hire as
defined in section 101 of title 17, United States
Code, and if the person registering the domain
name is the copyright owner or licensee of the
work, the person intends to sell the domain
name in conjunction with the lawful exploitation
of the work, and such registration is not prohib-
ited by a contract between the registrant and
the named person. The exception under this
subsection shall apply only to a civil action
brought under paragraph (1) and shall in no
manner limit the protections afforded under the
Trademark Act of 1946 (15 U.S.C. 1051 et
seq.) or other provision of Federal or State law.

(2) REMEDIES.—In any civil action brought
under paragraph (1), a court may award injunctive
relief, including the forfeiture or cancellation of the
domain name or the transfer of the domain name to
the plaintiff. The court may also, in its discretion,
award costs and attorneys fees to the prevailing party.

(3) DEFINITION.—In this subsection, the term “domain name” has the meaning given that term in section 45 of the Trademark Act of 1946 (15 U.S.C. 1127).

(4) EFFECTIVE DATE.—This subsection shall apply to domain names registered on or after the date of the enactment of this Act.

SEC. 3003. DAMAGES AND REMEDIES.

(a) REMEDIES IN CASES OF DOMAIN NAME PIRACY.—

(1) INJUNCTIONS.—Section 34(a) of the Trademark Act of 1946 (15 U.S.C. 1116(a)) is amended in the first sentence by striking “(a) or (c)” and inserting “(a), (c), or (d)”.

(2) DAMAGES.—Section 35(a) of the Trademark Act of 1946 (15 U.S.C. 1117(a)) is amended in the first sentence by inserting “, (c), or (d)” after “section 43(a)”.

(b) STATUTORY DAMAGES.—Section 35 of the Trademark Act of 1946 (15 U.S.C. 1117) is amended by adding at the end the following:

“(d) In a case involving a violation of section 43(d)(1), the plaintiff may elect, at any time before final
judgment is rendered by the trial court, to recover, instead
of actual damages and profits, an award of statutory dam-
ages in the amount of not less than $1,000 and not more
than $100,000 per domain name, as the court considers
just.

SEC. 3004. LIMITATION ON LIABILITY.

Section 32(2) of the Trademark Act of 1946 (15
U.S.C. 1114) is amended—

(1) in the matter preceding subparagraph (A)
by striking "under section 43(a)" and inserting
"under section 43(a) or (d)"; and

(2) by redesignating subparagraph (D) as sub-
paragraph (E) and inserting after subparagraph (C)
the following:

"(D)(i)(I) A domain name registrar, a domain
name registry, or other domain name registration
authority that takes any action described under
clause (ii) affecting a domain name shall not be lia-
bile for monetary relief or, except as provided in sub-
clause (II), for injunctive relief, to any person for
such action, regardless of whether the domain name
is finally determined to infringe or dilute the mark.

"(II) A domain name registrar, domain name
registry, or other domain name registration author-
ity described in subclause (I) may be subject to in-

S 1948 IS
junctive relief only if such registrar, registry, or
other registration authority has—

“(aa) not expeditiously deposited with a
court, in which an action has been filed regard-
ing the disposition of the domain name, docu-
ments sufficient for the court to establish the
court’s control and authority regarding the dis-
position of the registration and use of the do-
main name;

“(bb) transferred, suspended, or otherwise
modified the domain name during the pendency
of the action, except upon order of the court; or

“(cc) willfully failed to comply with any
such court order.

“(ii) An action referred to under clause (i)(I) is
any action of refusing to register, removing from
registration, transferring, temporarily disabling, or
permanently canceling a domain name—

“(I) in compliance with a court order
under section 43(d); or

“(II) in the implementation of a reasonable
policy by such registrar, registry, or authority
prohibiting the registration of a domain name
that is identical to, confusingly similar to, or di-
lutive of another’s mark.
“(iii) A domain name registrar, a domain name registry, or other domain name registration authority shall not be liable for damages under this section for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name.

“(iv) If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney’s fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant.

“(v) A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name registrant's domain name is not infringing the mark owner’s mark. The court may grant declaratory relief to the domain name registrant.  

-S 1948 IS
name by such registrant is not unlawful under this
Act. The court may grant injunctive relief to the do-
main name registrant, including the reactivation of
the domain name or transfer of the domain name to
the domain name registrant.”.

SEC. 3005. DEFINITIONS.
Section 45 of the Trademark Act of 1946 (15 U.S.C.
1127) is amended by inserting after the undesignated
paragraph defining the term “counterfeit” the following:
“The term ‘domain name’ means any alphanumeric
designation which is registered with or assigned by any
domain name registrar, domain name registry, or other
domain name registration authority as part of an elec-
tronic address on the Internet.
“The term ‘Internet’ has the meaning given that term
in section 230(f)(1) of the Communications Act of 1934
(47 U.S.C. 230(f)(1)).”.

SEC. 3006. STUDY ON ABUSIVE DOMAIN NAME REGIS-
TIONS INVOLVING PERSONAL NAMES.
(a) IN GENERAL.—Not later than 180 days after the
date of the enactment of this Act, the Secretary of Com-
merce, in consultation with the Patent and Trademark Of-
office and the Federal Election Commission, shall conduct
a study and report to Congress with recommendations on
guidelines and procedures for resolving disputes involving
includes the personal name of another person, in whole or in part, or a name confusingly similar thereto.

SEC. 3007. HISTORIC PRESERVATION.

Section 101(a)(1)(A) of the National Historic Preservation Act (16 U.S.C. 470a(a)(1)(A)) is amended by adding at the end the following: "Notwithstanding section 43(c) of the Act entitled 'An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes', approved July 5, 1946 (commonly known as the 'Trademark Act of 1946' (15 U.S.C. 1125(c))), buildings and structures on or eligible for inclusion on the National Register of Historic Places (either individually or as part of a historic district), or designated as an individual landmark or as a contributing building in a historic district by a unit of State or local government, may retain the name historically associated with the building or structure."

SEC. 3008. SAVINGS CLAUSE.

Nothing in this title shall affect any defense available to a defendant under the Trademark Act of 1946 (including any defense under section 43(c)(4) of such Act or relating to fair use) or a person's right of free speech or expression under the first amendment of the United States Constitution.
SEC. 3009. TECHNICAL AND CONFORMING AMENDMENTS.

Chapter 85 of title 28, United States Code, is amended as follows:

(1) Section 1338 of title 28, United States Codes, is amended—

(A) in the section heading by striking "trade-marks" and inserting "trademarks";

(B) in subsection (a) by striking "trademarks" and inserting "trademarks"; and

(C) in subsection (b) by striking "trademark" and inserting "trademark".

(2) The item relating to section 1338 in the table of sections for chapter 85 of title 28, United States Code, is amended by striking "trade-marks" and inserting "trademarks".

SEC. 3010. EFFECTIVE DATE.

Sections 3002(a), 3003, 3004, 3005, and 3008 of this title shall apply to all domain names registered before, on, or after the date of the enactment of this Act, except that damages under subsection (a) or (d) of section 35 of the Trademark Act of 1946 (15 U.S.C. 1117), as amended by section 3003 of this title, shall not be available with respect to the registration, trafficking, or use of a domain name that occurs before the date of the enactment of this Act.
Uniform Domain Name Dispute Resolution Policy

(As Approved by ICANN on October 24, 1999)

1. **Purpose.** This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at www.icann.org/udrp/udrp-rules-24oct99.htm, and the selected administrative-dispute-resolution service provider's supplemental rules.

2. **Your Representations.** By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else’s rights.

3. **Cancellations, Transfers, and Changes.** We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

   a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;

   b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or

   c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in
accordance with the terms of your Registration Agreement or other legal requirements.


This Paragraph sets forth the type of disputes for which you are required to submit to an mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without
limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding
requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings.
commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at <URL> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration.

Page updated 5-December-99.
Rules for Uniform Domain Name Dispute Resolution Policy

Policy Adopted: August 26, 1999
Implementation Documents Approved: October 24, 1999

Note: These rules are going into effect on a phased implementation schedule that began December 1, 1999 for some cases. Watch www.icann.org/udrp/udrp-schedule.htm for the implementation schedule.

Rules for Uniform Domain Name Dispute Resolution Policy
(the "Rules")

(As Approved by ICANN on October 24, 1999)

Administrative proceedings for the resolution of disputes under the Uniform Dispute Resolution Policy adopted by ICANN shall be governed by these Rules and also the Supplemental Rules of the Provider administering the proceedings, as posted on its web site.

1. Definitions

In these Rules:

**Complainant** means the party initiating a complaint concerning a domain-name registration.

**ICANN** refers to the Internet Corporation for Assigned Names and Numbers.

**Mutual Jurisdiction** means a court jurisdiction at the location of either (a) the principal office of the Registrar (provided the domain-name holder has submitted in its Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain-name holder's address as shown for the registration of the domain name in Registrar's Whois database at the time the complaint is submitted to the Provider.

**Panel** means an administrative panel appointed by a Provider to decide a complaint concerning a domain-name registration.

**Panelist** means an individual appointed by a Provider to be a member of a Panel.

**Party** means a Complainant or a Respondent.

**Policy** means the Uniform Domain Name Dispute Resolution Policy that is incorporated by reference and made a part of the Registration Agreement.

**Provider** means a dispute-resolution service provider approved by ICANN. A list of such Providers appears at www.icann.org/udrp/approved-providers.htm.

**Registrar** means the entity with which the Respondent has registered a domain name that is the subject of a complaint.
Registration Agreement means the agreement between a Registrar and a domain-name holder.

Respondent means the holder of a domain-name registration against which a complaint is initiated.

Reverse Domain Name Hijacking means using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name.

Supplemental Rules means the rules adopted by the Provider administering a proceeding to supplement these Rules. Supplemental Rules shall not be inconsistent with the Policy or these Rules and shall cover such topics as fees, word and page limits and guidelines, the means for communicating with the Provider and the Panel, and the form of cover sheets.

2. Communications

(a) When forwarding a complaint to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint in electronic form (including annexes to the extent available in that form) by e-mail to:

(A) the e-mail addresses for those technical, administrative, and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or "www." followed by the domain name) resolves to an active web page (other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint to any address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other addresses provided to the Provider by Complainant under Paragraph 3(b)(v).

(b) Except as provided in Paragraph 2(a), any written communication to Complainant or Respondent provided for under these Rules shall be made by the preferred means stated by the Complainant or Respondent, respectively (see Paragraphs 3(b)(iii) and 5(b)(iii)), or in the absence of such specification

(i) by telecopy or facsimile transmission, with a confirmation of transmission; or

(ii) by postal or courier service, postage pre-paid and return receipt
requested; or

(iii) electronically via the Internet, provided a record of its transmission is available.

(c) Any communication to the Provider or the Panel shall be made by the means and in the manner (including number of copies) stated in the Provider's Supplemental Rules.

(d) Communications shall be made in the language prescribed in Paragraph 11. E-mail communications should, if practicable, be sent in plaintext.

(e) Either Party may update its contact details by notifying the Provider and the Registrar.

(f) Except as otherwise provided in these Rules, or decided by a Panel, all communications provided for under these Rules shall be deemed to have been made:

(i) if delivered by telexcopy or facsimile transmission, on the date shown on the confirmation of transmission; or

(ii) if by postal or courier service, on the date marked on the receipt; or

(iii) if via the Internet, on the date that the communication was transmitted, provided that the date of transmission is verifiable.

(g) Except as otherwise provided in these Rules, all time periods calculated under these Rules to begin when a communication is made shall begin to run on the earliest date that the communication is deemed to have been made in accordance with Paragraph 2(f).

(h) Any communication by

(i) a Panel to any Party shall be copied to the Provider and to the other Party;

(ii) the Provider to any Party shall be copied to the other Party; and

(iii) a Party shall be copied to the other Party, the Panel and the Provider, as the case may be.

(i) It shall be the responsibility of the sender to retain records of the fact and circumstances of sending, which shall be available for inspection by affected parties and for reporting purposes.

(j) In the event a Party sending a communication receives notification of non-delivery of the communication, the Party shall promptly notify the Panel (or, if no Panel is yet appointed, the Provider) of the circumstances of the notification. Further proceedings concerning the communication and any response shall be as directed by the Panel (or the Provider).

3. The Complaint

(a) Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the Policy and these Rules to any Provider approved by ICANN. (Due to capacity constraints or for other reasons, a Provider's ability to
accept complaints may be suspended at times. In that event, the Provider shall refuse the submission. The person or entity may submit the complaint to another Provider.)

(b) The complaint shall be submitted in hard copy and (except to the extent not available for annexes) in electronic form and shall:

(i) Request that the complaint be submitted for decision in accordance with the Policy and these Rules;

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Complainant and of any representative authorized to act for the Complainant in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Complainant in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy;

(iv) Designate whether Complainant elects to have the dispute decided by a single-member or a three-member Panel and, in the event Complainant elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(v) Provide the name of the Respondent (domain-name holder) and all information (including any postal and e-mail addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a);

(vi) Specify the domain name(s) that is/are the subject of the complaint;

(vii) Identify the Registrar(s) with whom the domain name(s) is/are registered at the time the complaint is filed;

(viii) Specify the trademark(s) or service mark(s) on which the complaint is based and, for each mark, describe the goods or services, if any, with which the mark is used (Complainant may also separately describe other goods and services with which it intends, at the time the complaint is submitted, to use the mark in the future.);

(ix) Describe, in accordance with the Policy, the grounds on which the complaint is made including, in particular,

(1) the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; and

(2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and

(3) why the domain name(s) should be considered as having
been registered and being used in bad faith

(The description should, for elements (2) and (3), discuss any aspects of Paragraphs 4(b) and 4(c) of the Policy that are applicable. The description shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(x) Specify, in accordance with the Policy, the remedies sought;

(xi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;

(xii) State that a copy of the complaint, together with the cover sheet as prescribed by the Provider's Supplemental Rules, has been sent or transmitted to the Respondent (domain-name holder), in accordance with Paragraph 2(b);

(xiii) State that Complainant will submit, with respect to any challenges to a decision in the administrative proceeding canceling or transferring the domain name, to the jurisdiction of the courts in at least one specified Mutual Jurisdiction;

(xiv) Conclude with the following statement followed by the signature of the Complainant or its authorized representative:

"Complainant agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the domain-name holder and waives all such claims and remedies against (a) the dispute-resolution provider and panelists, except in the case of deliberate wrongdoing, (b) the registrar, (c) the registry administrator, and (d) the Internet Corporation for Assigned Names and Numbers, as well as their directors, officers, employees, and agents."

"Complainant certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."

(xv) Annex any documentary or other evidence, including a copy of the Policy applicable to the domain name(s) in dispute and any trademark or service mark registration upon which the complaint relies, together with a schedule indexing such evidence.

(c) The complaint may relate to more than one domain name, provided that the domain names are registered by the same domain-name holder.

4. Notification of Complaint

(a) The Provider shall review the complaint for administrative compliance with the Policy and these Rules and, if in compliance, shall forward the complaint (together
with the explanatory cover sheet prescribed by the Provider's Supplemental Rules) to the Respondent, in the manner prescribed by Paragraph 2(a), within three (3) calendar days following receipt of the fees to be paid by the Complainant in accordance with Paragraph 19.

(b) If the Provider finds the complaint to be administratively deficient, it shall promptly notify the Complainant and the Respondent of the nature of the deficiencies identified. The Complainant shall have five (5) calendar days within which to correct any such deficiencies, after which the administrative proceeding will be deemed withdrawn without prejudice to submission of a different complaint by Complainant.

(c) The date of commencement of the administrative proceeding shall be the date on which the Provider completes its responsibilities under Paragraph 2(a) in connection with forwarding the Complaint to the Respondent.

(d) The Provider shall immediately notify the Complainant, the Respondent, the concerned Registrar(s), and ICANN of the date of commencement of the administrative proceeding.

5. The Response

(a) Within twenty (20) days of the date of commencement of the administrative proceeding the Respondent shall submit a response to the Provider.

(b) The response shall be submitted in hard copy and (except to the extent not available for annexes) in electronic form and shall:

(i) Respond specifically to the statements and allegations contained in the complaint and include any and all bases for the Respondent (domain-name holder) to retain registration and use of the disputed domain name (This portion of the response shall comply with any word or page limit set forth in the Provider's Supplemental Rules.);

(ii) Provide the name, postal and e-mail addresses, and the telephone and telefax numbers of the Respondent (domain-name holder) and of any representative authorized to act for the Respondent in the administrative proceeding;

(iii) Specify a preferred method for communications directed to the Respondent in the administrative proceeding (including person to be contacted, medium, and address information) for each of (A) electronic-only material and (B) material including hard copy;

(iv) If Complainant has elected a single-member panel in the Complaint (see Paragraph 3(b)(iv)), state whether Respondent elects instead to have the dispute decided by a three-member panel;

(v) If either Complainant or Respondent elects a three-member Panel, provide the names and contact details of three candidates to serve as one of the Panelists (these candidates may be drawn from any ICANN-approved Provider's list of panelists);

(vi) Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the complaint;
(vii) State that a copy of the response has been sent or transmitted to the Complainant, in accordance with Paragraph 2(b); and

(viii) Conclude with the following statement followed by the signature of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

(ix) Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

(c) If Complainant has elected to have the dispute decided by a single-member Panel and Respondent elects a three-member Panel, Respondent shall be required to pay one-half of the applicable fee for a three-member Panel as set forth in the Provider's Supplemental Rules. This payment shall be made together with the submission of the response to the Provider. In the event that the required payment is not made, the dispute shall be decided by a single-member Panel.

(d) At the request of the Respondent, the Provider may, in exceptional cases, extend the period of time for the filing of the response. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Provider.

(e) If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.

6. Appointment of the Panel and Timing of Decision

(a) Each Provider shall maintain and publish a publicly available list of panelists and their qualifications.

(b) If neither the Complainant nor the Respondent has elected a three-member Panel (Paragraphs 3(b)(iv) and 5(b)(iv)), the Provider shall appoint, within five (5) calendar days following receipt of the response by the Provider, or the lapse of the time period for the submission thereof, a single Panelist from its list of panelists. The fees for a single-member Panel shall be paid entirely by the Complainant.

(c) If either the Complainant or the Respondent elects to have the dispute decided by a three-member Panel, the Provider shall appoint three Panelists in accordance with the procedures identified in Paragraph 6(e). The fees for a three-member Panel shall be paid in their entirety by the Complainant, except where the election for a three-member Panel was made by the Respondent, in which case the applicable fees shall be shared equally between the Parties.

(d) Unless it has already elected a three-member Panel, the Complainant shall submit to the Provider, within five (5) calendar days of communication of a response in which the Respondent elects a three-member Panel, the names and contact details of three candidates to serve as one of the Panelists. These candidates may be drawn from any ICANN-approved Provider's list of panelists.
(e) In the event that either the Complainant or the Respondent elects a three-member Panel, the Provider shall endeavor to appoint one Panelist from the list of candidates provided by each of the Complainant and the Respondent. In the event the Provider is unable within five (5) calendar days to secure the appointment of a Panelist on its customary terms from either Party's list of candidates, the Provider shall make that appointment from its list of panelists. The third Panelist shall be appointed by the Provider from a list of five candidates submitted by the Provider to the Parties, the Provider's selection from among the five being made in a manner that reasonably balances the preferences of both Parties, as they may specify to the Provider within five (5) calendar days of the Provider's submission of the five-candidate list to the Parties.

(f) Once the entire Panel is appointed, the Provider shall notify the Parties of the Panelists appointed and the date by which, absent exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider.

7. Impartiality and Independence

A Panelist shall be impartial and independent and shall have, before accepting appointment, disclosed to the Provider any circumstances giving rise to justifiable doubt as to the Panelist's impartiality or independence. If, at any stage during the administrative proceeding, new circumstances arise that could give rise to justifiable doubt as to the impartiality or independence of the Panelist, that Panelist shall promptly disclose such circumstances to the Provider. In such event, the Provider shall have the discretion to appoint a substitute Panelist.

8. Communication Between Parties and the Panel

No Party or anyone acting on its behalf may have any unilateral communication with the Panel. All communications between a Party and the Panel or the Provider shall be made to a case administrator appointed by the Provider in the manner prescribed in the Provider's Supplemental Rules.

9. Transmission of the File to the Panel

The Provider shall forward the file to the Panel as soon as the Panelist is appointed in the case of a Panel consisting of a single member, or as soon as the last Panelist is appointed in the case of a three-member Panel.

10. General Powers of the Panel

(a) The Panel shall conduct the administrative proceeding in such manner as it considers appropriate in accordance with the Policy and these Rules.

(b) In all cases, the Panel shall ensure that the Parties are treated with equality and that each Party is given a fair opportunity to present its case.

(c) The Panel shall ensure that the administrative proceeding takes place with due expedition. It may, at the request of a Party or on its own motion, extend, in exceptional cases, a period of time fixed by these Rules or by the Panel.

(d) The Panel shall determine the admissibility, relevance, materiality and weight of the evidence.

(e) A Panel shall decide a request by a Party to consolidate multiple domain name disputes in accordance with the Policy and these Rules.

11. Language of Proceedings
(a) Unless otherwise agreed by the Parties, or specified otherwise in the Registration Agreement, the language of the administrative proceeding shall be the language of the Registration Agreement, subject to the authority of the Panel to determine otherwise, having regard to the circumstances of the administrative proceeding.

(b) The Panel may order that any documents submitted in languages other than the language of the administrative proceeding be accompanied by a translation in whole or in part into the language of the administrative proceeding.

12. Further Statements

In addition to the complaint and the response, the Panel may request, in its sole discretion, further statements or documents from either of the Parties.

13. In-Person Hearings

There shall be no in-person hearings (including hearings by teleconference, videoconference, and web conference), unless the Panel determines, in its sole discretion and as an exceptional matter, that such a hearing is necessary for deciding the complaint.

14. Default

(a) In the event that a Party, in the absence of exceptional circumstances, does not comply with any of the time periods established by these Rules or the Panel, the Panel shall proceed to a decision on the complaint.

(b) If a Party, in the absence of exceptional circumstances, does not comply with any provision of, or requirement under, these Rules or any request from the Panel, the Panel shall draw such inferences therefrom as it considers appropriate.

15. Panel Decisions

(a) A Panel shall decide a complaint on the basis of the statements and documents submitted and in accordance with the Policy, these Rules and any rules and principles of law that it deems applicable.

(b) In the absence of exceptional circumstances, the Panel shall forward its decision on the complaint to the Provider within fourteen (14) days of its appointment pursuant to Paragraph 6.

(c) In the case of a three-member Panel, the Panel’s decision shall be made by a majority.

(d) The Panel’s decision shall be in writing, provide the reasons on which it is based, indicate the date on which it was rendered and identify the name(s) of the Panelist(s).

(e) Panel decisions and dissenting opinions shall normally comply with the guidelines as to length set forth in the Provider’s Supplemental Rules. Any dissenting opinion shall accompany the majority decision. If the Panel concludes that the dispute is not within the scope of Paragraph 4(a) of the Policy, it shall so state. If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse.
of the administrative proceeding.

16. **Communication of Decision to Parties**

(a) Within three (3) calendar days after receiving the decision from the Panel, the Provider shall communicate the full text of the decision to each Party, the concerned Registrar(s), and ICANN. The concerned Registrar(s) shall immediately communicate to each Party, the Provider, and ICANN the date for the implementation of the decision in accordance with the Policy.

(b) Except if the Panel determines otherwise (see Paragraph 4(j) of the Policy), the Provider shall publish the full decision and the date of its implementation on a publicly accessible web site. In any event, the portion of any decision determining a complaint to have been brought in bad faith (see Paragraph 15(e) of these Rules) shall be published.

17. **Settlement or Other Grounds for Termination**

(a) If, before the Panel’s decision, the Parties agree on a settlement, the Panel shall terminate the administrative proceeding.

(b) If, before the Panel’s decision is made, it becomes unnecessary or impossible to continue the administrative proceeding for any reason, the Panel shall terminate the administrative proceeding, unless a Party raises justifiable grounds for objection within a period of time to be determined by the Panel.

18. **Effect of Court Proceedings**

(a) In the event of any legal proceedings initiated prior to or during an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, the Panel shall have the discretion to decide whether to suspend or terminate the administrative proceeding, or to proceed to a decision.

(b) In the event that a Party initiates any legal proceedings during the pendency of an administrative proceeding in respect of a domain-name dispute that is the subject of the complaint, it shall promptly notify the Panel and the Provider. See Paragraph 8 above.

19. **Fees**

(a) The Complainant shall pay to the Provider an initial fixed fee, in accordance with the Provider’s Supplemental Rules, within the time and in the amount required. A Respondent electing under Paragraph 5(b)(iv) to have the dispute decided by a three-member Panel, rather than the single-member Panel elected by the Complainant, shall pay the Provider one-half the fixed fee for a three-member Panel. See Paragraph 5(c). In all other cases, the Complainant shall bear all of the Provider’s fees, except as prescribed under Paragraph 19(d). Upon appointment of the Panel, the Provider shall refund the appropriate portion, if any, of the initial fee to the Complainant, as specified in the Provider’s Supplemental Rules.

(b) No action shall be taken by the Provider on a complaint until it has received from Complainant the initial fee in accordance with Paragraph 19(a).

(c) If the Provider has not received the fee within ten (10) calendar days of receiving the complaint, the complaint shall be deemed withdrawn and the administrative proceeding terminated.
(d) In exceptional circumstances, for example in the event an in-person hearing is held, the Provider shall request the Parties for the payment of additional fees, which shall be established in agreement with the Parties and the Panel.

20. **Exclusion of Liability**

Except in the case of deliberate wrongdoing, neither the Provider nor a Panelist shall be liable to a Party for any act or omission in connection with any administrative proceeding under these Rules.

21. **Amendments**

The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN.

---

Page updated 5-December-99.
U.S. 9th Circuit Court of Appeals

AVERY DENNISON v SUMPTON
9855810

AVERY DENNISON CORPORATION,
Plaintiff-Counter-Defendant-
Appellee,
No. 98-55810
v.
D.C. No.
JERRY SUMPTON, Individually d/b/a
CV-97-00407-JSL
Free View Listings Ltd.; FREE
VIEW LISTINGS, LTD., an Unknown
Entity,
Defendants-Counter-Claimants-
Appellants.

Appeal from the United States District Court
for the Central District of California
J. Spencer Letts, District Judge, Presiding

Argued and Submitted
June 8, 1999--Pasadena, California

Filed August 23, 1999

Before: Dorothy W. Nelson, Stephen Reinhardt, and
Stephen S. Trott, Circuit Judges.

Opinion by Judge Trott

COUNSEL

G. Gervaise Davis, III, Davis & Schroeder, Monterey, Cali-
ifornia, for the defendants-counter-claimants-appellants.

Adrian Mary Pruetz (Argued), and David W. Quinto (On the Briefs), Quinn Emanuel Urquhart Oliver & Hedges, Los Angeles, California, for the plaintiff-counter-defendant-appellee.

OPINION

TROT, Circuit Judge:

Jerry Sumpton and Freeview Listings Ltd. (together, "Appellants") appeal an injunction in favor of Avery Dennison Corp., entered after summary judgment for Avery Dennison on its claims of trademark dilution under the Federal Trademark Dilution Act of 1995, 15 U.S.C. § 1125(c) (Supp. II 1996) (amending the Lanham Trademark Act of 1946, 15 U.S.C. §§ 1051-1127 (1994)), and the California dilution statute, Cal. Bus. & Prof. Code § 14330 (West 1987). The district court published an opinion, 999 F. Supp. 1337 (C.D. Cal. 1998), holding that Appellants' maintenance of domain name registrations for and diluted two of Avery Dennison's separate trademarks, "Avery" and "Dennison." (Note that when referencing Internet addresses, domain-name combinations, e-mail addresses, and other Internet-related character strings, we use the caret symbols ("< >"), in order to avoid possible confusion.) The district court then entered an injunction ordering Appellants to transfer the domain-name registrations to Avery Dennison in exchange for $300 each.

We have jurisdiction under 28 U.S.C. § 1291 (1994).

Because Avery Dennison failed to create a genuine issue of fact on required elements of the dilution cause of action, we reverse and remand with instructions to enter summary judgment for Appellants and to consider Appellants' request for attorneys' fees in light of this decision.

I

Background

We are the third panel of this court in just over a year faced with the challenging task of applying centuries-old trademark law to the newest medium of communication -- the Internet. (See Brookfield Communications, Inc. v. West Coast Ent. Corp., 174 F.3d 1036 (9th Cir. 1999), and Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).) Although we attempt to set out the background facts as clearly as possible, the interested reader may wish to review some of the following sources for a more complete understanding of the Internet: Brookfield, 174 F.3d at 1044-45; Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1230-32 (N.D. Ill. 1996); and Marshall Leaffer, Domain Names, Globalization and Internet Commerce, 6 Ind. J. Global Legal Stud. 139, 139-46 (1998).

Two communicative functions of the Internet are relevant to this appeal: the capacity to support web sites and the corollary capacity to support electronic mail ("e-mail"). A web site, which is simply an interactive presentation of data which a user accesses by dialing into the host computer, can be created by any user who reserves an Internet location -- called an Internet protocol address -- and does the necessary pro-
gramming. Because an Internet protocol address is a string of
integer numbers separated by periods, for example,
<129.137.84.101>, for ease of recall and use a user relies on
a "domain-name combination" to reach a given web site. The
registrar of Internet domain names, Network Solutions, Inc.
("NSI"),1 maintains a database of registrations and translates
entered domain-name combinations into Internet protocol
addresses. When accessing a web site, a user enters the char-
acter string ,2 followed by the reserved domain-
name combination. The domain-name combination must
include a top-level domain ("TLD"), which can be <.com>,
.<net>, <.org>, <.gov> or <.edu>, among others, although
some, like <.gov> and <.edu>, are reserved for specific pur-
poses. The combination also includes a second-level domain
("SLD"), which can be any word not already reserved in com-
bination with the TLD.3 Once a domain-name combination is
reserved, it cannot be used by anybody else, unless the first
registrant voluntarily or otherwise relinquishes its registration.

A web site can be programmed for multiple purposes.
Some merchants maintain a form of "electronic catalog" on
the Internet, permitting Internet users to review products and
services for sale. A web site can also be programmed for e-
mail, where the provider licenses e-mail addresses in the for-
mat , with selected by the e-mail
user. A person or company maintaining a web site makes
money in a few different ways. A site that aids in marketing
goods and services is an asset to a merchant. E-mail providers
make money from licensing fees paid by e-mail users. Money
is also made from advertising and links to other web sites.

II
Facts

Sumpton is the president of Freeview, an Internet e-mail
provider doing business as "Mailbank." Mailbank offers
"vanity" e-mail addresses to users for an "initial" fee of $19.95
and $4.95 per year thereafter, and has registered thousands of
domain-name combinations for this purpose. Most SLDs that
Mailbank has registered are common surnames, although
some represent hobbies, careers, pets, sports interests, favorite
music, and the like. One category of SLDs is titled "Rude"
and includes lewd SLDs, and another category, titled
"Business," includes some common trademark SLDs. Mail-
bank's TLDs consist mainly of <.net> and <.org>, but some
registered domain name combinations, including most in the
"Business" and "Rude" categories, use the TLD <.com>.
Mailbank's surname archives include the domain-name com-
binations and .

Avery Dennison sells office products and industrial fasten-
ers under the registered trademarks "Avery" and "Dennison,"
respectively. "Avery" has been in continuous use since the
1930s and registered since 1963, and "Dennison" has been in
continuous use since the late 1800s and registered since 1908.
Avery Dennison spends more than $5 million per year adver-
tising its products, including those marketed under the sepa-
rate "Avery" and "Dennison" trademarks, and the company
boasts in the neighborhood of $3 billion in sales of all of its
trademarks annually. No evidence indicates what percentage
of these dollar figures apply to the "Avery" or "Dennison"
trademarks. Avery Dennison maintains a commercial pres-
ence on the Internet, marketing its products at
and , and maintaining registrations for
several other domain-name combinations, all using the TLD <.com>.

Avery Dennison sued Appellants, alleging trademark dilution under the Federal Trademark Dilution Act and California Business and Professional Code § 14330. Avery Dennison also sued NSI, alleging contributory dilution and contributory infringement. The district court granted summary judgment to NSI on Avery Dennison's claims. The district court then concluded as a matter of law that the disputed trademarks were famous and denied summary judgment to Appellants and granted summary judgment to Avery Dennison on its dilution claims, entering an injunction requiring Appellants to transfer the registrations to Avery Dennison. 983 F. Supp. at 1342.

III

Trademark Law


Until recently, federal law provided protection only against infringement of a registered trademark, or the unregistered trademark analog, unfair competition. See SS 32 & 43(a) of the Lanham Trademark Act of 1946, as amended, 15 U.S.C. SS 1114, 1125(a) (1994). These causes of action require a plaintiff to prove that the defendant is using a mark confusingly similar to a valid, protectable trademark of the plaintiff's. Brookfield, 174 F.3d at 1046.

[1] Many states, however, have long recognized another cause of action designed to protect trademarks: trademark dilution. Lori Krafe-Jacobs, Comment, Judicial Interpretation of the Federal Trademark Dilution Act of 1995, 66 U.Cin. L. Rev. 659, 660-62 (1998) (discussing the evolution of the dilution doctrine). With the 1995 enactment of the Federal Trademark Dilution Act, dilution became a federal-law concern. Unlike infringement and unfair competition laws, in a dilution case competition between the parties and a likelihood of confusion are not required to present a claim for relief. See 15 U.S.C. S 1127 (Supp. II 1996) (definition of "dilution"); Leslie F. Brown, Note, Avery Dennison Corp. v. Sumpton, 14 Berkeley Tech. L.J. 247, 249 (1999). Rather, injunctive relief is available under the Federal Trademark Dilution Act if a plaintiff can establish that (1) its mark is famous; (2) the defendant is making commercial use of the mark in commerce; (3) the defendant's use began after the plaintiff's mark became famous; and (4) the defendant's use presents a likelihood of dilution of the distinctive value of the mark. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1324 (9th Cir. 1998) (interpreting 15 U.S.C. S 1125(c)(1)).

[2] California's dilution cause of action is substantially similar, providing relief if the plaintiff can demonstrate a "[l]ikelihood of injury to business reputation or of dilution of the distinctive quality of a mark . . . , notwithstanding the absence of competition between the parties or the absence of
Basis for Trademark Protection, 40 Harv. L. Rev. 813 (1927) (proposing a cause of action for dilution); Krafte-Jacobs, supra, at 689-91. Dilution causes of action, much more so than infringement and unfair competition laws, tread very close to granting "rights in gross" in a trademark. See 3 McCarthy, supra, S 24:108. In the infringement and unfair competition scenario, where the less famous a trademark, the less the chance that consumers will be confused as to origin, see AMP Inc. v. Sleekcraft Boats, 599 F.2d 341, 349 (9th Cir. 1979), a carefully-crafted balance exists between protecting a trademark and permitting non-infringing uses. In the dilution context, likelihood of confusion is irrelevant. See 15 U.S.C. S 1127; Cal. Bus. & Prof. Code S 14330; Panavision, 141 F.3d at 1326. If dilution protection were accorded to trademarks based only on a showing of inherent or acquired distinctiveness, we would upset the balance in favor of overprotecting trademarks, at the expense of potential non-infringing uses. See Fruit of the Loom, 994 F.2d at 1363 ("[The plaintiff] would sweep clean the many business uses of this quotidian word.").

We view the famousness prong of both dilution analyses as reinstating the balance -- by carefully limiting the class of trademarks eligible for dilution protection, Congress and state legislatures granted the most potent form of trademark protection in a manner designed to minimize undue impact on other uses. See San Francisco Arts & Athletics, Inc. v. United States Olympic Comm., 483 U.S. 522, 564 n.25 (1987) (Brennan, J., dissenting) (citing 2 J. McCarthy, Trademarks & Unfair Competition S 24:16, at 229 (2d ed. 1984)) (discussing limits on the dilution doctrine that help prevent overprotection of trademarks).

Therefore, to meet the "famousness" element of protection under the dilution statute, " 'a mark[must] be truly prominent and renowned.' " I.P. Lund Trading ApS v. Kohler Co., 163 F.3d 27, 46 (1st Cir. 1998) (quoting 3 McCarthy, supra, S 24.91). In a 1987 report, which recommended an amendment to the Lanham Act to provide a federal dilution cause of action, the Trademark Review Commission of the United States Trademark Association emphasized the narrow reach of a dilution cause of action: "We believe that a limited category of trademarks, those which are truly famous and registered, are deserving of national protection from dilution." Trademark Review Commission, Report & Recommendations, 77 Trademark Rep. 375, 455 (Sept.-Oct. 1987).

[3] The Federal Trademark Dilution Act lists eight non-exclusive considerations for the famousness inquiry, 15 U.S.C. S 1125(c)(1)(A)-(H), which are equally relevant to a famousness determination under Business and Professional Code S 14330, see Panavision, 141 F.3d at 1324 ("Panavision's state law dilution claim is subject to the same analysis as its federal claim."). These are:

(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 or 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 mark's 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 . . . on the principal register.


[4] We note the overlap between the statutory famousness considerations and the factors relevant to establishing acquired distinctiveness, which is attained "when the purchasing public associates the [mark] with a single producer or source rather than just the product itself." First Brands Corp. v. Fred Meyer, Inc., 809 F.2d 1376, 1383 (9th Cir. 1987). Proof of acquired distinctiveness is a difficult empirical inquiry which a factfinder must undertake, Taco Cabana Int'l, Inc. v. Two Pesos, Inc., 932 F.2d 1113, 1119-20 & n.7 (5th Cir. 1991), aff'd, 505 U.S. 763 (1992), considering factors including:

[1] whether actual purchasers . . . associate the [mark] with [the plaintiff]; [2] the degree and manner of [the plaintiff's] advertising; [3] the length and manner of [the plaintiff's] use of the [mark]; and [4] whether [the plaintiff's] use of the [mark] has been exclusive.


[5] However, the Federal Trademark Dilution Act and Business and Professional Code § 14330 apply "only to those marks which are both truly distinctive and famous, and therefore most likely to be adversely affected by dilution." S. Rep. No. 100-515, at 42 (emphasis added). The Trademark Review Commission stated that "a higher standard must be employed to gauge the fame of a trademark eligible for this extraordinary remedy." 77 Trademark Rep. at 461. Thus, "[t]o be capable of being diluted, a mark must have a degree of distinctiveness and 'strength' beyond that needed to serve as a trademark." 3 McCarthy, supra, § 24:109; see also Krafte-Jacobs, supra, at 690 ("If all marks are distinctive, and a showing of distinctiveness meets the element of fame, what marks would be outside the protection of the FTDA?[T]he FTDA does not indicate that any particular degree of distinctiveness should end the inquiry." (interpreting the Federal Trademark Dilution Act)). We have previously held likewise under California Business and Professional Code § 14330. Accuride Int'l, Inc. v. Accuride Corp., 871 F.2d 1531, 1539
Applying the famousness factors from the Federal Trademark Dilution Act to the facts of the case at bench, we conclude that Avery Dennison likely establishes acquired distinctiveness in the "Avery" and "Dennison" trademarks, but goes no further. Because the Federal Trademark Dilution Act requires a showing greater than distinctiveness to meet the threshold element of fame, as a matter of law Avery Dennison has failed to fulfill this burden.

Distinctiveness

[6] We begin with the first factor in the statutory list: "inherent or acquired distinctiveness." S 1125(c)(1)(A). No dispute exists that "Avery" and "Dennison" are common surnames -- according to evidence presented by Appellants, respectively the 775th and 1768th most common in the United States. A long-standing principle of trademark law is the right of a person to use his or her own name in connection with a business. See Howe Scale Co. v. Wyckoff, Seamans & Benedict, 198 U.S. 119, 140 (1905). This principle was incorporated into the Lanham Act, which states that a mark that is "primarily merely a surname" is not protectable unless it acquires secondary meaning. 15 U.S.C. S 1052(e)(4), (f) (1994); Abraham Zion Corp. v. Lebow, 761 F.2d 93, 104 (2d Cir. 1985); see L.E. Waterman Co. v. Modern Pen Co., 235 U.S. 88, 94 (1914) (pre-Lanham Act case stating that protection from confusion is available to the holder of a surname trademark that has acquired public recognition); Horlick's Malted Milk Corp. v. Horluck's, Inc., 59 F.2d 13, 15 (9th Cir. 1932) (pre-Lanham Act case limiting the defendant's right to use his surname as a trademark where the name had acquired public recognition from the efforts of a competitor). Avery Dennison cannot claim that "Avery" and "Dennison" are inherently distinctive, but must demonstrate acquired distinctiveness through secondary meaning.

The drafters of the Federal Trademark Dilution Act continued the concern for surnames when adding protection against trademark dilution to the federal scheme. On early consideration of the Act, the report from the Senate Judiciary Committee emphasized: "[T]he committee intended to give special protection to an individual's ability to use his or her own name in good faith." S. Rep. No. 100-515, at 43 (1988). The Federal Trademark Dilution Act imports, at a minimum, the threshold secondary-meaning requirement for registration of a surname trademark.

[7] Avery Dennison maintains registrations of both "Avery" and "Dennison" on the principal register, prima facie evidence that these marks have achieved the secondary meaning required for protection from infringement and unfair competition. See Americana Trading, 966 F.2d at 1287. We reject Appellants' argument that the distinctiveness required for famousness under the Federal Trademark Dilution Act is inherent, not merely acquired distinctiveness. See 15 U.S.C. S 1125(c)(1)(A) (referencing "inherent or acquired distinctiveness"). However, because famousness requires a showing greater than mere distinctiveness, the presumptive secondary meaning associated with "Avery" and "Dennison" fails to persuade us that the famousness prong is met in this case.
Overlapping Channels of Trade

[8] We next consider the fifth and sixth factors of the statutory inquiry: the channels of trade for the plaintiff's goods and the degree of recognition of the mark in the trading areas and channels of trade used by plaintiff and defendant. S 1125(c)(1)(E), (F). The drafters of the Federal Trademark Dilution Act broke from the Trademark Review Commission's recommendation that only marks "which have become famous throughout a substantial part of the United States" could qualify for protection. Report & Recommendation, 77 Trademark Rep. at 456. Instead, fame in a localized trading area may meet the threshold element under the Act if plaintiff's trading area includes the trading area of the defendant. S. Rep. No. 100-515, at 43; Washington Speakers Bureau, Inc. v. Leading Auths., Inc., 33 F. Supp. 2d 488, 503-04 (E.D. Va. 1999) (citing I.P. Lund, 163 F.3d at 46; Teletech Customer Care Mgt., Inc. v. TeleTech Co., 977 F. Supp. 1407, 1413 (C.D. Cal. 1997)). The rule is likewise for specialized market segments: specialized fame can be adequate only if the "diluting uses are directed narrowly at the same market segment." Washington Speakers, 33 F. Supp. 2d at 503. No evidence on the record supports Avery Dennison's position on these two prongs of the famousness inquiry.

[9] In Teletech, fame in a narrow market segment was present when the plaintiff showed "that the Teletech Companies may be the largest provider of primarily inbound integrated telephone and Internet customer care nationwide." 977 F. Supp. at 1409. The defendant was "a contractor providing engineering and installation services to the telecommunications industry," and maintained the domain-name combination. Id. at 1409-10. The court held that the showing on the threshold element under the Federal Trademark Dilution Act was adequate to qualify for a preliminary injunction. Id. at 1413. In Washington Speakers, both the plaintiff and defendant were in the business of scheduling speaking engagements for well-known lecturers. 33 F. Supp. 2d at 490, 503 & n.31 (citing cases). In the instant case, by contrast, Appellants' sought-after customer base is Internet users who desire vanity e-mail addresses, and Avery Dennison's customer base includes purchasers of office products and industrial fasteners. No evidence demonstrates that Avery Dennison possesses any degree of recognition among Internet users or that Appellants direct their e-mail services at Avery Dennison's customer base.

Use of the Marks by Third Parties

[10] The seventh factor, "the nature and extent of use of the same . . . marks by third parties," S 1125(c)(1)(G), undercuts the district court's conclusion as well. All relevant evidence on the record tends to establish that both "Avery" and "Dennison" are commonly used as trademarks, both on and off the Internet, by parties other than Avery Dennison. This evidence is relevant because, when "a mark is in widespread use, it may not be famous for the goods or services of one business." Report & Recommendation, 77 Trademark Rep. at 461; see Accuride, 871 F.2d at 1539 (affirming the district court's holding that widespread use of elements of a trade-
mark helped to defeat a dilution claim).

The record includes copies of five trademark registrations for "Avery" and "Avery's," a computer printout of a list of several businesses with "Avery" in their names who market products on the Internet, and a list of business names including "Avery," which, according to a declaration submitted by NSI, is a representative sample of over 800 such businesses. The record also contains a computer printout of a list of several businesses with "Dennison" in their names which market products on the Internet and a list of business names including "Dennison," a representative sample of over 200 such businesses. Such widespread use of "Avery" and "Dennison" makes it unlikely that either can be considered a famous mark eligible for the dilution cause of action.

4

Other Famousness Factors

[11] Avery Dennison argues that evidence of extensive advertising and sales, international operations, and consumer awareness suffices to establish fame. We agree that the remaining four statutory factors in the famousness inquiry likely support Avery Dennison's position. Both "Avery" and "Dennison" have been used as trademarks for large fractions of a century and registered for decades. Avery Dennison expends substantial sums annually advertising each mark, with some presumable degree of success due to Avery Dennison's significant annual volume of sales. In addition, Avery Dennison markets its goods internationally. See 15 U.S.C. S 1125(c)(1)(B)-(D), (G). However, we disagree that Avery Dennison's showing establishes fame.

Avery Dennison submitted three market research studies regarding perceptions of the "Avery" and "Avery Dennison" brands. Discussion groups through which one study was conducted were formed "using Avery client lists," and produced the conclusion that the "Avery" name has "positive associations . . . among current customers." Surveyed persons in the other two studies were mostly "users and purchasers of office products" and "[o]ffice supply consumers." The one consumer group that did not necessarily include office supply purchasers for businesses was still required to be "somewhat" or "very" familiar with Avery products in order to be counted.

[12] Avery Dennison's marketing reports are comparable to a survey we discussed in Anti-Monopoly, Inc. v. General Mills Fun Group, Inc., 684 F.2d 1316 (9th Cir. 1981), proving only the near tautology that consumers already acquainted with Avery and Avery Dennison products are familiar with Avery Dennison. See id. at 1323-24. The marketing reports add nothing to the discussion of whether consumers in general have any brand association with "Avery" and "Avery Dennison," and no evidence of product awareness relates specifically to the "Dennison" trademark. Although proper consumer surveys might be highly relevant to a showing of fame, we reject any reliance on the flawed reports submitted by Avery Dennison.

[13] Finally, Avery Dennison -- like any company marketing on the Internet -- markets its products worldwide. See 15 U.S.C. S 1125(c)(1)(D). By itself, this factor carries no weight; worldwide use of a non-famous mark does not establish fame. Because famousness requires more than mere dis-
tinctiveness, and Avery Dennison's showing goes no further than establishing secondary meaning, we hold that Avery Dennison has not met its burden to create a genuine issue of fact that its marks are famous. Avery Dennison's failure to fulfill its burden on this required element of both dilution causes of action mandates summary judgment for Appellants.

5

Likelihood of Confusion Remains Irrelevant

[14] We recognize that our discussion of the breadth of fame and overlapping market segments begins to sound like a likelihood of confusion analysis, and we agree with Avery Dennison that likelihood of confusion should not be considered under either the Federal Trademark Dilution Act or Business and Professional Code S 14330. However, as we discuss above, the famousness element of the dilution causes of action serves the same general purpose as the likelihood of confusion element of an infringement or unfair competition analysis -- preventing the trademark scheme from granting excessively broad protection at the expense of legitimate uses. See Fruit of the Loom, 994 F.2d at 1363 ("Whittling away will not occur unless there is at least some subliminal connection in a buyer's mind between the two parties' uses of their marks."). The close parallels between the two analyses are therefore not surprising; nor do they cause us concern.

B

Commercial Use

Addressing the second element of a cause of action under the Federal Trademark Dilution Act, the district court held that Appellants' registration of and constituted commercial use. 999 F. Supp. at 1339-40. We disagree.

[15] Commercial use under the Federal Trademark Dilution Act requires the defendant to be using the trademark as a trademark, capitalizing on its trademark status. See Panavision, 141 F.3d at 1325. Courts have phrased this requirement in various ways. In a classic "cybersquatter" case, one court referenced the defendants "intention to arbitrage" the registration which included the plaintiff's trademark. Intermatic, 947 F. Supp. at 1239. Another court, whose decision we affirmed, noted that the defendant "traded on the value of marks as marks." Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1303 (C.D. Cal. 1996), aff'd, 141 F.3d 1316 (9th Cir. 1998). In our Panavision decision, we considered the defendant's "attempt to sell the trademarks themselves." 141 F.3d at 1325.

[16] All evidence in the record indicates that Appellants register common surnames in domain-name combinations and license e-mail addresses using those surnames, with the consequent intent to capitalize on the surname status of "Avery" and "Dennison." Appellants do not use trademarks qua trademarks as required by the caselaw to establish commercial use. Rather, Appellants use words that happen to be trademarks for their non-trademark value. The district court erred in holding that Appellants' use of and constituted commercial use under the Federal Trademark Dilution Act, and this essential element of the dilution causes of action likewise mandates summary judgment for Appellants.
Dilution

The district court then considered the dilution requirement under both statutes, holding that Appellants' use of and caused dilution, or a likelihood of dilution, of "Avery" and "Dennison." 999 F. Supp. at 1340-41. We hold that genuine issues of fact on this element of the causes of action should have precluded summary judgment for Avery Dennison.

Two theories of dilution are implicated in this case. First, Avery Dennison argues that Appellants' conduct is the cybersquatting dilution that we recognized in Panavision. See 141 F.3d at 1326-27. Second, Avery Dennison argues that Appellants' conduct in housing the and domain names in the same database as various lewd SLDs causes tarnishment of the "Avery" and "Dennison" marks.

1

Cybersquatting

[17] Cybersquatting dilution is the diminishment of "the capacity of the [plaintiff's] marks to identify and distinguish the [plaintiff's] goods and services on the Internet." Panavision, 141 F.3d at 1326 (quoting the Panavision district court, 945 F. Supp. at 1304). We recognized that this can occur if potential customers cannot find a web page at . Id. at 1327; see also Brookfield, 174 F.3d at 1045 ("The Web surfer who assumes that " 'X'.com' will always correspond to the web site of company X or trademark X will, however, sometimes be misled."). Dilution occurs because " '[p]rospective' users of plaintiff's services ... may fail to continue to search for plaintiff's own home page, due to anger, frustration or the belief that plaintiff's home page does not exist." Panavision, 141 F.3d at 1327 (quoting Jews for Jesus v. Brodsky, 993 F. Supp. 282, 306-07 (D.N.J. 1998)).

[18] In the instant case, Appellants registered the TLD <.net>, rather than <.com>, with the SLDs and . As we recognized in Panavision, <.net> applies to networks and <.com> applies to commercial entities. 141 F.3d at 1318. Evidence on the record supports this distinction, and courts applying the dilution cause of action to domain name registrations have universally considered registrations. See Brown, Note, supra, at 251-54 (discussing cases); id. at 262-63 (addressing the <.com> versus <.net> distinction). Although evidence on the record also demonstrates that the <.com> and <.net> distinction is illusory, a factfinder could infer that dilution does not occur without a registration. This genuine issue of fact on the question of cybersquatting dilution should have prevented summary judgment for Avery Dennison.

2

Tarnishment

[19] Tarnishment occurs when a defendant's use of a mark similar to a plaintiff's presents a danger that consumers will form unfavorable associations with the mark. See Hasbro,
Inc. v. Internet Ent. Group, Ltd., 40 U.S.P.Q.2d 1479, 1480
(W.D. Wash. 1996) (as a domain-name
combination for a sexually explicit web site diluted plaintiff's
trademark, "Candyland," for a children's game); 3 McCarthy,
supra, S 24:104. The district court did not reach Avery Denni-
son's claims regarding tarnishment.

[20] Avery Dennison offers, as an alternative ground for
affirming the district court, the fact that Appellants house
and at the same web site as lewd
domain-name registrations. However, the evidence likewise
indicates that to move from or dennison.net> to
a lewd SLD requires "linking" through the Mailbank home
page, which might remove any association with the "Avery"
and "Dennison" trademarks that the Internet user might have
had. See Fruit of the Loom, 994 F.2d at 1363 (requiring some
connection between the two parties' uses of their marks).
Whether Appellants' use of the registrations presents a danger
of tarnishment is an issue of fact that could not be decided on
summary judgment.

D

Injunction

[21] Under the Federal Trademark Dilution Act and Business
and Professional Code S 14330, an injunction may issue
if Appellants' conduct dilutes, or is likely to dilute, Avery
& Prof. Code S 14330. Actual success on the merits of a claim
is required for a permanent injunction. Walters v. Reno, 145
F.3d 1032, 1048 (9th Cir. 1998). Because we conclude that
the district court erred as a matter of law in finding "Avery" and
"Dennison" to be famous and Appellants' use of
and to be commercial use, and because genu-
ine issues of material fact existed as to whether Appellants'
use of the domain-name registrations dilutes or is likely to
dilute Avery Dennison's marks, the district court necessarily
erred in granting Avery Dennison an injunction.

VI

Attorneys' Fees

Finally, we address Appellants' application for attorneys' fees. The Lanham Act permits an award of attorneys' fees to a prevailing party "in exceptional cases." 15 U.S.C. S 1117(a).
Imposition of attorneys' fees is warranted if "a plaintiff's case is groundless, unreasonable, vexatious, or pursued in bad faith." Stephen W. Boney, Inc. v. Boney Servs., Inc., 127
F.3d 821, 826-27 (9th Cir. 1997) (quoting Scott Fetzer Co. v.
Williamson, 101 F.3d 549, 555 (8th Cir. 1996)).

As an appellate court, we are ill-equipped to determine
Avery Dennison's motivation for bringing and pursuing this
litigation. We therefore remand the attorneys' fees question to
the district court for determination.

VII

Conclusion

We reverse the district court's summary judgment in favor
of Avery Dennison and remand with instructions to enter
summary judgment for Sumpton and Freeview. We also
remand Appellants' request for attorneys' fees for a determination by the district court. Finally, we deny Avery Dennison's motion to strike portions of Appellants' brief, and we deny Appellants' request for judicial notice.

REVERSED and REMANDED. the end

FOOTNOTES

1 At the time of publication of this opinion, NSI is no longer the exclusive registrar of domain names. A new competitive scheme is being implemented by the Commerce Department, and one competitor, "register.com," is currently in operation. See generally Jeri Clausing, 3-Week Delay in Opening Up Internet Name Registration, N.Y. Times, June 28, 1999, at B10.

2 Although initial character strings other than are also used, see, e.g., Michael K. Lindsey, Just an Address, Los Angeles Daily Journal, Friday, June 18, 1999, at 7 (citing a web page at ), we only consider, which stands for "World-Wide Web."

3 Some specific "vulgar" words and a few words that are prevented by federal statute from being used by private entities are not available as SLDs.

4 Although the famousness of "Avery" and "Dennison" is disputed, no dispute exists on the third element of dilution under Panavision: Appellants' use must begin after the marks became famous. Any fame that Avery Dennison's marks have acquired existed before November, 1996, when Appellants' use began.

5 The Trademark Review Commission's recommended amendment is very similar to the language of the eventually-enacted Federal Trademark Dilution Act. The main difference relevant to the famousness inquiry is that the Commission's recommendation only permitted a cause of action to the owner of a registered mark, while the owner of any protectable mark or trade name can bring a cause of action under the enacted version of the Federal Trademark Dilution Act.

6 The Clamp court specifically discussed a trademark in a product configuration, rather than in a word or symbol, and the First Brands and Two Pesos courts dealt with trade dress. However, the analysis is the same. See Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 768 -76 (1992) (applying the rules applicable to unfair competition to trade dress); Clamp Mfg. Co. v. Enco Mfg. Co., 870 F.2d 512, 515-16 (9th Cir. 1989) (applying the rule for acquired distinctiveness to the design of a product); see generally Graeme B. Dinwoodie, Reconceptualizing the Inherent Distinctiveness of Product Design Trade Dress, 75 N.C. L. Rev. 471 (1997) (discussing the application of trademark infringement and unfair competition law to product design and trade dress).
UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA  
PLAYBOY ENTERPRISES INC.  
a Delaware corporation,  
Plaintiff,  
v.  
TERRI WELLES,  
Defendant.  
CASE NO. 98-CV-0413-K (JFS)  
April 22, 1998  
ORDER DENYING PLAINTIFF'S  
MOTION FOR PRELIMINARY INJUNCTION  

On February 27, 1998, plaintiff Playboy Enterprises Inc. (PEI) filed a Complaint against defendant Terri Welles. The Complaint consists of five causes of action. 1) trademark infringement pursuant to 15 U.S.C. §1114(1); 2) false designation of origin and unfair competition under 15 U.S.C. §1125(a); 2) dilution of trademarks pursuant to 15 U.S.C. 1125(c), 4) trademark infringement and unfair competition under California common law; 5) unfair competition in violation of Cal. Bus. & Prof. Code §17200, et seq.


I. BACKGROUND

The following background facts are taken from the parties' contentions in their papers, but the court does not make any ultimate findings of fact with respect to this case. Plaintiff Playboy Enterprises, Inc. (PEI) is an international publishing and entertainment company. Since 1953, PEI has published Playboy magazine, a widely popular magazine with approximately ten (10) million readers each month. PEI also publishes numerous specialty magazines such as Playboy's Playmate Review, Playboy's Playmates of the Year, and Playboy's Calendar Playmates among other publications. In addition to its publishing ventures, PEI produces television programming for cable and direct-to-home satellite transmission and sells and licenses various goods and services including videos.

PEI has established two websites. According to plaintiff, its free website, http://www.playboy.com has become one of the most popular sites on the Web and is used to promote its magazine, goods, and services. Its other website, called the Playboy Cyber Club, http://www.cyber.playboy.com, is devoted to promoting current and former PEI models.

PEI owns federally registered trademarks for the terms Playboy Playmate, Playmate of the Month, and Playmate of the Year. The term Playmate of the Year is sometimes abbreviated "PMOY" PEI does not have a federally registered trademark in the abbreviation PMOY, although PEI argues that "PMOY" is worthy of trademark protection because it is a well-known abbreviation for the trademark Playmate of the Year.

Defendant Terri Welles is a self-employed model and spokesperson, who began her modeling career with Playboy magazine in 1980. In May of 1980, Ms. Welles appeared on the cover of Playboy
magazine and was subsequently featured as the Playmate of the Month in the December 1980 issue. Ms. Welles received the Playmate of the Year award in June of 1981. Since 1980 Ms. Welles has appeared in no less than thirteen (13) issues of Playboy magazine and eighteen (18) newsstand specials published by PEI. Defendant claims that she has always referred to herself since 1980 as a Playmate or Playmate of the Year with the knowledge of PEI.

On June 29, 1997 Ms. Welles opened a website, http://www.terriwelles.com, which includes photographs of herself and others (both nude and clothed), a fan club posting board, an autobiography section, and a listing of current events and personal appearances. The domain name for defendant’s site is "terriwelles," the heading for the website is "Terri Welles--Playmate of the Year 1981," and title of the link page is "Terri-Welles--Playboy Playmate of the Year 1981." Each of the pages uses "PMOY ’81" as a repeating watermark in the background. According to defendant, eleven (11) of the fifteen (15) free web pages include a disclaimer at the bottom of the pages in varying font sizes depending on the page, which indicates that the website is not endorsed by PEI; the disclaimer reads as follows: "This site is neither endorsed, nor sponsored by, nor affiliated with Playboy Enterprises, Inc. PLAYBOY PLAYMATE OF THE YEAR and PLAYMATE OF THE MONTH are registered trademarks of Playboy Enterprises, Inc." Defendant uses the terms Playboy and Playmate along with other terms within the keywords section of the meta tags, which constitutes the internal index of the website used by some search engines.

The site contains link pages to other erotic, adult-oriented websites. It also contains advertising "banners" for those types of websites.

Since May of 1997, defendant has been in contact with plaintiff about the design and creation of her website. Defendant claims that plaintiff, through Marcia Terrones, the director of the "Rights and Permission" department at PEI, informed her that she could identify herself as the Playmate of the Year 1981 but that she could not reproduce the rabbit head logo on her proposed website. Various communications between defendant and plaintiff ensued. According to defendant, PEI, through Hugh Hefner, initially complimented her website and encouraged her to use the title Playmate of the Year 1981. However, Mr. Hefner later informed defendant that use of PEI’s trademarks were restricted; instead, he invited defendant to join PEI's new Cyber Club. Defendant refused this invitation, and PEI continued to demand that defendant remove the Playmate of the Year title from the home page as well as remove the PMOY watermark from the background.

Plaintiff has moved for a preliminary injunction which would enjoin defendant from 1) using the trademarked term Playmate of the Year in the title of the home page and link page; 2) from using the watermark PMOY ‘81 in the background; and 3) from using the trademarked terms Playboy and Playmate in the meta-tagging of defendant's site. Therefore, the task before the court is to determine whether a preliminary injunction against defendant is warranted in this instance.

II. STANDARD OF LAW

To be entitled to a preliminary injunction, a party must either (1) a combination of probable success on the merits and a possibility of irreparable harm, or (2) the existence of serious questions on the merits and the balance of hardships weighing heavily in its favor. Vision Sports v. Melskine, 888 F.2d 609, 612 (9th Cir. 1988). These are not two distinct tests, but ends of a continuum in which the required showing of harm "varies inversely with the required showing of meritoriousness." Rodeo Collection v. West Seventh, 812 F.2d 1215, 1217 (9th Cir. 1987) (citation omitted). "Thus, a moving party need not demonstrate that [it] risks irreparable injury, but [it] must at least show that [it] will suffer a degree of hardship that outweighs the hardship facing the opposing party if the injunction is not issued. Similarly, a moving party need not demonstrate that [it] will succeed on the merits, but must at least show that [its] cause presents serious questions of law worthy of litigation." Topanga Press, Inc. v. City of Los Angeles, 989 F.2d 1524, 1528 (9th Cir. 1993).

III. DISCUSSION

In general, plaintiff argues that defendant's use of the Playboy and Playmate trademarks in conjunction
with her website is likely to cause confusion, mistake or deception. See Complaint at ¶ 32. Specifically, PEI avers that these alleged infringements are harming it and its trademark since websurfing consumers are likely to believe that defendant's website is authorized, sponsored or otherwise approved of by PEI when it is not. Id. Defendant, on the other hand, contends that her use of the title Playmate of the Year and the abbreviation PMOY is merely a descriptive use of those terms so as to identify herself to her customers. She argues that any use of PEI's trademarked terms is merely used in an editorial fashion.

In this motion, plaintiff concentrates on defendant's use of the Playmate of the Year in Ms. Welles' web page heading and link page, he use of the PMOY "81 term as a watermark in the web page background, and her use of the Playboy and Playmate marks as meta tags. These appear to be the only infringements alleged by PEI; accordingly, the court will focus on these three particular issues in this order.

Based on these alleged infringements, plaintiff states five causes of action against defendant in its Complaint. However, in this motion, PEI moves for a preliminary injunction on the basis of only three of those causes of action: (First Cause of Action) federal trademark infringement; (Second Cause of Action) false designation of origin under section 43(a) of the Lanham Act; and (Third Cause of Action) dilution under section 43(e) of the Lanham Act. Defendant refers to these two causes of action as the trademark causes of action and can be treated together. Plaintiff does not make direct reference to the remaining causes of action which are related state law causes of action. Therefore, the court will not address those issues. The court will now address whether a preliminary injunction is warranted in this case.

A. Irreparable Harm

"In copyright and trademark cases, irreparable injury is presumed upon a showing of likelihood of success." Dr. Seuss Enters. v. Penguin Books USA, Inc., 924 F.Supp. 1559, 1574 (SD. Cal. 1996), aff'd. 109 F.3d 1394 (9th Cir. 1997). Thus, the court will examine the plaintiff's likelihood of success on the three causes of action upon which it relies.

B. Likelihood of Success in Trademark Causes of Action

Plaintiff asserts that defendant is infringing on its registered trademarks in violation of Section 32(1) of the Lanham Act, 15 U.S.C. §1114(1), and that said infringement is causing confusion, mistake, or deception which constitutes false designation of origin and unfair competition is violation of Section 43(a) of the Lanham Act, 15 U.S.C. §1125(a). The purpose of trademarks is to allow for customer identification of the manufacturer or sponsor of a good or the provider of a service. See New Kids on the Block v. New Am. Pub., Inc., 971 F.2d 302, 305 (9th Cir. 1992).

It is undisputed that PEI owns federally-registered trademarks for the words Playboy Playmate, Playmate of the Month, and Playmate of the Year. The term Playboy has gained widespread public recognition and is distinctive due in large part to the long-standing success and popularity of Playboy magazine and related publications from PEI. See Playboy Enters., Inc. v. Chuckleberry Publishing, Inc., 687 F.2d 563, 566-67 (2d Cir. 1982) (holding that the Playboy mark is distinctive, widely recognized, and of great value). However, the other trademarks such as Playmate are not only trademarks related to Playboy magazine, but they are titles bestowed upon particular models who appear in that magazine. From the papers submitted and the oral arguments, it appears that the terms Playmate, Playmate of the Month, and Playmate of the Year are titles which Playboy magazine awards to certain Playboy models, who then use the titles to describe themselves. Much like Academy Award winners, all the crowned Miss Americas, and the Heisman Trophy winners, Playboy Playmates are given a title which becomes part of their identity and adds value to their name. Indisputably, these winners represent the awarding organization or sponsor, but the title becomes part of who they are to the public.

In the case of Playboy Playmates, PEI encourages these select models to use their titles for their self-promotion and the promotion of its magazine and assorted goods and services. In the case of Ms. Welles, it appears that PEI had no objections to her use of the terms Playmate of the Year or Playboy Playmate until she launched her competing website.3 In oral argument, PEI conceded that these models may use their title for their own benefit, as in the title of an autobiography. PEI also admitted that Ms.
Welles is not contractually restricted from using the terms *Playmate of the Month* or *Playmate of the Year* based on her previous contracts with PEI. However, it contends that Ms. Welles may not trade on PEI's marks so as to compete with PEI, specifically, PEI argues that the prominent use of its marks to attract the attention of potential customers is a trademark infringement as well as a dilution of its marks.

In papers submitted, the parties engage in an extensive analysis of whether defendant's use of PEI's trademarks creates confusion among users. Indeed, the dispositive legal issue in the standard trademark case concerns "customer confusion." See *WCVB-TV v. Boston Athletic Ass'n*, 926 F.2d 42, 44 (1st Cir. 1991). The Ninth Circuit has articulated an eight-factor test which the court may consider in determining the likelihood of confusion: 1) the strength of the mark; 2) proximity or relatedness of the goods; 3) similarity in appearance, sound, and meaning of the marks; 4) evidence of actual confusion; 5) degree to which the marketing channels converge; 6) type of goods and degree of care customers are likely to exercise in purchasing them; 7) evidence of the intention of defendant in selecting and using the alleged infringing name; and 8) likelihood that the parties will expend their product lines. See *Metro Pub. Ltd. v. San Jose Mercury News*, 987 F.2d 637, 640 (9th Cir. 1993); see also *Century 21 Real Estate Corp. v. Sandlin*, 846 F.2d 1175, 1178-79 (9th Cir. 1988) (applying a similar six-factor test). These factors are simply helpful guidelines for the determination of potential customer confusion. See *Metro Pub.*, 987 F.2d at 640.

This case, however, is not a standard trademark case and does not lend itself to the systematic application of the eight factors. In the case at bar, defendant has used the terms *Playmate of the Year* and its abbreviation PMOY on her website. She has also used the terms *Playboy* and *Playmate* as meta tags for her site so that those using search engines on the Web can find her website if they were looking for a *Playboy* Playmate. The problem in this case is that the trademarks that defendant uses, and the manner in which she uses them, describe her and identify her. This raises a question of whether there is a "fair use" of these marks pursuant to 15 U.S.C. §§1115(b)(4) and 1125(c)(4). See *New Kids*, 971 F.2d at 306 (noting that the "fair use" defense arises when the trademark also describes a person, a place or an attribute of a product). Terri Welles was and is the "Playmate of the Year for 1981." Plaintiff has conceded this fact and has not submitted any evidence for the court to conclude that PEI may prevent defendant from using that term to identify herself and her award; as noted above, PEI conceded that there are no contractual agreements between it and defendant which restrict her use of any of the marks. Thus, defendant has raised a "fair use" defense which must be overcome by the plaintiff before a potential infringement under Section 43(a) of the Lanham Act or trademark dilution under Section 43(c) of the Lanham Act may be found.

In a case where the "mark is used only to describe the goods or services of [a] party, or their geographic origin," trademark law recognizes a "fair use" defense. *Id.* (quoting 15 U.S.C. §1115(b)(4)).

Title 15 U.S.C. §1115(b)(4) states the following:

That the use of the name, term, or device charged to be infringement is a use, otherwise than as a mark, of the party's individual name in his own business, or of the individual name of anyone in privity with such party, or of a term or device which is descriptive of and used fairly and in good faith only to describe the goods or services or such party, or their geographic origin ... *Id.* "The 'fair use' defense, in essence, forbids a trademark registrant to appropriate a descriptive term for his exclusive use and so prevent others from accurately describing a characteristic of their goods." *New Kids*, 971 F.2d at 306 (quoting *Soweco, Inc. v. Shell Oil Co.*, 617 F.2d 1178, 1185 (5th Cir. 1980)). In the case at bar, Ms. Welles has used the trademark term *Playmate of the Year* to identify and describe herself. As the court noted above, Ms. Welles earned the title of "Playboy Playmate of the Year" in 1981 and has used that title ever since, without objection from PEI.

From the exhibits submitted with the parties' paper and presented at oral argument, it is evident that Ms. Welles has minimized her references to *Playboy* on her website and has not attempted to trick consumers into believing that they are viewing a *Playboy*-endorsed website. In *Volkswagenwerk Aktiengesellschaft v. Church*, 411 F.2d 350, 352 (9th Cir. 1969), the Ninth Circuit held that the defendant was able to advertise that he repaired Volkswagen vehicles as long as he did not do so in a manner "which is likely
to suggest to his prospective customers that he is part of Volkswagen's organization of franchised dealers and repairmen." **Id.** In the case at bar, Ms. Welles has not created a Playboy-related website. She does not use **Playboy** or **Playmate** in her domain name, she does not use the classic **Playboy** bunny logo, she inserted disclaimers which clearly state that the website is not endorsed by PEI, and the font of the **Playmate of the Year 1981** title is not recognizable as a **Playboy** magazine font.

It is clear that defendant is selling Terri Welles and only Terri Welles on the website. There is no overt attempt to confuse the websurfer into believing that her site is a Playboy-related website. In this case, then, defendant's use of the term **Playmate of the Year 1981** "is descriptive of and used fairly and in good faith only to describe [herself]." 15 U.S.C. §1115(b)(4). As such, the use of the abbreviation **PMOY '81** is also permissible since it makes reference to her title as Playmate of the Year 1981. Since the court finds that "POMY '81 is a fair description of Ms. Terri Welles, it is not necessary to rule on whether the abbreviation **PMOY** is a protected trademark.

With respect to the meta tags, the court finds there to be no trademark infringement where defendant has used plaintiff's trademarks in good faith to index the content of her website. The meta tags are not visible to the websurfer although some search engines rely on these tags help websurfers find certain websites. Much like the subject index of a card catalog, the meta tags give the websurfer using a search engine a clearer indication of the content of a website. The use of the term **Playboy** is not an infringement because it references not only her identity as a "**Playboy Playmate of the Year 1981.**" but it may also reference the legitimate editorial uses of the term **Playboy** contained in the text of defendant's website. Plaintiff conceded, both in its papers and in oral argument, that defendant may properly use the term **Playboy** in an editorial fashion (i.e. in reference to the Playboy Mansion). Therefore, the court finds that defendant has not infringed on defendant's trademarks by using them in her website meta tags.

Since defendant is entitled to the "fair use" defense pursuant to 15 U.S.C. §1115(b)(4), it is not necessary to determine the likelihood of confusion in this case. However, even if the court were to determine the likelihood of confusion in this case, it does not appear that there is a likelihood that the websurfer would think that Ms. Welles' website is endorsed or sanctioned in way by PEI. Even if Ms. Welles were not entitled to the fair use defense, plaintiff has failed to demonstrate that there is a likelihood of confusion for websurfers. Certainly, the PEI trademarks are strong and are used by PEI to sell adult entertainment on the Internet. Defendant claims she is selling a different class of goods since she is offering her promotional services and related goods like her line of cigars. However, it appears that PEI and Terri Welles are in competition for websurfers who pay money for on-line erotica, regardless of what the underlying promotion is.

Other factors weigh in defendant's favor. Though she is using the trademarks, she has done nothing else to make her use identical to the **Playboy** trademark. There is not bunny logo, the font for the terms is different, and there is no other indication that PEI is sponsoring the website. Plaintiff has presented no empirical evidence to show that there is actual confusion among consumers. Though not necessary, the lack of any such demonstration weighs in defendant's favor. Finally, it appears that defendant has used the trademarks in good faith. She has removed some of the references per PEI's request, has not used the bunny logo, and has added a disclaimer to the vast majority of her free web pages. See Consumers Union of U.S. v. General Signal Corp., 724 F.2d 1044, 1053 (2d Cir. 1983) ("Disclaimers are a favored way of alleviating consumer confusion as to source or sponsorship.") This indicates good faith in the use of the trademarks and weighs in favor of defendant. Hence, even if the court were to apply the Ninth Circuit's eight-factor test, plaintiff has failed to demonstrate that it would likely succeed in proving that defendant's use of the trademarks causes a likelihood of confusion for the consumer. As the court has already noted, the Terri Welles web page appears to promote Terri Welles only and makes no attempt to connect itself with **Playboy** or PEI.

C. Dilution Claim

Given that the court has found that defendant is entitled to the "fair use" defense pursuant to 15 U.S.C. §1115(b)(4), plaintiff cannot make a sufficient dilution claim under 15 U.S.C. §1125(c) to warrant the granting of a preliminary injunction. 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 ... (2)
likelihood of confusion, mistake, or deception." 15 U.S.C. §1127. Title 15 U.S.C. §1125(c)(1) provides the following:

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 and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection.

Id. The section provides factors the court may consider in determining whether a mark is distinctive and famous. See 15 U.S.C. §1125(c)(1)(A-H). Though PEI's marks are arguably famous, their distinctiveness does not preclude defendant from the fair use of those items.

Under the Federal Trademark Dilution Act, a dilution claim is not actionable if there is a "[f]air 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." 15 U.S.C. §1125(c)(4)(A). As the court has indicated, Ms. Welles' use of the terms Playmate and Playmate of the Year constitute identification of herself. The use of those terms, in the website and in the meta tags, allows web surfers and potential customers to identify her services, whether it be her line of cigars, her promotional services, or her nude photographs. Given that Ms. Welles is the "Playmate of the Year 1981," there is no other way that Ms. Welles can identify or describe herself and her services without venturing into absurd descriptive phrases. In cases where the trademarked term must be used to identify the individual or a good, infringement and dilution laws do not apply. See New Kids, 971 F.2d at 306 ("In such cases, use of the trademark does not imply sponsorship or endorsement of the product because the mark is used only to describe the thing, rather than to identify its source."). Accordingly, plaintiff has failed to show that there is a likelihood of success on the merits of its dilution claim.

IV. CONCLUSION

In Prestonettes v. Coty, 264 U.S. 359, 368 (1924), Justice Holmes explained the purpose of trademark protection and noted that "[w]hen the mark is used in a way that does not deceive the public we see no such sanctity in the word as to prevent its being used to tell the truth. It is not taboo." In this case, Ms. Welles has used PEI's trademarks to identify herself truthfully as the Playmate of the Year 1981. Such use is not "taboo" under the law. Based on the foregoing analysis, the court finds that plaintiff has failed to demonstrate that a preliminary injunction is warranted since there is not a strong likelihood of success on the merits. Consequently, the court cannot find that the balance of harm tips strongly enough in plaintiff's favor to overcome the lack of merit of the court has found. See Stokely-Van Camp Inc. v. Coca-Cola Co., 2 U.S.P.Q.2d 1225, 1227 (N.D. Ill. 1987). In addition, it is unclear that irreparable harm would ensue from the continued operation of Ms. Welles' website since plaintiff has not demonstrated that there is a likelihood of confusion. As such, the court, hereby DENIES plaintiff's Motion for a Preliminary Injunction.

IT IS SO ORDERED.

Date 4/21/98

/s/ Judge Judith N. Keep
United States District Court
Southern District of California

FOOTNOTES

1 15 U.S.C. §1114(1)(a) reads as follows. "Any person who shall, without the consent of the registrant use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark 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 ... shall be liable in a civil action by the registrant for the remedies hereinafter provided."

2 15 U.S.C. §1125(a)(1)(A) reads as follows. "Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person ... shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act."

3 Defendant raised the issue of PEI's acquiescence in Ms. Welles' use of the terms Playmate; Playmate of the Month, and Playmate of the Year. Plaintiff does not contest that it allowed defendant to use these terms previously, but it argues that the defense of acquiescence does not apply in this case since defendant is now engaged in a competitive "trademark use" of those terms. "The defense of acquiescence is a type of estoppel which constitutes a ground for denial of relief upon a finding of conduct on plaintiff's part that amounts to an assurance by the plaintiff to the defendant, either express or implied that plaintiff will not assert his trademark rights against the defendant." CBS Inc. v. Man's Day Publishing Company, Inc., 205 U.S.P.Q. 470, 473-74 (1980). The court does not find it necessary to decide if this defense is applicable in this case.
ORDER GRANTING FABER'S MOTION FOR ...MENT AGAINST BALL
http://www.compupix.com/ballysucks/summaryjudgment.htm

UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA

BALLY TOTAL FITNESS HOLDING CORPORATION,
Plaintiff,
v.
ANDREW S. FABER,
Defendant.

Case No. CV 98-1278 DDP (MANx)

ORDER

ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

Andrew S. Faber's motion for summary judgment came before the Court for oral argument on November 23, 1998. After reviewing and considering the materials submitted by the parties and hearing oral argument, the Court GRANTS Faber's motion for summary judgment.

BACKGROUND
Bally Total Fitness Holding Corp. ("Bally") brings this action for trademark infringement, unfair competition, and dilution against Andrew S. Faber ("Faber") in connection with Bally's federally registered trademarks and service marks in the terms "Bally," "Bally's Total Fitness," and "Bally Total Fitness," including the name and distinctive styles of these marks. Bally is suing Faber based on his use of Bally's marks in a web site he designed.

Faber calls his site "Bally sucks." The web site is dedicated to complaints about Bally's health club business. When the web site is accessed, the viewer is presented with Bally's mark with the word "sucks" printed across it. Immediately under this, the web site states "Bally Total Fitness Complaints! Un-Authorized."

Faber has several web sites in addition to the "Bally sucks" site. The domain "Domains" are used to provide organization to the Internet. The domain name is a word or series of words followed by ".edu" for education; ".org" for organizations; ".gov" for government entities; ".net" for networks; and ".com" as the catchall for other Internet users. Within each of these top level domains, there are many different sub-domains. An example of a domain name would be "www.Bally.com." Domain names are licensed to individuals by Network Solutions, Inc. Within any domain, the domain owner may place additional sub-domains and multiple web pages or may merely have one web site. In which Faber has placed his web sites is "www.compupix.com." Faber's other web sites within "www.compupix.com" include the "Bally sucks" site (URL address "www.compupix.com/ballysucks"); "Images of Men," a web site displaying and selling photographs of nude males (URL address "www.compupix.com/index.html"); a web site containing information regarding the gay community (URL address "www.compupix.com/gay"); a web site containing photographs of flowers and landscapes (URL address "www.compupix.com/fl/index.html"); and a web site advertising "Drew Faber Web Site Services" (URL address "www.compupix.com/biz.htm").

On April 22, 1998, Bally applied for a temporary restraining order directing Faber to withdraw his web site from the Internet. Bally represents that when its application for a TRO was initially filed, the "Bally sucks" site contained a direct link to Faber's "Images of Men" site. In his opposition to the application for a TRO, Faber indicated that this link had been removed. The Court denied Bally's application on April 30, 1998.

Bally brought a motion for summary judgment on its claims of trademark infringement, trademark dilution, and unfair competition which the Court denied on October 20, 1998. In that order, the Court ordered Faber to bring a motion for summary judgment. This motion is now before the Court.
DISCUSSION

I. Faber’s Motion for Summary Judgment

A. Legal Standard

Summary judgment is appropriate where “there is no genuine issue as to any material fact and... the moving party is entitled to a judgment as a matter of law.” Fed. R. Civ. P. 56(c). A genuine issue exists if “the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). Thus, the mere existence of a scintilla of evidence in support of the nonmoving party’s claim is insufficient to defeat summary judgment. Id. at 252. In determining a motion for summary judgment, all reasonable inferences from the evidence must be drawn in favor of the non-moving party. Id. at 242.

B. Trademark Infringement

The Lanham Act provides the basic protections that a trademark owner receives. To find that Faber has infringed Bally’s marks the Court would have to find that Bally has valid protectable trademarks and that Faber’s use creates a likelihood of confusion. 15 U.S.C. § 1114(1)(a). Faber asserts that Bally cannot meet this standard as a matter of law.

1. Validity of Bally’s marks

Bally has demonstrated that it has invested a substantial amount of money and effort to create valuable trademarks. Bally’s marks are registered on the Principle Register of the U.S. Patent and Trademark Office. Additionally, Bally asserts that “[s]ince 1990, Bally has spent over $500,000,000.00 (one-half billion dollars) in advertising the Bally name in the health club industry.” Further, “[i]n 1996, Bally spent over $5,000,000 in external signage for its clubs nationwide.” Finally, Bally argues that it is the only business in the health club industry which uses the Bally marks. These facts establish that Bally has valid protectable marks.

2. Likelihood of confusion

In determining whether a defendant’s use of a plaintiff’s trademarks creates a likelihood of confusion, the courts apply an eight-factor test, including:

(1) strength of the mark;
(2) proximity of the goods;
(3) similarity of the marks;
(4) evidence of actual confusion;
(5) marketing channels used;
(6) type of goods and the degree of care likely to be exercised by the purchaser;
(7) defendant’s intent in selecting the mark; and
(8) likelihood of expansion of the product lines.

See AMF Inc. v. Sleekcraft Boots, 599 F.2d 341, 348-49 (9th Cir. 1979).

The Sleekcraft factors apply to related goods. Id. at 348. Bally is involved in the health club industry. Faber is an Internet web page designer who believes that Bally engages in unsatisfactory business practices. Faber operates a web site which critical of Bally’s operations. Bally, however, states that it uses the Internet to communicate with its members and to advertise its services. Consequently, Bally asserts that the parties have related goods because both parties use the Internet to communicate with current and potential Bally members.

"Related goods are those goods which, though not identical, are related in the minds of consumers." Levi Strauss & Co. v. Blue Bell, Inc., 778 F.2d 1352, 1363 (9th Cir. 1985). Several courts have addressed whether goods are related. See id. (shirts and pants are related goods); Fleischmann Distilling Corp. v. Maier Brewing Co., 314 F.2d 149, 152-53 (9th Cir. 1963) (beer and whiskey are related goods); Yale Elec. Corp. v. Robertson, 26 F.2d 972 (2d Cir. 1928) (locks and flashlights are related goods). The modern rule protects marks against "any product or service which would reasonably be thought by the buying public to come from the same source, or thought to be affiliated with, connected with, or sponsored by, the trademark owner." 3 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition § 24.6 at 24-13 (1997).

The Court finds that the goods here are not related. Web page design is a service based on computer literacy and design skills. This service is far removed from the business of managing health clubs. The fact that the parties both advertise their respective services on the Internet may be a factor tending to show confusion, but it does not make the goods related. The Internet is a communications medium. It is not itself a product or a service. Further, Faber’s site states that it is "unauthorized" and contains the words "Bally sucks." No reasonable consumer comparing Bally’s official web site with Faber’s site would assume Faber’s site "to come from the same source, or thought to be affiliated with, connected with, or sponsored by, the trademark owner." Therefore, Bally’s claim for trademark infringement falls as a matter of law.

However, even assuming that these goods are related, Bally’s claims also fail to satisfy the Sleekcraft factors.

a. Strength of mark

This factor tips greatly toward Bally. Bally owns registered marks. Bally uses these marks extensively throughout the United States and Canada. Bally spends a significant amount of money each year to promote its marks. Finally, Bally asserts that no other company uses these marks in connection with health clubs, and that these marks are arbitrary. These facts demonstrate that Bally has strong marks.

b. Similarity of the marks

0218
Bally argues that the marks are identical. Bally argues that the only difference between the marks is that Faber attached the word "sucks" to Bally's marks. Bally argues that this is a minor difference. "Sucks" has entered the vernacular as a word loaded with criticism. Faber has superimposed this word over Bally's mark. It is impossible to see Bally's mark without seeing the word "sucks." Therefore, the attachment cannot be considered a minor change. See Int'l Ass'n of Machinists & Aerospace Workers v. Winship Green Nursing Ctr., 103 F.3d 196, 202-03 (1st Cir. 1996). This factor cuts against Bally.

c. Competitive proximity of the goods
Bally argues that the goods are in close proximity because both parties use the Internet. Bally uses the Internet to generate revenue and disseminate information to its customers in support of its health clubs. Faber uses his web site to criticize Bally and to provide others with a forum for expressing their opinions of Bally. Faber does not attempt to pass-off his site as Bally's site. Faber states that his site is "unauthorized." Bally asserts that its site offers similar services because it has a complaints section and it provides information about Bally's services and products. The Court finds that Faber's site does not compete with Bally's site. It is true that both sites provide Internet users with the same service - information about Bally. These sites, however, have fundamentally different purposes. Bally's site is a commercial advertisement. Faber's site is a consumer commentary. Having such different purposes demonstrates that these sites are not proximately competitive. Therefore, this factor cuts against Bally.

d. Evidence of actual confusion
Bally does not offer evidence of actual confusion. Instead, Bally states, "consumer confusion is patently obvious in this case because of the strength of the Bally marks, combined with the obvious similarities in appearance and proximity of the marks, although there is no evidence of actual confusion." Faber's states that his site is "unauthorized" and he has superimposed the word "sucks" over Bally's mark. The Court finds that the reasonably prudent user would not mistake Faber's site for Bally's official site. Therefore, this factor cuts against Bally.

e. Marketing channels used
Bally argues that both parties use the Internet to reach current and potential Bally members. Bally states that it uses the Internet to disseminate information and generate revenue. Bally contends that it has spent over $500,000,000 in advertisements including the Internet, television, radio, billboards and signage since 1990. Therefore, Bally has a broad marketing strategy which includes the Internet. Bally has not shown that Faber uses all of these channels for marketing. Instead, Bally has shown that Faber has one site which offers his services for web design, and this site included a reference to his "Bally sucks" site for some time. However, this site no longer includes this link.
Arguably, listing the "Bally sucks" site as one of many sites Faber has created in order to advertise his web design services is a form of marketing. This factor, however, does not change the primary purpose of the "Bally sucks" site which is consumer commentary. Bally's goods and Faber's goods are not related. Therefore, the fact that marketing channels overlap is irrelevant.
This factor is, at best, neutral, and likely cuts against Bally.

f. Degree of care likely to be exercised
Bally argues that individual users may mistakenly access Faber's site rather than the official Bally site. Bally argues that this may happen when users employ an Internet search engine to locate Bally's site. Bally argues that the search result may list Faber's site and Bally's site. The result, it argues, will be that "[p]rospective users of plaintiff's services who mistakenly access defendant's web site may fail to continue to search for plaintiff's own home page, due to anger, frustration or the belief that plaintiff's own home page does not exist." (Bally's Mot. for Sum. Judg. 19:1-3, quoting Panavision Int'l, L.P. v. Toepken, 141 F.3d 1316, 1327 (9th Cir. 1998).) The Panavision case, however, concerned an individual who engaged in commercial use of plaintiff's registered mark in his Internet domain name, "Panavision.com." See Panavision, 141 F.3d at 1324.

Here, Faber uses the Bally mark in the context of consumer criticism. He does not use Bally in his domain name. He communicates that the site is unauthorized and that it is not Bally's official site. Moreover, Faber's use of the Bally mark does not significantly add to the large volume of information that the average user will have to sift through in performing an average Internet search. See Teletech Customer Care Mgmt., Inc. v. Tele-Tech Co., 977 F. Supp. 1407, 1410 (C.D. Cal. 1997) (noting that average search can result in 800 to 1000 "hits"). Whether the average user has to sift through 799 or 800 "hits" to find the official Bally site will not cause the frustration indicated in Teletech and Panavision because Faber is not using Bally's marks in the domain name. Moreover, even if Faber did use the mark as part of a larger domain name, such as "ballysucks.com", this would not necessarily be a violation as a matter of law. The Court notes that there is a distinction between this example and cases like Panavision where an individual appropriates another's registered trademark as its domain name. In the "cybersquatter" cases like Panavision, there is a high likelihood of consumer confusion - reasonably prudent consumers would believe that the site using the appropriated name is the trademark owner's official site. Here, however, no reasonably prudent Internet user would believe that "Ballysucks.com" is the official Bally site or is sponsored by Bally.

Further, the average Internet user may want to receive all the information available on Bally. The user may want to access the official Internet site to see how Bally sells itself. Likewise, the user may also want to be apprised of the opinions of others about Bally. This individual will be unable to locate sites containing outside commentary unless those sites include Bally's marks in the machine readable code. The machine readable code is the hidden part of the Internet upon which search engines rely to find sites that contain content which the individual user wishes to locate. The basic mechanics is that the web page designer places certain keywords in an unreadable portion of the web page
that tells the search engines what is on a particular page, upon which search engines rely. Prohibiting Faber from using Bally's name in the machine readable code would effectively isolate him from all but the most savvy of Internet users.

Therefore, this factor cuts against Bally.

f. Defendant's intent in selecting the mark

Here, Faber purposely chose to use Bally's mark to build a "web site that is 'dedicated to complaint, issues, problems, beefs, grievances, grumblings, accusations, and gripes with Bally Total Fitness health clubs.'" Faber, however, is exercising his right to publish critical commentary about Bally. He cannot do this without making reference to Bally. Faber concedes that Faber has some right to use Bally's name as part of his consumer commentary. However, Bally argues that Faber uses more than is necessary when making his commentary and that he has alternative means of communication. Specifically, Bally argues that Faber could use the name "Bally" or "Bally Total Fitness" in block lettering without using Bally's stylized "B" mark or distinctive script. This argument, however, would create an artificial distinction that does not exist under trademark law. Trademarks are defined broadly to include both names and stylized renditions of those names or other symbols. 15 U.S.C. §§ 1051, 1127 (1997). Furthermore, the purpose of a trademark is to identify the source of goods. Id. § 1127. An individual who wishes to engage in consumer commentary must have the full range of marks that the trademark owner has to identity the trademark owner as the object of the criticism. (See infra Part I-C.) In this regard, Professor McCarthy states:

The main remedy of the trademark owner is not an injunction to suppress the message, but a rebuttal to the message. As Justice Brandeis long ago stated, "If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the process of education, the remedy to be applied is more speech, not enforced silence."

5 McCarthy, § 31:148 at 31-216.

Applying Bally's argument would extend trademark protection to eclipse First Amendment rights. The courts, however, have rejected this approach by holding that trademark rights may be limited by First Amendment concerns. See L. L. Bean, Inc. v. Drake Publishers, Inc., 811 F.2d 26 (1st Cir.), cert. denied, 483 U.S. 1013 (1987).

Therefore, this factor is neutral.

h. Likelihood of expansion of the product line

Bally essentially concedes that there is no likelihood that Bally will expand its product lines into the same areas in which Faber operates. However, Bally claims that Faber's intentional acts reduce the significance of this factor. Bally, though, relies on conclusions rejected by the Court. (See supra Part I-B-2-g.) It is apparent that the parties will not expand into the other's line of business. Bally intends to use the Internet as a means of increased communication. However, Bally has not represented that it intends to enter the web design business or that it intends to operate an official anti-Bally site. Further, Faber has not indicated that he intends to operate a health club.

Therefore, this factor also cuts against Bally.

3. Conclusion

Bally owns valuable marks. However, Faber has established that there is no likelihood of confusion as a matter of law. Therefore, the Court grants Faber's motion for summary judgment on trademark infringement.

C. Trademark Dilution

The elements of a dilution claim are that:

(1) The plaintiff is the owner of a mark which qualifies as a "famous" mark as measured by the totality of the eight factors listed in § 43(c)(1),
(2) The defendant is making commercial use,
(3) In interstate commerce,
(4) Of a mark or trade name,
(5) And defendant's use began after the plaintiff's mark became famous,
(6) And defendant's use causes dilution by lessening the capacity of the plaintiff's mark to identify and distinguish goods or services.

3 McCarthy, § 24:89 at 24-137-38 (footnote omitted). Dilution may be either by blurring or by tarnishment. See id. §§ 24:69, 24:68, at 24-116-17. Here, Bally argues that Faber has tarnished its mark by associating it with pornography.

Commercial use is an essential element of any dilution claim. Here, Bally argues that Faber has used Bally's mark to demonstrate his skills as a web site designer and to show current members how to effectively cancel their memberships with Bally. Bally asserts that Faber listed the "Bally sucks" web site on the "Drew Faber Web Site Services" site in an effort to advertise Faber's services.

Bally cites several "cybersquatting" cases in which individuals registered the trademarks of others as domain names for the purpose of selling or ransoming the domain name to the trademark owner. Bally asserts that these cases hold that using another's mark on the Internet is per se commercial use. The mere use of another's name on the Internet, however, is not per se commercial use. See 3 McCarthy, § 24-97.2 at 24-172.
Here, Faber used Bally's marks in connection with a site devoted to consumer product review of Bally's services. In congressional hearings, Senator Orrin Hatch stated that the dilution statute "will not prohibit or threaten noncommercial expression, such as parody, satire, editorial and other forms of expression that are not a part of a commercial transaction." 141 Cong. Rec. S 19306-10 (Daily ed. Dec. 29, 1995). Therefore, this exception encompasses both parodies and consumer product reviews. See Panavision Intl 'L P v. Toeppen, 945 F. Supp. 1296, 1303 (C.D. Cal. 1996).

Faber has shown that Bally cannot demonstrate that he is using Bally's mark in commerce. Bally argues that Faber's listing of the "Bally sucks" site, among others, in a site listing his available services and qualifications using the Bally mark to promote a service. This argument is unpersuasive. Faber is not using the Bally mark to sell his services. Faber is not using Bally's mark to identify his goods in commerce. Faber merely listed the "Bally sucks" site as one of several web sites that he has designed so that those who are interested in his services may view his work. This is akin to an on-line resume.

Further, the courts have held that trademark owners may not quash unauthorized use of the mark by a person expressing a point of view. See L.L. Bean, 811 F.2d at 29, citing Lucasfilm Ltd. v. High Frontier, 622 F. Supp. 931, 933-35 (D.D.C. 1985). This is so even if the opinion may come in the form of a commercial setting. See id., at 33 (discussing Maine's anti-dilution statute). In L.L. Bean, the First Circuit held that a sexually-oriented parody of L.L. Bean's catalog in a commercial adult-oriented magazine was non-commercial use of the trademark. See id. The court stated:

"If the anti-dilution statute were construed as permitting a trademark owner to enjoin the use of his mark in a noncommercial context found to be negative or offensive, then a corporation could shield itself from criticism by forbidding the use of its name in commentaries critical of its conduct. The legitimate aim of the anti-dilution statute is to prohibit the unauthorized use of another's trademark in order to market incompatible products or services. The Constitution does not, however, permit the range of the anti-dilution statute to encompass the unauthorized use of a trademark in a noncommercial setting such as an editorial or artistic context.

Id.

Here, Bally wants to protect its valuable marks and ensure that they are not tarnished or otherwise diluted. This is an understandable goal. However, for the reasons set forth above, Faber's "Bally sucks" site is not a commercial use.

Even if Faber's use of Bally's mark is a commercial use, Bally also cannot show tarnishment. Bally cites several cases such as the "Enjoy Cocaine" and "Mutant of Omaha" cases for the proposition that this site and its relationship to other sites tarnishes their mark. See Mutual of Omaha Ins. Co. v. Novak, 648 F. Supp. 905 (D. Neb. 1986) (discussing both infringement and disparagement); aff'd 836 F.2d 397 (8th Cir. 1987) (addressing infringement, but not disparagement); Coca-Cola v. Gemini Rising, Inc., 346 F. Supp. 1183 (E.D.N.Y. 1972).

There are, however, two flaws with Bally's argument. First, none of the cases that Bally cites involve consumer commentary. In Coca-Cola, the court enjoined the defendant's publication of a poster stating "Enjoy Cocaine" in the same script as Coca-Cola's trademark. See Coca-Cola, 346 F. Supp. at 1192. Likewise, in Mutual of Omaha, the court prohibited the use of the words "Mutant of Omaha" with a picture of an emaciated human head resembling the Mutual of Omaha's logo on a variety of products as a means of protesting the arms race. See Mutual of Omaha, 836 F.2d at 398. Here, however, Faber is using Bally's mark in the context of a consumer commentary to say that Bally engages in business practices which Faber finds distasteful or unsatisfactory. This is speech protected by the First Amendment. See L.L. Bean, 811 F.2d at 29; McCarthy, § 24:105 at 24-191. As such, Faber can use Bally's mark to identify the source of the goods or services of which he is complaining. This use is necessary to maintain broad opportunities for expression. See Restatement (Third) of Unfair Competition § 25(2), cmt. i (1995) (stating "extension of the antidualation statutes to protect against damaging nontrademark uses raises substantial free speech issues and duplicates other potential remedies better suited to balance the relevant interests").

The second problem with Bally's argument is that it is too broad in scope. Bally argues that the proximity of Faber's "Images of Men" site tarnishes the good will that Bally's mark enjoys because it improperly creates an association between Bally's mark and pornography. If the Court accepted this argument it would be an impossible task to determine dilution on the Internet. It is true that both sites are under the same domain name; "Compupix.com." Furthermore, it is also true that at a variety of times there were links between Faber's various sites. However, at no time was any pornographic material contained on Faber's "Bally sucks" site. From its inception, this site was devoted to consumer commentary. Looking beyond the "Bally sucks" site to other sites within the domain or to other linked sites would, to an extent, include the Internet in its entirety. The essence of the Internet is that sites are connected to facilitate access to information. Including linked sites as grounds for finding commercial use or dilution would extend the statute far beyond its intended purpose of protecting trademark owners from uses that have the effect of "lessening . . . the capacity of a famous mark to identify and distinguish goods or services." 15 U.S.C. § 1127. Further, it is not logical that a reasonably prudent Internet user would believe that sites which contains no reference to a trademark and which are linked to, or within the same domain as, a site that is clearly not sponsored by the trademark owner are in some way sponsored by the trademark owner.

Therefore, the Court grants Faber's motion for summary judgment on the claim of trademark dilution.
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

LOCKHEED MARTIN CORPORATION,
Plaintiff-Counter-Defendant-Appellant,

v.

NETWORK SOLUTIONS, INC.,
Defendant-Counter-Claimant-Appellee.

Appeal from the United States District Court
for the Central District of California
Dean D. Pregerson, District Judge, Presiding

Argued and Submitted
June 8, 1999--Pasadena, California

Filed October 25, 1999

Before: Dorothy W. Nelson, Stephen Reinhardt, and
Stephen S. Trott, Circuit Judges.

Opinion by Judge Trott

COUNSEL

David W. Quinto, Quinn Emanuel Urquhart Oliver & Hedges,
Los Angeles, California, for the plaintiff-counter-defendant-appellant.

Ronald L. Johnston, Blanc Williams Johnston & Kronstadt,
Los Angeles, California, for the defendant-counter-claimant-appellee.
OPINION

TROTT, Circuit Judge:

Plaintiff Lockheed Martin Corp. ("Lockheed") appeals summary judgment in favor of Defendant Network Solutions, Inc. ("NSI") on Lockheed's action for trademark infringement, unfair competition, dilution, and contributory infringement under the Lanham Trademark Act of 1946, 15 U.S.C. SS 1051-1127 (1994 & Supp. 1 1995), as amended (the "Lanham Act"). The district court published its decision granting summary judgment to NSI and refusing to grant Lockheed's motion for leave to amend its complaint. 985 F. Supp. 949 (C.D. Cal. 1997). Lockheed contends that (1) genuine issues of material fact remain on its contributory infringement claim, (2) the district court erred in holding that 15 U.S.C. S 1114(2) did not create an independent basis for liability, and (3) the district court should have permitted Lockheed to amend the complaint to add a cause of action for contributory dilution. We have jurisdiction under 28 U.S.C. S 1291 (1994), and we affirm the judgment of the district court.

I

This appeal concerns the NSI registration scheme for domain-name combinations, which we discussed in our recent Avery Dennison Corp. v. Sumpton, No. 98-55810 (9th Cir. August 23, 1999), decision. An interested reader may wish to review the district court's in-depth discussion of the Internet technology that forms the basis of this cause of action. 985 F. Supp. at 951-53.

When a third party seeks to maintain an Internet web site, that party must reserve a location, called an Internet Protocol ("IP") Address, and do the necessary programming. When an Internet user accesses the third party's web site, the user enters the domain-name combination that corresponds to the

IP Address and is routed to the host computer. An industry of surrogate hosts has developed, where an Internet Service Provider licenses space on its computers to a third-party web-site operator, permitting the operator to maintain a web site without keeping his or her computer continually connected to the Internet. The Internet Service Providers do not provide the translation service from an entered domain-name combination to the appropriate IP Address. A separate organization has the responsibility to perform the translation function.

A

At all relevant times, NSI was the sole National Science Foundation contractor in charge of registering domain-name combinations for the top-level domains <.gov>, <.edu>, <.com>, <.org>, and <.net>. (For clarity, we set off Internet-related character strings with the caret symbols ("^>").) After registration, NSI entered the combination and the corresponding IP Address in its database, permitting automatic translation when an Internet user entered a domain-name combination. NSI is no longer the exclusive registrar. Since
oral argument on this appeal, a new competitive scheme has been implemented. See Jeri Clausing, 3-Week Delay in Opening Up Internet Name Registration, N.Y. Times, June 28, 1999, at C1.

When registering with NSI to receive a domain-name combination, an applicant submits NSI's "template" electronically over the Internet. On approval, NSI puts the domain-name combination in its database in conjunction with the correct IP Address. NSI then routes Internet users who enter a certain domain-name combination to the registrant's computer. At the time of argument on this appeal, NSI was receiving approximately 130,000 registrations per month, although evidence indicates that the number of monthly registrations has been increasing steadily and is possibly much larger today. Ninety percent of templates are processed electronically, and the entire registration process for each application requires

between a few minutes and a few hours. Ten percent of the time, an employee of NSI reviews the application. Human intervention might occur because of an error in filling out the form or because the applied-for domain name includes a "prohibited" character string -- such as specific variations on the words Olympic, Red Cross, or NASA, and certain "obscene" words. NSI also performs a conflict check on all applications, which compares an application to other registered domain-name combinations. However, NSI does not consult third parties during the registration process, check for a registrant's right to use a particular word in a domain-name combination, or monitor the use of a combination once registered. NSI is also not an Internet Service Provider. It performs none of the "hosting" functions for a web site.

NSI does maintain a post-registration dispute-resolution procedure. Anyone who feels that his or her rights are violated by the domain-name combination maintained by a registrant can submit a certified copy of a trademark registration to NSI. NSI then requires the registrant to obtain a declaratory judgment of the right to maintain the domain-name combination. If the registrant fails to do so, its registration is terminated.

B

Lockheed owns and operates "The Skunk Works," an aircraft design and construction laboratory. Since 1943, The Skunk Works has developed prototypes of this country's first jet fighter, the U-2 and SR-71 spy planes, and the F-117 and F-22 fighter planes. The Skunk Works is currently involved in designing a possible replacement for the space shuttle. "Skunk Works" is a registered and incontestable service mark.

II

Third parties, not involved in this litigation, have registered domain-name combinations with NSI which are variations on

the phrase "skunk works." These include:
Lockheed sent two letters, on May 7 and June 18, 1996, bringing the <skunkworks.com> and <skunkworks.net> registrations to NSI's attention. Lockheed's letters informed NSI of its belief that the third-party registrants were infringing or diluting Lockheed's service mark. Lockheed requested that NSI cancel the allegedly offending registrations. Lockheed also requested that NSI cease registering domain-name combinations that included "Skunk Works" or variations on the phrase and report to Lockheed all such domain-name combinations contained in its registry. NSI took no action on Lockheed's requests, informing Lockheed by letter that Lockheed had failed to comply with the terms of NSI's dispute resolution policy. Due to Lockheed's dealings with the third-party registrants, <skunkworks.com> and <skunkworks.net> ceased being used, but NSI did not immediately cancel the registrations and later permitted a new registrant to register <skunkworks.com>.

Lockheed sued NSI on October 22, 1996, claiming contributory service mark infringement, infringement, unfair competition, and service mark dilution, all in violation of the Lanham Act, and also seeking declaratory relief. The complaint alleged that four specific domain-name registrations infringed or diluted Lockheed's "Skunk Works" service mark. The parties stipulated to April 1, 1997, as the cut-off date for motions to amend the pleadings. Lockheed later proposed, over NSI's objection, that the cutoff date be moved to July 7, 1997. NSI moved for summary judgment. On August 19, 1997, Lockheed moved to amend its complaint to add a cause of action for contributory dilution and to allege several additional domain-name combinations registered with NSI. The district court denied the motion to amend and granted summary judgment to NSI.

III

We review the district court's grant of summary judgment de novo. Margolis v. Ryan, 140 F.3d 850, 852 (9th Cir. 1998). Viewing the evidence in the light most favorable to the non-moving party, summary judgment is appropriate if no genuine issues of material fact remain and the non-moving party is entitled to judgment as a matter of law. See id. We review for an abuse of discretion the district court's decision denying a motion to amend a complaint. Griggs v. Pace Am. Group, Inc., 170 F.3d 877, 879 (9th Cir. 1999).

IV

[1] Contributory infringement occurs when the defendant either intentionally induces a third party to infringe the plaintiff’s mark or supplies a product to a third party with actual or constructive knowledge that the product is being used to
infringe the service mark. Inwood Lab., Inc. v. Ives Lab., Inc., 456 U.S. 844, 853-54 (1982). Lockheed alleges only the latter basis for contributory infringement liability and therefore must prove that NSI supplies a product to third parties with actual or constructive knowledge that its product is being used to infringe "Skunk Works." Id. at 854.

[2] The district court assumed for purposes of summary judgment that third parties were infringing Lockheed's "Skunk Works" service mark, and NSI does not ask us to affirm on the alternate ground that no genuine issue of material fact exists as to infringement. We are thus left to consider two issues on Lockheed's contributory infringement cause of action: (1) whether NSI supplied a product to third parties and

12958

(2) whether NSI had actual or constructive knowledge of any infringement. Because we accept the district court's excellent analysis on the first question, see 985 F. Supp. at 960-62, we affirm summary judgment without reaching the second.

A

Under the plain language of the Inwood Lab. formulation, to be liable for contributory infringement, NSI must supply a "product" to a third party with which the third party infringes Lockheed's service mark. 456 U.S. at 854. In Inwood Lab., the Supreme Court considered an action against a manufacturer of generic pharmaceuticals. Id. at 847. Non-party pharmacists packaged the defendant's less-expensive generic pills, but labeled them with the plaintiff's brand name. Id. at 850. The plaintiff stated a cause of action for contributory infringement by alleging that the defendant "continued to supply [the product] to pharmacists whom the petitioners knew were mislabeling generic drugs." Id. at 855.

Inwood Lab. has been applied in the broader context of renting booth space at a flea market. See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148-49 (7th Cir. 1992). In Hard Rock, the Seventh Circuit explicitly addressed the distinction between a product and a service, noting that while the pharmaceutical company in Inwood Lab. clearly supplied a product to the third-party pharmacists, a "temporary help service ... might not be liable if it furnished [to the defendant] the workers he employed to erect his stand." Hard Rock, 955 F.2d at 1148. The court then held that space at a flea market was more comparable to pharmaceuticals than to manpower, in part because of the close comparison between the legal duty owed by a landlord to control illegal activities on his or her premises and by a manufacturer to control illegal use of his or her product. Id. at 1149. We adopted the Hard Rock analysis in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), holding that a flea market could be liable for contributory infringe-

12959

ment if it "suppl[ied] the necessary marketplace" for the sale of infringing products. Id. at 265 (citing Hard Rock, 955 F.2d at 1149).

[3] Hard Rock and Fonovisa teach us that when measuring
and weighing a fact pattern in the contributory infringement context without the convenient "product" mold dealt with in Inwood Lab., we consider the extent of control exercised by the defendant over the third party's means of infringement. Hard Rock, 955 F.2d at 1148-49 (noting the common-law responsibilities of a landlord regarding illegal activity on a rented premises); see Fonovisa, 76 F.3d at 265 (adopting Hard Rock's analysis). Direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark permits the expansion of Inwood Lab.'s "supplies a product" requirement for contributory infringement.

B

[4] The case at bench involves a fact pattern squarely on the "service" side of the product/service distinction suggested by Inwood Lab and its offspring. All evidence in the record indicates that NSI's role differs little from that of the United States Postal Service: when an Internet user enters a domain-name combination, NSI translates the domain-name combination to the registrant's IP Address and routes the information or command to the corresponding computer. Although NSI's routing service is only available to a registrant who has paid NSI's fee, NSI does not supply the domain-name combination any more than the Postal Service supplies a street address by performing the routine service of routing mail. As the district court correctly observed,

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 on a web site or other Internet form of communication in connection with goods or services

12960

... NSI's involvement with the use of domain names does not extend beyond registration.

985 F. Supp. at 958.

[5] The "direct control and monitoring" rule established by Hard Rock and Fonovisa likewise fails to reach the instant situation. The district court correctly recognized that NSI's rote translation service does not entail the kind of direct control and monitoring required to justify an extension of the "supplies a product" requirement. See 985 F. Supp. at 962 ("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."). Such a stretch would reach well beyond the contemplation of Inwood Lab. and its progeny.

In an attempt to fit under Fonovisa's umbrella, Lockheed characterizes NSI's service as a licensing arrangement with alleged third-party infringers. Although we accept Lockheed's argument that NSI licenses its routing service to domain-name registrants, the routing service is just that -- a service. In Fonovisa and Hard Rock, by contrast, the defendants licensed real estate, with the consequent direct control over the activity that the third-party alleged infringers engaged in on the premises. Hard Rock, 955 F.2d at 1149; see Fonovisa, 96 F.3d at 265.
V

[6] Lockheed also urges that NSI is liable as a printer or publisher under 15 U.S.C. § 1114(2) (1994), which reads in pertinent part:

"The remedies given to the owner of a right infringed under this chapter or to a person bringing an action under section 1125(a) of this title shall be limited as follows:

(A) Where an infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer or innocent violator, the [plaintiff] shall be entitled as against such infringer or violator only to an injunction against future printing.

(B) Where the infringement or violation complained of is contained in ... an electronic communication ... the remedies ... shall be limited to an injunction against the presentation ... in future transmissions of such electronic communications."

Id. Section 1114(2) does not create an independent cause of action, but limits the remedies available to a plaintiff from an innocent infringer, requiring infringement of a trademark right or success on an unfair competition claim for injunctive relief. Barrios v. American Thermal Instruments, Inc., 712 F. Supp. 611, 620 (S.D. Ohio 1988) ("It is important to note that § 1114(2)(a) ... does not relate to the potential liability of a printer. Instead, this statute limits the relief which a Court may grant against a printer to an injunction against future printing."); see 3 J. Thomas McCarthy, Trademarks & Unfair Competition, S 25:29 (Supp. 1998) ("The Lanham Act, as amended effective in 1989, limits the liability of innocent infringement ... "). Because Lockheed does not appeal summary judgment for NSI on Lockheed's claims of service mark infringement and unfair competition, Lockheed cannot establish the necessary predicate for its § 1114(2) argument on appeal.

VI

[7] Finally, Lockheed argues that the district court abused its discretion in failing to grant leave to amend its complaint to (1) add a contributory dilution cause of action and (2) include allegations of several other offending domain-name combinations. As a general rule, leave to amend should be "freely given when justice so requires." Fed. R. Civ. P. 15(a); Foman v. Davis, 371 U.S. 178, 182 (1962). We consider four factors when reviewing a decision whether to permit an amendment: (1) bad faith on the part of the plaintiff; (2) undue delay; (3) prejudice to the opposing party; and (4) futility of the proposed amendment. Griggs, 170 F.3d at 877.

[8] Although delay is not a dispositive factor in the amend...
ment analyzers, it is relevant, Morongo Band of Mission Indians v. Rose, 893 F.2d 1074, 1079 (9th Cir. 1990), especially when no reason is given for the delay, Swanson v. United States Forest Serv., 87 F.3d 339, 345 (9th Cir. 1996). Lockheed's motion to amend came several months after the stipulated deadline for amending or supplementing the complaint. Nothing in the proposed amended complaint relied on facts that were unavailable before the stipulated deadline. The amendment was one that Lockheed had been considering three months before the stipulated deadline. Finally, Lockheed did not explain the delay, but supported it based on a claim of no prejudice to NSI.

[9] A need to reopen discovery and therefore delay the proceedings supports a district court's finding of prejudice from a delayed motion to amend the complaint. Solomon v. North Am. Life & Cas. Ins. Co., 151 F.3d 1132, 1139 (9th Cir. 1998). Lockheed sought to add complaints regarding new domain-name registrants which would require NSI to conduct discovery on each new registrant. Lockheed's new cause of action would also require NSI to conduct discovery of whether the domain-name registrants were diluting Lockheed's service mark. The district court's factual finding that allowing the late amendment would prejudice NSI is not clearly erroneous.

[10] Bad faith on the part of the moving party also supports denying the motion to amend. Griggs, 170 F.3d at 881. Facing a summary judgment motion, Lockheed sought to amend its complaint to add causes of action on which discovery had not been undertaken. The district court noted that this might reflect bad-faith on the part of Lockheed.

[11] Although we conclude from the above discussion that the district court was well within its discretion to deny Lockheed leave to amend its complaint, the fourth factor -- futility of the proposed amendment -- also supports the decision. Where the legal basis for a cause of action is tenuous, futility supports the refusal to grant leave to amend. Morongo Band, 893 F.2d at 1079. Although courts have discussed contributory dilution, no appellate court or statute has yet established the cause of action. Academy of Motion Picture Arts & Sciences v. Network Solutions, Inc., 989 F. Supp. 1276, 1279 (C.D. Cal. 1997).

The one court to recognize the contributory dilution cause of action defined the claim as encouraging others to dilute. Keegan v. Apple Computer Inc., 42 U.S.P.Q.2d 1053, 1062 (N.D. Ill. 1996). The proposed cause of action thus appears to import the definition of "contributory" from Inwood Lab., 456 U.S. at 854. Indeed, Lockheed's proposed amended complaint alleged that NSI continued to supply its routing service to registrants, knowing that these parties were diluting Lockheed's "Skunk Works" service mark. As we have already concluded, however, NSI does not supply a product or engage in the kind of direct control and monitoring required to extend the Inwood Lab. rule. We agree with the district court that futility supports its decision to refuse leave to amend the complaint.

VII
NSI requested attorneys' fees pursuant to the Lanham Act, 15 U.S.C. § 1117(a). We deny its request because Lockheed's appeal was not sufficiently unreasonable or frivolous to constitute an "exceptional case[ ]" as required by the Lanham Act for attorneys' fees to be warranted.

12964

VIII

NSI is not liable for contributory infringement as a matter of law. Lockheed does not appeal the district court's decision on its infringement, unfair competition, and dilution claims against NSI, and the district court did not abuse its discretion in refusing leave to amend the complaint. We have also considered Lockheed's request for judicial notice and motion to strike and deny both.

AFFIRMED.

12965

Go to top
§ 512. Limitations on liability relating to material online

(a) Transitory digital network communications. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System caching.

(1) Limitation on liability. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),
if the conditions set forth in paragraph (2) are met.

(2) Conditions. The conditions referred to in paragraph (1) are that—

(A) the material described in paragraph (1) is transmitted to the

$\text{subsequent users described in paragraph (1)(C) without modification to its}

content from the manner in which the material was transmitted from the person

described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules

concerning the refreshing, reloading, or other updating of the material when

specified by the person making the material available online in accordance with

a generally accepted industry standard data communications protocol for the

system or network through which that person makes the material available, except

that this subparagraph applies only if those rules are not used by the person

described in paragraph (1)(A) to prevent or unreasonably impair the intermediate

storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology

associated with the material to return to the person described in paragraph

(1)(A) the information that would have been available to that person if the

material had been obtained by the subsequent users described in paragraph (1)(C)

directly from that person, except that this subparagraph applies only if that

technology—

(i) does not significantly interfere with the performance of the

provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard

communications protocols; and

(iii) does not extract information from the provider's system or

network other than the information that would have been available to the person

described in paragraph (1)(A) if the subsequent users had gained access to the

material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition

that a person must meet prior to having access to the material, such as a

condition based on payment of a fee or provision of a password or other

information, the service provider permits access to the stored material in

significant part only to users of its system or network that have met those

conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material

available online without the authorization of the copyright owner of the

material, the service provider responds expeditiously to remove, or disable

access to, the material that is claimed to be infringing upon notification of

claimed infringement as described in subsection (c)(3), except that this

subparagraph applies only if—

(i) the material has previously been removed from the originating site

or access to it has been disabled, or a court has ordered that the material be

removed from the originating site or that access to the material on the

originating site be disabled; and

(ii) the party giving the notification includes in the notification a

statement confirming that the material has been removed from the originating

site or access to it has been disabled or that a court has ordered that the

material be removed from the originating site or that access to the material on

the originating site be disabled.

(c) Information residing on systems or networks at direction of users.

(1) In general. A service provider shall not be liable for monetary relief,

or, except as provided in subsection (j), for injunctive or other equitable

relief, for infringement of copyright by reason of the storage at the direction
of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—
(A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
§ (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.
(2) Designated agent. The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:
(A) the name, address, phone number, and electronic mail address of the agent.
(B) other contact information which the Register of Copyrights may deem appropriate.
The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.
(3) Elements of notification.
(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:
(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(B) (i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be
considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information location tools. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—

(1) (A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on liability of nonprofit educational institutions.

(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if—

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and
(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

§

(f) Misrepresentations. Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of removed or disabled material and limitation on other liability.

(1) No liability for taking down generally. Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception. Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider—

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification. To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before
it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability. A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena to identify infringer.

(1) Request. A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request. The request may be made by filing with the clerk--

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena. The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena. If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena. Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena. Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for eligibility.
(1) Accommodation of technology. The limitations on liability established by this section shall apply to a service provider only if the service provider—
   (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
   (B) accommodates and does not interfere with standard technical measures.

(2) Definition. As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and—
   (A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;
   (B) are available to any person on reasonable and nondiscriminatory terms; and
   (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions. The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:
   (1) Scope of relief.
      (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:
         (i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.
         (ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
         (iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.
      (B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:
         (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
         (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.
   (2) Considerations. The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider--
(A) whether such an injunction, either alone or in combination with other
such injunctions issued against the same service provider under this subsection,
would significantly burden either the provider or the operation of the
provider's system or network;
(B) the magnitude of the harm likely to be suffered by the copyright owner
in the digital network environment if steps are not taken to prevent or restrain
the infringement;
(C) whether implementation of such an injunction would be technically
feasible and effective, and would not interfere with access to noninfringing
material at other online locations; and
(D) whether other less burdensome and comparably effective means of
preventing or restraining access to the infringing material are available.
(3) Notice and ex parte orders. Injunctive relief under this subsection shall
be available only after notice to the service provider and an opportunity for
the service provider to appear are provided, except for orders ensuring the
preservation of evidence or other orders having no material adverse effect on
the operation of the service provider's communications network.

(k) Definitions.
(1) Service provider.
(A) As used in subsection (a), the term "service provider" means an entity
offering the transmission, routing, or providing of connections for digital
online communications, between or among points specified by a user, of material
of the user's choosing, without modification to the content of the material as
sent or received.
(B) As used in this section, other than subsection (a), the term "service
provider" means a provider of online services or network access, or the operator
of facilities therefor, and includes an entity described in subparagraph (A).
(2) Monetary relief. As used in this section, the term "monetary relief"
means damages, costs, attorneys' fees, and any other form of monetary payment.

(1) Other defenses not affected. The failure of a service provider's conduct to
qualify for limitation of liability under this section shall not bear adversely
upon the consideration of a defense by the service provider that the service
provider's conduct is not infringing under this title or any other defense.

(m) Protection of privacy. Nothing in this section shall be construed to
condition the applicability of subsections (a) through (d) on--
(1) a service provider monitoring its service or affirmatively seeking facts
indicating infringing activity, except to the extent consistent with a standard
technical measure complying with the provisions of subsection (i); or
(2) a service provider gaining access to, removing, or disabling access to
material in cases in which such conduct is prohibited by law.

(n) Construction. Subsections (a), (b), (c), and (d) describe separate and
distinct functions for purposes of applying this section. Whether a service
provider qualifies for the limitation on liability in any one of those
subsections shall be based solely on the criteria in that subsection, and shall
not affect a determination of whether that service provider qualifies for the
limitations on liability under any other such subsection.

2877; Aug. 5, 1999, P.L. 106-44, § 1(d), 113 Stat. 222.)
ARTICLE

The Intellectual Property Renaissance in Cyberspace:
Why Copyright Law Could Be Unimportant on the Internet

ERIC SCHLACHTER †

TABLE OF CONTENTS

I. INTRODUCTION

II. UNITED STATES COPYRIGHT LAW BASICS

III. THREATS TO ENFORCING COPYRIGHT RIGHTS ON THE INTERNET

A. No Loss of Quality In Reproduction
B. No Meaningful Marginal Costs of Reproduction or Distribution
C. Ability to Act Anonymously
D. Uneducated Users
E. Conclusion

IV. ECONOMICS AND THE INTERNET

A. Price-Setting Behavior in a Nearly Efficient Marketplace When Marginal Costs Are Meaningfully Zero
B. Cross-subsidization of Intellectual Property Creation
C. Importance of Attribution
D. Conclusion

V. SOCIOLOGY OF THE INTERNET

A. Attitudes Towards Intellectual Property
B. Internet Culture and Micro-Infringements
C. Conditioning to Expect Freebies

VI. TECHNOLOGIES AND METHODS FOR CONTROLLING INTELLECTUAL PROPERTY

A. Pre-Infringement
B. Metering
C. Post-Infringement
D. Additional Problems Under Copyright Law Possibly Solvable by Technology
E. Is Technology a Substitute for Copyright Law?

VII. CONCLUSION
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 production 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 in 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 VI 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 replaced with the Copyright Act of 1976 (the "Copyright Act").(8)

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.(2) 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.\(^{(10)}\)

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.\(^{(11)}\) [Note: these time limits have generally been extended 20 years]

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,\(^{(12)}\) 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 machines, 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, no quality-related limits inhibit pirates from making as many copies as they please, and recipients 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 costs are 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 harm 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 and 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.\(^\text{[15]}\)

D. Uneducated Users

Many users do not understand the existing copyright legal framework.\(^\text{[16]}\) While the lack of user 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 significant 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.\(^\text{[17]}\) 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 it 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. 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.

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. If marginal costs are 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 once the intellectual property is produced. 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, then some producers will accept zero marginal revenues. In other words, the profit-maximizing price for theses 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 no profits are being made, all producers will exit this business. This is fundamentally the assertion of those who believe that intellectual property owners must be paid directly for their creative efforts, or else they will not produce.

(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.

(iii) Traditional economic theory may break down on the Internet so that intellectual property will not be offered for free despite the absence of marginal variable costs. If this were true, the profit-maximizing price may not lie 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 lie 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 of 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. However, the deployment of this strategy is inherently limited because a razor is a tangible "thing" that will always have marginal costs to produce. On 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.

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, interactive news agents, editorial periodicals and search engines and indexes.

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. Because the supply of advertisement placement opportunities exceeds the demand of advertisers, advertisers are becoming more demanding. 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.

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 forms of ancillary revenues. Nevertheless, advertising remains a critically important component of Internet cross-subsidization business models.

2. Sponsorships

A variant on the advertising model, sponsorship is the "co-branding" of intellectual property with the sponsor's trademarks. In the old days of television, sponsorship was common; companies 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 will be more integrated with the content than just sticking its banner ad at the top of the page. For example, Riddler promotes a contest which gives rewards 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 consumers 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 costs are associated with manufacturing or distributing trial copies. Thus, software and subscription services 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 on-line. 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 without 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" (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. Although the commercial use of this personal information can create some significant privacy issues, 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. 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 communication 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, subscribers 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 as 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 the 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 key business models on the Internet.

The NII White Paper recognized that attribution could be important and therefore recommended 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. [H was adopted - 17 USC 1201 & 1202.]

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 users through a direct hypertext link to the remote content. Intellectual property owners whose files 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. 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.

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. A 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 will 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. 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 and 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.

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.(69)

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.(70) 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 or all of their life, they have had easy access—often in their home—to a number of devices they could use to infringe copyrights: 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.(71) 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,(72) that linking to a third party's materials is an infringement,(73) that forwarding an email to a mail list could be copyright infringement,(74) or that setting up a fan site could be an infringement.(75) 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.(76) Indeed, such an approach could ultimately prove economically counterproductive for intellectual property owners as well.(77)

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.(78) 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. In 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.(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."

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.\(^{81}\)

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.\(^{82}\) Under a variant of this approach, the vendor can lock off access after a certain number of uses (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.\(^{83}\) While users are unlikely to be significantly more responsive to copy protection schemes now, copy protection is currently being used in certain situations.\(^{84}\) 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.\(^{85}\) While this form of copy protection is probably not "hack-proof," it is sufficient to inhibit the vast majority of users from copying files.\(^{86}\)

4. Encryption Envelopes

Encryption envelopes are software devices which encrypt intellectual property in such a way that access can be obtained only by using the proper key.\(^{87}\) These devices are often referred to by IBM's trademark name "cryptolopes." Creators can protect their works by distributing files 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.\(^{88}\) An unresolved debate continues about the extent to which on-line shrinkwrap contracts (sometimes referred to as "clickthrough agreements") are enforceable.\(^{89}\) 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 home base to implement the business parameters imposed by the intellectual property owner. For example, Wave Interactive Networks <http://www.winhome.com/> provides a system which allows publishers to encrypt a file as a .wxn 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, by 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 certificate from either the vendor or a third party.

7. Copyright Clearinghouses

Under this approach, intellectual property owners would vest "clearinghouses" with the ability to 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.\(^{96}\)

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.\(^{97}\) 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 files 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.\(^{98}\) 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.\(^{99}\)

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.\(^{100}\) Copyright litigation not only helps the intellectual property owner obtain relief for specific acts of infringement, it publically warns others of the dangers of infringement. Indeed, a number of intellectual property owners have had well-publicized successes enforcing their copyrights against on-line infringers.\(^{101}\)

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.

15 of 28
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 clearer. This clarity will lead to the question, discussed in part VI.E, infra, of whether situations exist the intellectual property owner should have the obligation—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 (102) 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 (103).

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" (104) 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 (105). 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, the 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 (106).
- 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 (107).

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.\(^{108}\)

However, caching could cause harm because the copies in the cache are not necessarily the most current and up-to-date copies.\(^{109}\) 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 they have been replicated.\(^{110}\) Also, since caching is an infringement under a literal reading of U.S. copyright law, either caching must be the subject of an implied license or fair use defense or it 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.\(^{111}\) Why should the Internet create a new paradigm?

On the other hand, the normal functioning of the Internet is predicated on multiple infringements 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
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 to generate revenues without charging users for intellectual property.
- A wide variety of sustainable business models permit businesses to accomplish that end.
- 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 owners 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 legislation 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 to 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 Cummard, Viraj Jha, Michael Lean, Mark Lemley, Shawn Molodow, Ross Mutton, Mark Perkins, Eric Reifschneider, Lisa Sanger, Paul Startz, and Shelly Warwick.

The views expressed in this article are the author's own and do not necessarily reflect those of Cooley Godward or its clients. Cooley Godward represents some of the companies referenced in this article.

The author can be reached at schlachtere@cooley.com.

[Blll.J 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.


16. See Jessica Litman, The Exclusive Right to Read, 13 Cardozo Arts & Ent. L.J. 29, at 50-51 (1994), available at <http://yul.yu.edu/80/csl/journals/aelj/articles/13-1/litman.html> ("The current copyright statute has proved to be remarkably education-resistant.... [O]ur current copyright statute could not be taught in elementary school, because elementary school students couldn't understand it. Indeed, their teachers couldn't understand it. Copyright lawyers 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.cstar.ac.com/bf/>.

19. See part III.B supra. In part, transaction costs are limited due to current market conditions of pricing for access that does not vary with usage. There has been much discussion suggesting 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-gts/Economic_FAQs/FAQs/FAQs.html>.

20. A producer will continue to produce so long as the marginal revenue from an additional unit of output is greater than 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 intellectual 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 sell 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/pcweek/ExecConnect/0715/15emain.html> (describing a number of high-profile failures of Internet businesses). This limited empirical evidence does not yet prove 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 3 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/wired/4.12/esmadsen.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. Rebello, 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 to 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 received more patents than anyone else for 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 and 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 teaser to purchasing access to the remaining database of photos. See generally <http://www.yahoosearch.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/telex/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/speccress/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 entree 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 10E (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, Music 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).

with regard to the processing of personal data and the free movement of such data).


50. See Neil Gross & Peter McCoy, The Technology Paradox, Business Week, Mar. 6, 1995, at 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, prints 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. While 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. See Mark A. Lemley, Rights of Attribution and Integrity in On-line Communications, 1995 J. On-line 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 note 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 only on 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/jun/96-1139.htm>, no consensus currently exists that the federal government should be dictating that licensees should be permitted to unilaterally impose contract terms on licensees. See U.C.C. proposed Article 2B (Mar. 21, 1997 draft) <http://www.lawlib.uh.edu/ucc2b/> (a controversial attempt to develop model state legislation permitting increased ease in the formation of unilateral contracts by licensees); 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 56.

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 on its server. Issues related to linking are discussed in part V.I.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 welcome, 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.ljx.com/internet/complain.html>. However, Totalnews does provide attribution to the sites it frames.

62. But see Cohen, Right to Read Anonymously, supra note 56 (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 Lucasfilms, the owner of Star Wars, contacted a dedicated fan who had established a Star Wars appreciation website regarding alleged infringements, the fan transcribed the conversation and posted the transcription on the website. After Lucasfilms 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," Lucasfilms 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. Borsok, 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 confuse 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).

87. See <http://www.cryptolope.ibm.com/wiacc.htm>; See also Digital Delivery's TitleBuilder
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.urich.edu/~joli/v111/hardy.html>; See also, O'Rourke, supra, note 56.

89. Cf. ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), available at <http://www.kentlaw.edu/7circuit/1996/jun/96-1139.htm> (holding that a shrinkwrap license, the functional equivalent of a "clickthrough" license, could constitute a properly formed contract); Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) (following ProCD); U.C.C. proposed Article 2B (Mar. 21, 1997 draft) <http://www.lawlib.uh.edu/ucc2b/> (making it easier for licensors to form shrinkwrap agreements with end users).

90. See InterTrust <http://www.intertrust.com/products/flow.html> (describing the DigiBox envelope, which communicates with a clearinghouse 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.ip-workshop/www/Griswold.html> (describing a software envelope which requires periodic confirmation with a home base prior to permitting further access); Stefik, supra note 2 (describing protocols to permit the permanent transfer or temporary lending 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 phonorecord 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 set 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/xanadu/faq.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' Copysite <http://www.ip2.com/copysite.cgi> (offering a service similar to Hyperstamps); cf. MarkWatch <http://www.markwatch.com/> (providing an automated monitoring service for trademark usage on the Internet); Alex Alben, The Death of Copyright in a Digital World: The Reports are Slightly 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).

98. See Digimarc <http://www.digimarc.com/~digimarc/>; Highwater FBI


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, ACLU 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 NII White Paper, supra note 2 at 64-65, then the linking site has arguably committed contributory infringement by substantially contributing to the user's infringement (which occurred during the process of browsing). 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. 345, 353-56 (1995), available at <http://yul.yu.edu:80/csl/journals/aeli/articles/13-2/elkin.html>. The assertion that browsing is an actionable infringement has met strong criticism. See id. at 354; Samuelson, supra note 3, 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 justifiably 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); Kristi Coale, Intelleccast Smartens Up to Banner Bypass, Wired News (Mar. 28, 1997) <http://www.wired.com/news/technology/story/2844.html> (describing how Intelleccast, a weather site, prevented links to its weather maps which bypassed the associated banner advertisements).

107. This is one of the features of the Copiesight 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.gowebelex.com/>, WebWhacker <http://www.ffg.com/whacker/index.html>, InContext Flashsite <http://www.incontext.com/products/flashsite/index.html> and DocuMagix HotCargo Express <http://www.documagix.com/products/hotcargo_express/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., NII 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. At 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 syops 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 syops should not be liable in this circumstance, statutory clarification would be useful.

---

BTLJ Home Page

Last modified Aug 3, 1997
IN THE UNITED STATES COURT FOR THE DISTRICT OF UTAH
CENTRAL DIVISION

ORDER

INTELLECTUAL RESERVE, INC., a Utah corporation,

Plaintiff,

vs.

UTAH LIGHTHOUSE MINISTRY, INC., a Utah corporation, et al.,

Defendants.

Case No. 2:99-CV-808C

This matter is before the court on plaintiff’s motion for preliminary injunction. Plaintiff claims that unless a preliminary injunction issues, defendants will directly infringe and contribute to the infringement of its copyright in the Church Handbook of Instructions ("Handbook").

Defendants do not oppose a preliminary injunction, but argue that the scope of the injunction should be restricted to only prohibit direct infringement of plaintiff’s copyright.

Having fully considered the arguments of counsel, the submissions of the parties and applicable legal authorities, the court grants plaintiff’s motion for a preliminary injunction. However, the scope of the preliminary injunction is limited.

Discussion

The United States Copyright Act allows a court to “grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain infringement of a copyright.” 17
U.S.C. § 502(a). Here, in determining whether plaintiff is now entitled to the injunctive relief, the following factors are to be considered:

(1) substantial likelihood that the movant will eventually prevail on the merits; (2) a showing that the movant will suffer irreparable injury unless the injunction issues; (3) proof that the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) a showing that the injunction, if issued, would not be adverse to the public interest.

Equifax Servs., Inc. v. Hitz, 905 F.2d 1355, 1360 (10th Cir. 1990) (quoting Lundgren v. Claytor, 619 F.2d 61, 63 (10th Cir. 1980)).

1. Likelihood of Plaintiff Prevailing on the Merits

First, the court considers whether there is a substantial likelihood that plaintiff will eventually prevail on the merits. Plaintiff alleges that the defendants infringed its copyright directly by posting substantial portions of its copyrighted material on defendants' website, and also contributed to infringement of its copyright by inducing, causing or materially contributing to the infringing conduct of another. To determine the proper scope of the preliminary injunction, the court considers the likelihood that plaintiff will prevail on either or both of its claims.

A. Direct Infringement

To prevail on its claim of direct copyright infringement, "[p]laintiff must establish both: (1) that it possesses a valid copyright and (2) that [d]efendants 'copied' protectable elements of the copyrighted work." Country Kids 'N City Clicks, Inc. v. Sheen, 77 F.3d 1280, 1284 (10th Cir. 1996). Defendants initially conceded in a hearing, for purposes of the temporary restraining order and preliminary injunction, that plaintiff has a valid copyright in the Handbook, and that defendants directly infringed plaintiff's copyright by posting substantial portions of the
copyrighted material. Defendants changed their position, in a motion to dismiss, claiming that plaintiff has failed to allege facts necessary to show ownership of a valid copyright. Despite the defendants' newly-raised argument, the court finds, for purpose of this motion, that the plaintiff owns a valid copyright on the material defendants posted on their website. Plaintiff has provided evidence of a copyright registration certificate, (see Verified Compl., Ex. A), and the certificate "constitutes prima facie evidence of the validity of the copyright." Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 831 (10th Cir. 1993). Defendants have not advanced any additional affirmative defenses to the claim of direct infringement. Therefore, the court finds that there is a substantial likelihood that plaintiff will prevail on its claim of direct infringement.

B. Contributory Infringement

According to plaintiff, after the defendants were ordered to remove the Handbook from their website, the defendants began infringing plaintiff's copyright by inducing, causing, or materially contributing to the infringing conduct of others. It is undisputed that defendants placed a notice on their website that the Handbook was online, and gave three website addresses of websites containing the material defendants were ordered to remove from their website. Defendants also posted e-mails on their website that encouraged browsing¹ those websites, printing copies of the Handbook and sending the Handbook to others.

Although the copyright statute does not expressly impose liability for contributory

¹ By so doing, defendants did not admit fault or liability. (See Consent to Extension of Temporary Order and Response, at 1.)

² This issue will be fully explored when the court decides the motion to dismiss.

² The term browse, as used in this order, means to call up or open a website onto a computer screen.
infringement,

[1] The absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements 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 accountable for the actions of another.


Liability for contributory infringement is imposed when ""one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."" Gershwin Publ's Corp. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971). Thus, to prevail on its claim of contributory infringement, plaintiff must first be able to establish that the conduct defendants allegedly aided or encouraged could amount to infringement. See Subafilms, Ltd. v. MGM-Pathe Comms., Co., 24 F.3d 1088, 1092 (9th Cir. 1994). Defendants argue that they have not contributed to copyright infringement by those who posted the Handbook on websites nor by those who browsed the websites on their computers.
1. Can the Defendants Be Liable Under a Theory of Contributory Infringement for the Actions of Those Who Posted the Handbook on the Three Websites?

   a. Did those who posted the Handbook on the websites infringe plaintiff’s copyright?

   During a hearing on the motion to vacate the temporary restraining order, defendants accepted plaintiff’s proffer that the three websites contain the material which plaintiff alleges is copyrighted. Therefore, plaintiff at trial is likely to establish that those who have posted the material on the three websites are directly infringing plaintiff’s copyright.

   b. Did the defendants induce, cause or materially contribute to the infringement?

   The evidence now before the court indicates that there is no direct relationship between the defendants and the people who operate the three websites. The defendants did not provide the website operators with the plaintiff’s copyrighted material, nor are the defendants receiving any kind of compensation from them. The only connection between the defendants and those who operate the three websites appears to be the information defendants have posted on their website concerning the infringing sites. Based on this scant evidence, the court concludes that plaintiff has not shown that defendants contributed to the infringing action of those who operate the infringing websites.

* Defendants also have stated that they believe the three websites contain the material which plaintiff alleges is copyrighted. (See Memo. Re: Contributory Infringement, at 9 n.6.)
2. *Can the Defendants Be Liable Under a Theory of Contributory Infringement for the Actions of Those Who Browse the Three Infringing Websites?*

Defendants make two arguments in support of their position that the activities of those who browse the three websites do not make them liable under a theory of contributory infringement. First, defendants contend that those who browse the infringing websites are not themselves infringing plaintiff’s copyright; and second, even if those who browse the websites are infringers, defendants have not materially contributed to the infringing conduct.

a. *Do those who browse the websites infringe plaintiff’s copyright?*

The first question, then, is whether those who browse any of the three infringing websites are infringing plaintiff’s copyright. Central to this inquiry is whether the persons browsing are merely viewing the Handbook (which is not a copyright infringement), or whether they are making a copy of the Handbook (which is a copyright infringement). See 17 U.S.C. § 106.

“Copy” is defined in the Copyright Act as: “material objects ... in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.” 17 U.S.C. §101. “A work is ‘fixed’ ... when its ... sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.” Id.

When a person browses a website, and by so doing displays the Handbook, a copy of the Handbook is made in the computer’s random access memory (RAM), to permit viewing of the material. And in making a copy, even a temporary one, the person who browsed infringes the
copyright. See MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993) (holding that when material is transferred to a computer's RAM, copying has occurred; in the absence of ownership of the copyright or express permission by licence, such an act constitutes copyright infringement); Marohio-Pl., Inc. v. National Ass'n of Fire Equip. Distrib., 983 F. Supp. 1167, 1179 (N.D. Ill. 1997) (noting that liability for copyright infringement is with the persons who cause the display or distribution of the infringing material onto their computer); see also Nimmer on Copyright §8.08(A)(1) (stating that the infringing act of copying may occur from "loading the copyrighted material . . . into the computer's random access memory (RAM)"). Additionally, a person making a printout or re-posting a copy of the Handbook on another website would infringe plaintiff's copyright.

b. Did the defendants induce, cause or materially contribute to the infringement?

The court now considers whether the defendants' actions contributed to the infringement of plaintiff's copyright by those who browse the three websites.

The following evidence establishes that defendants have actively encouraged the infringement of plaintiff's copyright. After being ordered to remove the Handbook from their

---

1 Although this seems harsh, the Copyright Act has provided a safeguard for innocent infringers. Where the infringer "was not aware and had no reason to believe that his or her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages . . ." 17 U.S.C. § 504(c)(2).

4 Plaintiff at this point has been unable to specifically identify persons who have infringed its copyright because they were induced or assisted by defendants' conduct, however, there is a substantial likelihood that plaintiff will be able to do so after conducting discovery. There is evidence that at least one of the websites has seen a great increase in "hits" recently. (See Pl.'s Reply Supp. Mot. Prelim. Inj., Ex. 5.) Also, plaintiff does not have to establish that the defendants' actions are the sole cause of another's infringement; rather plaintiff may prevail
website, defendants posted on their website: "Church Handbook of Instructions is back online!" and listed the three website addresses. (See PL’s Reply Supp. Mot. Prelim. Inj., Ex. 1; Memo. Re: Contributory Infringement, at 9 n.6.) Defendants also posted e-mail suggesting that the lawsuit against defendants would be affected by people logging onto one of the websites and downloading the complete handbook. (See id., Ex. 2.) One of the e-mails posted by the defendants mentioned sending a copy of the copyrighted material to the media. (See id.) In response to an e-mail stating that the sender had unsuccessfully tried to browse a website that contained the Handbook, defendants gave further instruction on how to browse the material. (See id.) At least one of the three websites encourages the copying and posting of copies of the allegedly infringing material on other websites. (See id., Ex. 4 ("Please mirror these files . . . . It will be a LOT quicker for you to download the compressed version . . . . Needless to say, we need a LOT of mirror sites, as absolutely soon as possible.").)

Based on the above, the court finds that the first element necessary for injunctive relief is satisfied.

II. Irreparable Injury

Because this is a copyright infringement case and plaintiff has demonstrated a likelihood of success on the merits, there is a presumption of injury. See Country Kids ‘N City Sticks, Inc. v. Sheen, 77 F.3d 1280, 1288-89 (10th Cir. 1996). In addition, plaintiff will suffer additional immediate and real irreparable harm if defendants are permitted to post the copyrighted material or knowingly induce, cause or materially contribute to the infringement of plaintiff’s copyright by establishing that defendants’ conduct induces or materially contributes to the infringing conduct of another.
confusion as to the source of goods or services. " Cal. Bus. & Prof. Code § 14330. We have interpreted § 14330, like the Federal Trademark Dilution Act, to protect only famous marks. Fruit of the Loom, Inc. v. Girouard, 994 F.2d 1359, 1362-63 (9th Cir. 1993); see 3 J. Thomas McCarthy, Trademarks & Unfair Competition § 24:108 (Supp. 1998).

IV. Standard of Review

We review the district court's grant of a permanent injunction de novo. Erickson v. United States ex rel. Dep't of Health & Human Servs., 67 F.3d 858, 861 (9th Cir. 1995). To determine the legality of the injunction, we consider de novo the underlying grant of summary judgment to Avery Dennison and denial of summary judgment to Appellants. See Margolis v. Ryan, 140 F.3d 850, 852 (9th Cir. 1998). Viewing the evidence in the light most favorable to the non-moving party, summary judgment is appropriate if no genuine issues of material fact exist and the moving party is entitled to judgment as a matter of law. Id.

V. Dilution Protection

We now turn to the dilution causes of action at issue in this case, brought under the Federal Trademark Dilution Act and California Business and Professional Code § 14330.

In Panavision, we held that both the Federal Trademark Dilution Act and § 14330 were implicated when the defendant registered domain-name combinations using famous trademarks and sought to sell the registrations to the trademark owners. 141 F.3d at 1318, 1327. Three differences made Panavision easier than the instant case. First, the defendant did not mount a challenge on the famousness prong of the dilution tests. Panavision, 141 F.3d at 1324. Second, the Panavision defendant did not challenge the factual assertion that he sought to profit by arbitrage with famous trademarks. Id. at 1324-25. Third, the diluting registrations in Panavision both involved the TLD <.com>. In the instant case, by contrast, Appellants contest Avery Dennison's claim of famousness, Appellants contend that the nature of their business makes the trademark status of "Avery" and "Dennison" irrelevant, and the complained-of registrations involve the TLD <.net>.

A. Famousness

The district court considered evidence submitted by Avery Dennison regarding marketing efforts and consumer association with its marks and concluded as a matter of law that "Avery" and "Dennison" were famous marks entitled to dilution protection. 999 F. Supp. at 1339. We hold that Avery Dennison failed to create a genuine issue of fact on the famousness element of both dilution statutes.4

Dilution is a cause of action invented and reserved for a select class of marks -- those marks with such powerful consumer associations that even non-competing uses can impinge on their value. See generally Frank L. Schecter, The Rational
by others.

III. Harm to Defendants

Defendants argue that their First Amendment rights will be infringed by a preliminary injunction. However, the First Amendment does not give defendants the right to infringe on legally recognized rights under the copyright law. See Cable/Home Comm. Corp. v. Network Productions, Inc., 902 F.2d 829, 849 (11th Cir. 1990). "[C]opyright interests [] must be guarded under the Constitution, and injunctive relief is a common judicial response to infringement of a valid copyright." Id. The court, in fashioning the scope of injunctive relief, is aware of and will protect the defendants' First Amendment rights.

IV. The Public Interest

Finally, it is in the public's interest to protect the copyright laws and the interests of copyright holders.

Order

Therefore, for the reasons stated, the court orders the following preliminary injunction:

1. Defendants, their agents and those under their control, shall remove from and not post on defendants' website the material alleged to infringe plaintiff's copyright;

2. Defendants, their agents and those under their control, shall not reproduce or distribute verbatim, in a tangible medium, material alleged to infringe plaintiff's copyright;

3. Defendants, their agents and those under their control, shall remove from and not post on defendants' website, addresses to websites that defendants know, or have reason to know, contain the material alleged to infringe plaintiff's copyright;

Defendants have not requested that a security be obtained from plaintiff. If defendants
consider a security to be appropriate in this case, defendants shall file a motion and memorandum within twenty days from this date. Plaintiff shall then have fifteen days after service to respond. A reply memorandum may be filed by defendants within seven days after service.

IT IS SO ORDERED this _6_ day of December, 1999.

BY THE COURT:

TENA CAMPBELL
United States District Judge
§ 230. Protection for private blocking and screening of offensive material

(a) Findings. 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. It is the policy of the United States--

(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.

(1) Treatment of publisher or speaker. 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.

(2) Civil liability. No 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) Obligations of interactive computer service. A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws.

(1) No effect on criminal law. Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act [47 USCS § 223 or 231], chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code [18 USCS §§ 1460 et seq. or §§ 2251 et seq.], or any other Federal criminal statute.

(2) No effect on intellectual property law. Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law. Nothing 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 inconsistent 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 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.

(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.

HISTORY: (June 19, 1934, ch 652, Title II, Part I, § 230, as added Feb. 8,
Website Provider Liability for User Content and Actions
By Cooley Godward’s Information Technology Group

Introduction. Many websites have found that developing an online "community" is crucial to obtaining their business objectives. As a result, user-generated content is ubiquitous online.

While user-generated content can facilitate a website’s objectives, it raises a host of thorny legal issues. Default legal rules may impose liability on websites for intellectual property infringement and other harms caused by their users, and a single bad user could cause liability ranging into the millions of dollars. There have now been over a dozen cases on the topic, some with sensible rulings and others raising the specter of effectively unlimited liability.

Websites planning to permit users to exchange content should implement a number of techniques to manage their potential risk. This article identifies some of the problems arising from permitting user-generated content on websites and provides a few general suggestions for managing the associated risks.

Sources of Liability. Below are a few of the most common legal issues websites encounter when permitting user-generated content.

Intellectual Property Infringement.

Copyright. Copyright law recognizes three types of liability: direct, contributory, and vicarious.

Direct Infringement

Direct infringement occurs when an infringer copies a copyrighted work. Direct liability is a strict liability offense, and thus does not require the infringer to know he or she is infringing. If direct infringement applies, a website provider would be liable if a user posts a copyrighted work that is subsequently downloaded or viewed by others.

Some courts held website providers directly liable for user-committed copyright infringement, while other courts rejected imposing direct liability as unduly harsh and instead analyzed infringement claims against website providers under contributory or vicarious liability.

This fall, Congress enacted the Digital Millennium Copyright Act (the "DMCA"). The DMCA contains a number of provisions purporting to limit website liability for user-committed copyright infringements. Most specifically, the DMCA has established some safe harbors for websites from direct infringement if the websites follow the statutory schemes. Among other things, eligibility requires the website to (a) adopt a provision in its user agreement regarding the termination of repeat infringers, (b) accommodate and not interfere with "standard" technical measures used by copyright owners to identify and protect copyrighted works, and (c) provide certain information regarding an agent for service of process both on its website and to the Copyright Office.

The DMCA also sets up a complicated scheme to permit websites to avoid liability for taking down allegedly infringing material. In general, to avoid liability, this scheme requires the website to notify the user about the complaint and then take certain actions based on the user’s response. We are not aware of any claim ever brought by a user against a website for taking down allegedly infringing material, so we are unclear of the benefit of this safe harbor. As a result of their dubious efficacy, websites might choose not to follow the complicated procedures.

Contributory Infringement

Contributory infringement occurs when a party knows of an infringing activity and substantially participates in that activity. While the existing cases have not definitively addressed when a website is contributorily infringing based on its users’ activities, the cases generally have suggested a notice-based liability standard. In other words, once a website receives notice that a user is committing infringement,
the website will be deemed to be substantially participating in the infringement if it does not remove the infringement within a reasonable period of time. While the standards for notice historically have been murky, the DMCA clarified that the following elements are required to be a sufficient notice: (1) a signature, (2) identification of the work infringed (or if multiple works are infringed, a representative sample), (3) identification of the infringing work with sufficient information to permit the service provider to find it, (4) contact information of the notifier, (5) a statement that the notifier has a good faith belief that the use was not authorized, and (6) a statement that the information in the notice is accurate and, under penalty of perjury, that the notifier is authorized to act on behalf of the owner. A notice that does not substantially contain the foregoing probably can be ignored, unless the notice contains (2), (3) and (4), in which the website provider can ignore the notice only after contacting the notifier or taking other reasonable steps to try to get a conforming notice.

Of course, if a website actually knows of a particular infringement based on its practices, this knowledge will also trigger the duty to act. Thus, to minimize exposure for contributory copyright infringement, websites should (a) try to reduce actual knowledge of user-generated content by not monitoring their services, and (b) respond promptly to proper notices alleging that a user is committing copyright infringement.

The DMCA expressly carves out contributory infringement from the scope of its safe harbors. Thus, other than providing the standards for sufficient notice, the DMCA provides websites no relief from contributory copyright infringement.

Vicarious Infringement

Vicarious copyright infringement occurs when a party has the right and ability to control the infringer and reaps a direct financial benefit from the infringing activity. As a practical matter, many websites take the position that they have little or no ability to control their users. However, cases suggest that even nominal indicia of the right and ability to control users—such as a user agreement that contains subjective and arbitrary restrictions on users, or a pattern of disabling users’ accounts or yanking user content—could, when aggregated, lead to a finding that the website has the "right and ability to control" the infringing user.

Some cases have found "direct financial benefit" merely when parties charge flat fees for their services, even if these fees do not vary based on the amount of infringement committed by others. However, if these precedents are not followed, it is likely that a website will be deemed to have a direct financial benefit if its business model creates additional revenues as increased infringement occurs. This may occur when a website charges a transaction fee based on user activity (which includes situations where user activity is infringing) or when a website delivers advertisements on user content (which includes infringing content). In these circumstances, it is imperative that the website reduce all indicia of their right and ability to control their users—or else, regardless of their claim that it was not practical or possible to manage their users, the website may become vulnerable to claims, no matter how unjustified they may seem, for act of infringement committed by users.

The DMCA expressly carves out vicarious infringement from the scope of its safe harbors. Thus, the DMCA provides websites no relief from vicarious copyright infringement.

Trademark. Trademark law prevents the use of trademarks of others in a manner that creates a likelihood of confusion about the source of goods or services or in a manner that dilutes the value of the trademark. As with copyright law, liability can be found for direct, contributory, or vicarious infringement.

Of these three types of liability, websites face the greatest risk that they may be contributorily infringing based on their users’ content. Contributory trademark infringement occurs when a party supplies a "product" (such as a web page) knowing that the "product" is being used to infringe a third party’s trademark. Thus, in this respect, contributory trademark infringement appears to have the same characteristics as contributory copyright infringement—actual knowledge or notice of infringement initiates a duty to cease further infringement or face liability.
Defamation and Other "Publisher/Speaker" Torts. Section 230(c)(1) of the Communications Decency Act, passed in 1996, says "no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider." To date, courts have treated this language as a nearly complete bar against liability for users' defamatory postings.

While this statutory safe harbor has provided some welcome relief to websites, it is not a panacea. First, the safe harbor applies only to information "provided by another information content provider." Thus, information provided by employees and, perhaps, some independent contractors may still create liability. Second, the only claims courts have determined to be covered by the statute are defamation and certain conduct related to child pornography, and it is unclear whether other claims such as publicity or privacy rights violations would be covered by the statute. Intellectual property and federal criminal laws (including federal obscenity/child pornography claims) are not affected by the statute, and the words "publisher or speaker" have not been sufficiently interpreted to explain what other types of claims will be protected under the statute. Finally, the safe harbor applies only to "interactive computer services," a term which is not well-defined in the statute and which may not cover websites.

Obscenity and Child Pornography. No cases specifically address website liability for user-generated obscenity or child pornography. Websites faced with state law obscenity or child pornography charges can argue that such claims qualify for immunity under §230(c), but this defense is not certain. Further, the safe harbor in the Communications Decency Act (discussed above) expressly excludes federal criminal obscenity and child pornography laws from its safe harbor. Thus, websites could be liable for user-generated obscenity or child pornography in certain circumstances.

Other Claims. Until the scope of the Communications Decency Act's safe harbor is more fully understood, the range of potential claims against websites is impossible to define. If the safe harbor defense is not available, websites will need to develop other defenses, if they can, against claims for user-caused harms and attendant claims that the website knew of the harm and failed to take reasonable actions to prevent or remedy the harm.

Risk Management Suggestions. In light of the above analysis, Cooley Godward continues to believe that websites should take steps to avoid knowing their users' activities and content and, in most cases, reduce indicia of their right and ability to control user behavior and content. Thus, we propose that websites consider the following recommendations:

* Do Not Actively Monitor the Website. Active monitoring of the website will give the website actual or putative knowledge of user conduct and content. Thus, active monitoring creates the possibility that a website will be liable for all user-caused harms except those preempted by the Communications Decency Act's safe harbor.
* Consider Empowering Independent Contractors to Monitor the Website. Some websites believe that active monitoring is crucial to their business objectives. In these cases, the websites should have independent contractors do the monitoring. If done properly, the website will not be liable for the independent contractors' monitoring or knowledge of user content. However, to ensure that the independent contractors will not be deemed agents of the website—in which case this risk management strategy will have failed—the independent contractors must be given the authority necessary to resolve problems they find.
* Respond to Complaints. Although in general websites should minimize contact with user-generated content, if a website receives a legitimate complaint about user content (and, in the case of copyright infringement, the notice meets the statutory standards), it usually has a duty to respond promptly (unless the claim is preempted by the safe harbor in the Communications Decency Act).
* Review and Update the User Agreement. Provisions enabling websites to blacklist subscribers or edit content based on subjective or arbitrary standards provide strong evidence of the site's right and ability to control its users and their content. Thus, user agreements should only prohibit users from engaging in conduct that is illegal or tortious, or that interferes with the technological operation of the
site. Further, Congress has specified certain language that should be in a user agreement: (1) to be eligible for the DMCA safe harbors, the user agreement must say that repeat infringers will be terminated, and (2) in a separate statute, Congress required "interactive computer services" to notify their users of the availability of filtering tools.

* **Train Employees.** All employees who interact with the website can take legally significant actions that could undermine a risk management strategy. Thus, the website’s risk management strategy should be explained to all employees, and employees responsible for dealing with website problems should be given special training on how to implement the strategy.

* **Register with the Copyright Office.** To be eligible for one of the DMCA safe harbors, notice must be filed with the Copyright Office, with the same information placed on the website. For more information, see http://lcweb.loc.gov/copyright/onlinesp/.

* **Insurance.** Insurance is becoming increasingly available for risks associated with user-generated content. Insurance provides an excellent way to convert the risk of major liability into a manageable expense.

**Conclusion.** Deploying an effective strategy to manage risks associated with user-generated content is a complex and multifaceted effort with significant implications for the website, its relations with its users, and its associated liability. This article provides only a overview of the problems. Each website has its own unique business and technical practices that can minimize—or exacerbate—the problems described herein. Thus, websites should carefully map out and deploy a risk management strategy to meet their needs, and they continue to monitor developments to ensure maximum benefit as the law changes.

*About the author:* Cooley Godward LLP, a law firm with over 380 attorneys, serves clients from seven offices in California, Colorado and Washington. The Information Technology practice group consists of approximately 30 attorneys firmwide dedicated solely to providing information technology companies with focused, expert assistance in the acquisition, use and commercialization of information technology products.
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

PLAYBOY ENTERPRISES, INC.,
Plaintiff,

v.

RUSS HARDENBURGH, INC.,
Defendant.

No. 1:93 CV 0546.
Filed Nov. 25, 1997.

SAM H. BELL, District Judge.

ORDER:

This case raises the question of a computer bulletin board system operator's liability for copyright and trademark infringement regarding information available to its customers through their home computers. Plaintiff Playboy Enterprises, Inc. ("PEI") asks the court to find that Defendants Rusty-N-Edie's, Inc. ("RNB") and Russ Hardenburgh are liable for direct and/or contributory copyright infringement with respect to 412 graphic image files ("GIFs") which were allegedly available to paying customers of Defendants' bulletin board service (the "BBS"). These files, asserts PEI, contain illegal copies of adult photographs from PEI's Playboy Magazine. PEI also claims that Defendants' violated section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a), by removing the name or trademark of PEI and distributing the photographs under other names for a profit. Defendants answer that there are genuine issues of material fact with respect to each of Plaintiff's claims, precluding summary judgment.

The court has considered the evidence and arguments of the parties, and is now prepared to offer its decision in this matter.

Plaintiff's motion for summary judgment is granted with respect to its claims of direct and contributory copyright infringement against both RNE and Mr. Hardenburgh. Plaintiff's motion is denied with respect to its Lanham Act claim, which claim shall be set forth for trial.

The court's reasoning in this matter is set forth below.

Background

A computer bulletin board service (''BBS'') offers home computer owners a method for obtaining information from a central source by use of a modem.[1] Remote computers access the central service through telephone lines. Files of information are stored in the central system, and subscribers may either "download" information into their home units, or "upload" information from their home units into the central files. The owner of the service controls the terms by which remote computer owners will be able to access the system, and typically will control the conditions under which information may be downloaded or uploaded.

BBS owners often provide other services to subscribers, including electronic mail capabilities, "chat
rooms" where many subscribers may communicate at once, and Internet access to the World Wide Web. Local bulletin board services such as the one in this case might be

[Page 3]

distinguished from massive on-line services such as America On-Line or Compuserve, which provide similar services to customers on a much larger scale.

Defendant RNE and its President, Russ Hardenburgh, began operating a local BBS out of Boardman, Ohio in the early days (relatively speaking) of this technology. In July of 1988, "Rusty-N-Edie's BBS" became available to owners of home computers. (2nd Hardenburgh Aff. Para. 1.) For a fee, subscribers received access to certain files which were otherwise off limits to the general public; and had the right to download a set number of megabytes of electronic information from these files every week. (Hardenburgh dep. pp. 120-122.) The BBS also provided e-mail services, chat lines, advertisements for goods, computer technical assistance, and a "matchmaker" dating service. (2nd Hardenburgh Aff. Para. 3.)

By January of 1993, the central BBS had grown to 124 computers, with nearly 6000 subscribers. (2nd Hardenburgh Aff. Para. 6.) Approximately 105,000 to 110,000 files were available for downloading, nearly half of which were graphic image files, or "GIFS." (Id.) A GIF is created by scanning a photograph to create digital data that can be run through a computer. GIFs from Rusty-N-Edie's BBS could be downloaded by the customer to his or her home computer, and could be viewed only with the assistance of certain specialized software. (Id.) Approximately 40,000 of the GIFs available to subscribers at this time, Defendants admit, contained "adult" photographs. (1st Hardenburgh Aff. Para. 6.)

To increase its stockpile of available information, and thereby its attractiveness to new customers, Defendants provided an incentive to encourage subscribers to upload information onto the BBS. Subscribers were given a "credit" for each megabyte of electronic data that they uploaded onto the system. For each credit, the subscriber was entitled to download 1.5 extra megabytes of electronic information, in addition to the megabytes available under the normal terms of subscription. (Hardenburgh dep. p. 157.) According to Defendants, information uploaded onto the BBS went directly to an "upload file" where an RNE employee briefly checked the new files to ascertain whether they were "acceptable," meaning not pornographic, and not blatantly protected by copyright. (Hardenburgh dep. p. 138-142.)

PEI is understandably concerned that on-line systems can be used to transmit copies of its copyrighted photographs to people who have not themselves purchased Playboy Magazine. In the early 1990s, PEI employee Anne Steinfeldt was given the job of scanning on-line systems to determine whether such photographs were available to subscribers via their home computers. (2nd Steinfeldt Aff. Para. 1.) In November of 1992, Ms. Steinfeldt subscribed to Rusty-N-Edie's BBS under the pseudonym "Bob Campbell." (Id. at Para. 2.) She conducted key word searches in the files available on the BBS, and claims to have downloaded approximately 100 GIFs from the BBS which contained reproductions of PEI's photographs. (Id. at Para. 5.) She transferred these files to floppy disks, and then delivered the disks to PEI photo-librarian Timothy Hawkins. (Hawkins Aff. Para. Para. 2, 3.) Mr. Hawkins states that he examined the files by displaying the images on his computer monitor and comparing those images with photographs from Playboy Magazine. (Id. at Para. Para. 3, 4.)

On March 11, 1993, PEI filed its original complaint against RNE and Mr. Hardenburgh in this court, alleging copyright and trademark infringement. (Docket # 1.) The case was assigned to District Judge Battisti. On January 7, 1994, PEI moved for summary judgment on its claims of copyright infringement with respect to 99 GIFs allegedly downloaded from the BBS by Ms. Steinfeldt and reviewed by Mr. Hawkins. (Docket # 28.) PEI listed the
titles of the 99 GIFs at issue in its Exhibit A but only submitted ten actual copies of the allegedly infringing images. (Docket # 29.) PEI paired these ten reproductions of computer screens with ten virtually identical photographs from Playboy Magazine. (Id.) PEI also produced the certificates of copyright for each of the PEI photographs listed in its Exhibit A. (Id.) Based upon these submissions and the accompanying affidavits of its employees, PEI argued that Defendants could raise no genuine issue of material fact to dispute the assertion that all 99 GIFs had appeared on the BBS. (Id.) Defendants, PEI argued, were jointly and severally liable for copyright infringement as a matter of law.

On January 31, 1994, PEI moved for summary judgment on its Lanham Act unfair competition claim. (Docket # 33.) PEI argued that Defendants had falsely implied that they were the source of PEI's images by adding text to PEI photographs that was not present originally, and by deleting text that was originally present. (Id.) PEI claimed that the words "Rusty-N-Edies" had been added to some of the photographs along with the telephone number for one of Defendants' BBS phone lines. (Docket # 34.) PEI provided one actual example of this activity. (Id.)

Defendants responded to PEI's motions for summary judgment on February 24, 1994, arguing that there were genuine issues of material fact with respect to each of PEI's claims. (Docket # 40.) Defendants argued that PEI's submissions did not prove that the 99 GIFs listed in Exhibit A were actually present on the BBS. (Id.) Mr. Hardenburgh claimed that he had reviewed the floppy disks in question, and had found them to contain 85 GIFs, not 99. Only 82 of the files on the disks, he asserts, were even listed in Plaintiff's Exhibit A, four of which were created or modified after Ms. Steinfeldt turned the disks over to Mr. Hawkins. (1st Hardenburgh

[Page 6]

Aff. Para. 5.) Defendants argued that these inconsistencies cast doubt on the credibility of PEI employees Steinfeldt and Hawkins, and precluded summary judgment in PEI's favor. (Docket # 40.)

PEI replied to Defendants on June 10, 1994, and in doing so brought new evidence to light. (Docket # 46.) PEI explained to the court that on January 30, 1993 the Federal Bureau of Investigation had conducted an unrelated search of the Hardenburgh premises pursuant to a search warrant, and had seized Defendants' BBS equipment. (Id.; 1st Hardenburgh Aff. Para. 2.) In connection with this search, the FBI had created computer tapes (the "FBI Tapes") which contained all of the information present on the BBS at that time, including all GIFs available to subscribers for downloading. (1st Tesnakis Aff.) Both sides of the litigation, PEI explained, were in possession of copies of these tapes. (Gibson Aff. Para. Para. 4, 5, 6.) Having reviewed the tapes, PEI withdrew its motion for summary judgment with respect to 79 of the 99 GIFs originally at issue. PEI was apparently unable to confirm that these 79 GIFs were on the BBS at the time of the FBI search. (Docket # 46.) With respect to the other 20 GIFs, however, PEI asserted that the FBI Tapes conclusively established that these files were present on Defendants' BBS on January 30, 1993, and that they directly infringed PEI's copyrights. (Id.) PEI submitted copies of these 20 GIFs as extracted from the FBI Tapes, and also submitted the corresponding 20 photographs from Playboy Magazine. (Exhibit 2 to Tesnakis Aff.) PEI noted that it would continue to study the FBI Tapes to determine whether a future motion for summary judgment could be filed with respect to other files present on the BBS which may have infringed PEI's copyrights. (Docket # 46.)

Defendants surreplied to Plaintiff's answer on July 11, 1994. (Docket # 51.)

[Page 7]

Defendants implied that any PEI photographs which appeared on the BBS were placed there by RNE subscribers, not RNE employees. (Id.) Because Defendants had not themselves taken part in any infringing activity, they asserted, they could not have directly infringed PEI's copyrights. (Id.)

On September 14, 1994, Magistrate Judge Bartunek issued a Report and Recommendation regarding PEI's motions for summary judgment. (Docket # 60.) The Magistrate recommended that the court grant
Plaintiff's motion for summary judgment regarding Defendants' liability for direct copyright infringement. (Id.) The Magistrate found that there was no dispute that PEI owned the copyrights in question and that the 20 GIFs at issue had, in fact, appeared on Defendants' BBS. (Id.) Also, it was abundantly clear to the Magistrate that the GIFs produced by Plaintiff were copies of the 20 PEI photographs submitted into evidence. (Id.) As to Defendants' claim that it was BBS subscribers who uploaded the information onto the system, the Magistrate felt that this argument was immaterial in relation to a finding of copyright infringement. (Id.)

With respect to any Lanham Act violations, alternatively, the Magistrate recommended that the court deny Plaintiff's motion. (Id.) The Magistrate felt that in order to prevail on their Lanham Act claim, PEI would have to prove that it was Defendants, and not their subscribers, who engaged in activity which misled consumers about the source of the images. (Id.)

Both Plaintiff and Defendant filed objections to the Magistrate's Report and Recommendation. (Docket #s 64, 66, 69.)

On November 1, 1994, following Judge Battisti's death, the case was transferred to Senior Circuit Judge Krupansky. (Docket # 71.) Soon thereafter, on January 17, 1995, PEI filed its third motion for summary judgment. (Docket # 74.) As promised, PEI had scrutinized the FBI Tapes and announced that it was now prepared to prove that 392 additional GIFs containing copies of PEI photographs were present on Defendants' BBS at the time of the FBI search. (Docket # 75.) PEI produced, for the court's consideration, copies of each and every one of the GIFs at issue, in addition to the corresponding PEI photograph. (Exhibit D to 2nd Tesnakis Aff.) PEI also produced certificates of copyright for each photograph. (Exhibit B to 2nd Tesnakis Aff.) PEI repeated their claim that Defendants were liable for direct copyright infringement, but argued in addition that Defendants were liable for contributory copyright infringement. (Docket # 75.) PEI produced the deposition testimony of three RNE employees, each of whom stated that any GIFs which were uploaded onto the BBS were placed in an upload file, and were not released onto the system for subscribers until they were reviewed by RNE staff. (Hardenburgh dep., Little dep., McFarland dep.) Defendants responded, echoing many of the arguments they had made previously. (Docket # 88.) Defendants also argued that a finding of copyright infringement on the part of a computer bulletin board service would "halt the computer age at its inception" by overburdening BBS owners with the "impossible" task of screening their systems for any and all copyrighted material. (Id.) On March 1, 1996 the case was transferred here. (Docket # 104.)

The parties have offered numerous submissions and arguments in addition to those described above, some of which will be touched upon below. The question presented in this litigation, however, has remained fundamentally the same throughout. It is: has PEI produced sufficient evidence to warrant summary judgment on its claims of copyright and trademark infringement?

[Page 9]
Law and Analysis

PEI has moved for summary judgment on three independent claims. Each claim, the court will assume, applies to the 412 GIFs submitted into evidence.

I.

Direct Copyright Infringement

To sustain a case of direct copyright infringement, Plaintiff must first satisfy two threshold requirements. Plaintiff must prove "(1) ownership of a valid copyright, and (2) copying [by the defendants] of constituent elements of the work that are original." Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361, 111 S.Ct. 1282, 1296, 113 L.Ed.2d 358 (1991); Hi-Tech Video Prods., Inc. v. Capital Cities/ABC, Inc., 58 F.3d 1093, 1095 (6th Cir.1995), Wickham v. Knoxville Intl Energy Exposition, Inc., 739 F.2d 1094, 1097 (6th Cir.1984). PEI's certificates of copyright create a presumption of the validity of the copyrights in this case. 17 U.S.C.A. Section 410(c). Although the presumption may be rebutted, it is the burden of the party challenging the copyright to do so. Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 831 (10th Cir.1993). Defendants have not rebutted the ownership or validity of PEI's copyrights, which the court takes as established.

To prove the "copying" element, Plaintiff may either produce direct evidence that Defendants copied their material, or may create an inference that copying occurred by showing: (1) that Defendants had access to the protected work, and (2) that the two works are substantially similar. Wickham, 739 F.2d at 1097; Novelty Textile Mills, Inc. v. Joan Fabrics Corp., 558 F.2d 1090, 1092 (2d Cir.1977). Plaintiffs have no difficulty establishing the "copying" element. First, Defendants clearly had access to Playboy Magazine and the photographs contained therein at the time that the GIFs allegedly appeared on their BBS. Playboy Magazine is publicly available material. Second, there is no arguing that the 412 GIFs produced by PEI are not substantially similar to the 412 PEI photographs in evidence. They are virtually exact reproductions.

Having satisfied these threshold requirements, Plaintiff can establish direct infringement by proving that Defendant used the accused copies in any of the ways described in > Section 106 of the Copyright Statute. Under 17 U.S.C. Section 106, a copyright owner has the exclusive right to, among other things: (a) reproduce the copyrighted work, (b) distribute copies of the copyrighted work to the public by sale or other transfer of ownership, and (c) display the copyrighted work publicly.

A.

Findings of Fact
This court is bound to construe all of the evidence in a light most favorable to Defendants, the non-moving parties. In so doing, the court finds that Plaintiff has conclusively shown the following to be true: (1) in January of 1993, Defendants were operating a computer BBS; (2) prior to this date, Defendants adopted an incentive program to encourage their subscribers to upload information onto the BBS in order to increase the stockpile of information available to customers (Hardenburgh dep. p. 157); (3) information uploaded onto the system from subscribers' home computers was held in an upload file where it was briefly screened by RNE employees before it was released, by those employees, onto the general BBS; (Hardenburgh dep. p. 138-142); (4) Defendants had notice that PEI was in the habit of enforcing its copyrights against BBS owners (Hardenburgh dep. p. 192, Hardenburgh Aff. Para. 5); (5) as of January 30, 1993, when the FBI Tapes were created, 412 GIFs were available on Defendants' general BBS which contained virtually exact reproductions of copyrighted photographs from Playboy Magazine. (Exhibit 2 to 1st Tesnakis Aff., Exhibit D to 2nd Tesnakis Aff.)

B.

Defendants' Arguments

According to Defendants, the facts described above are insufficient to warrant a judgment of direct copyright infringement. First, they argue that they did not in any way usurp

[Page 12]

one of the protected rights of PEI as a copyright owner. Defendants claim that they did not "reproduce" copies of PEI photographs by simply providing an incentive to subscribers to upload electronic data onto the BBS. It was the subscribers who scanned the copyrighted photographs and turned them into electronic data, and it was subscribers who uploaded the information onto the system. Similarly, they claim that they never "distributed" PEI photographs to their customers because it was the customers themselves who chose whether or not to download the GIFs from the central system to their home computer. Defendants describe themselves as passive providers of the space in which the pictures were passed from one party to another. Defendants argue that they never "publicly displayed" PEI photographs either, because subscribers to the BBS could only view the GIFs on their own computers in the privacy of their own home, and only with the help of certain specialized software.

Defendants make a number of policy arguments as well. They point out that BBS operators must develop methods of obtaining new information in order to stay competitive in the crowded on-line computer market. New customers will be drawn to the BBS or on-line service which provides the most information. The incentive system developed by RNE was a reasonable way, then, to maintain competitiveness and allow the company to grow. At the same time, they argue that it would have been impossible to police each and every uploaded file to ensure that it did not contain copyrighted material. While RNE employees could quickly view an uploaded file to determine whether it contained clearly inappropriate material such as, for instance, child pornography, it would be unthinkable to require these employees to determine the source of each and every photograph to ensure that there was no possibility of copyright infringement. To place such liability on the owners of a BBS, Defendants argue, is an excessive burden on the rights of

[Page 13]

free speech as embodied in the First Amendment. In addition, they claim that such liability threatens to dismantle the computer on-line industry.

Even if, Defendants continue, the on-line industry as a whole is not destroyed by imposing copyright liability on service providers, such liability will irreversibly disadvantage local BBS owners in relation to massive on-line systems. Local BBS operators are less able to spread the cost of copyright liability to their more limited pool of subscribers. The outcome of a regime which imposes direct liability on owners of on-line systems, they warn, is the eventual extinction of local providers. Defendants claim that such an outcome could not be consistent with the primary objective of copyright law, which is "not to
reward the labor of authors, but "to promote the progress of Science and useful Arts." *Feist*, 499 U.S. at 349.

C.

**Plaintiff's Arguments**

Plaintiff, on the other hand, argues that copyright laws are meant to protect copyright owners from a situation in which their private material is used, without permission, by a non-owner for profit. Defendants, PEI claims, profited from a system in which PEI photographs were illegally provided to consumers who did not themselves purchase Playboy Magazine. Instead, these consumers purchased subscriptions to Rusty-N-Edie's BBS, and received the Playboy pictures for free.

Plaintiff notes that Defendants were aware that PEI was in the habit of enforcing its copyrights. Defendants should have, therefore, used their screening procedures to keep any

and all PEI photographs off of the BBS. Instead, PEI asserts, Defendants adopted a policy of willful blindness, ignoring the strong likelihood that PEI pictures were being copied and sent onto the system, yet encouraging subscribers to continue to upload any and all photographs. Procedurally, RNE employees viewed each and every photograph that was uploaded onto the system, and then moved those photographs that were not discarded from the upload file to the central files where they became available to RNE customers. If direct copyright infringement carries with it a volitional element, Plaintiff argues, that requirement is satisfied by the participation of the RNE employees in the screening process.

In response to Defendants' policy arguments, Plaintiff admits that it may have been costly for Defendants to police their system to prevent copyrighted information from passing through it. Plaintiff asserts that it is more reasonable, however, to place the cost of protecting against copyright infringement on the parties who provide the system which facilitates infringement, rather than the innocent owner of the copyright. Even if this type of liability regime favors larger on-line providers, Plaintiff argues that the diversity of the on-line computer industry is not the responsibility of copyright owners. If Defendants cannot divine an efficient way to operate a computer BBS free of copyrighted material, Plaintiff argues, then Defendants have the option of leaving the industry.

Plaintiff also points out, correctly, that a finding of direct copyright infringement carries no scienter requirement. PEI need not show that Defendants had any knowledge that PEI materials were available to their subscribers. PEI need only establish the threshold elements, ownership and copying, and that Defendants violated an exclusive right of a copyright owner.

According to Plaintiff, the mere fact that Defendants provided the space in which

[Page 15]

PEI photographs were copied and exchanged is sufficient to warrant a finding of direct copyright infringement. In the event that the court finds there is a further volitional requirement, PEI points to the screening procedures and the participation of RNE employees in moving PEI photographs onto the system. These facts, Plaintiff argues, establish Defendants' direct participation in the infringement which took place.

C. [D.]

**Case Law**

The case law in this area is relatively sparse, and the matter is one of first impression in our circuit. The court offers a brief discussion of the major cases in the area, to provide a foundation for its decision today.
In *Playboy Enterprises v. Frena*, 839 F.Supp. 1552 (M.D.Fla.1993), District Judge Schlesinger was presented with facts not unlike those which are presently before this court. PEI had sued the owner of a BBS for direct and contributory copyright infringement because copies of its photographs were available to BBS subscribers. *Id.* at 1554. The defendant BBS owner argued that it was his subscribers, and not he, who had placed the photographs on the system. *Id.*

The differences between *Frena* and this case are few, but should be mentioned. First, in the *Frena* case, the defendant admitted that the photographs appeared on his BBS. There has been no such concession here, though Defendant has made no factual showing to the contrary. Second, and more importantly, there is no discussion in the *Frena* case of any screening procedure utilized by the defendant's BBS before uploads were released onto the general system. It appears that subscribers to Mr. Frena's BBS were able to upload information directly into the central files where they became immediately available to other subscribers. Mr. Frena, then, was even more of a passive participant in the copying and exchange of copyrighted photographs than are the Defendants in this case.

District Judge Schlesinger held that Mr. Frena was liable for direct copyright infringement. *Id.* at 1556-57. As in our case, PEI easily established the threshold elements of ownership/validity and copying. Moving on to the more difficult consideration, the court found that defendant had violated PEI's exclusive "distribution" and "display" rights. *Id.*

The court found that defendant had "distributed" PEI photographs simply by providing the space in which those photographs were uploaded and downloaded. The court stated that, "[t]here is no dispute that Defendant Frena supplied a product [the BBS] containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies itself [sic]." *Id.* at 1556. Judge Schlesinger apparently felt that a finding of direct copyright infringement does not carry with it a volitional element, or, if it does, that such requirement was satisfied by defendant's past action of setting up the BBS.

In regard to the violation of PEI's "display" rights, the court defined the word broadly, to include:

the projection of an image on a screen or other surface by any method, the transmission of an image by electronic or other means, and the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system.

*Id.* (citing H.R.Rep. No. 1476, 94th Cong., 2d Sess. 64 (Sept. 3., 1976), reprinted in U.S.Code Cong. & Admin. News 1976 p. 5659, 5677). The fact that PEI materials were only available to BBS subscribers did not change the public nature of the "display." *Id.* (citations omitted). The court did not consider whether Mr. Frena was liable for contributory copyright infringement.

In *Sega Enterprises Ltd. v. Maphia*, 857 F.Supp. 679 (N.D.Cal.1994), a computer software company sued the owner of a BBS for copyright infringement because copyrighted video games were available to BBS subscribers. The court granted plaintiff's request for a preliminary injunction, finding that plaintiff had shown a likelihood of success on the merits with respect to its claims of direct and contributory copyright infringement. *Id.* at 686. Plaintiff had shown its ownership of valid copyrights, and had proven that its games were available on defendant's system. *Id.*

The court was explicit in its discussion of contributory copyright infringement, holding that defendant's knowledge and encouragement of the infringing activity was sufficient to establish contributory liability.
Id. at 687. The court was less clear on the specific factors that led it to its finding of direct infringement. The court stated:

Sega has established a prima facie case of direct copyright infringement under 17 U.S.C. § 501. Sega has established that unauthorized copies of its games are made when such games are uploaded to the MAPHA bulletin board, here with the knowledge of Defendant Scherman. These copied games are thereby placed on the storage media of the electronic bulletin board by unknown users.

Sega has established that unauthorized copies of these games are also made when they are downloaded to make additional copies by users, which copying is facilitated and encouraged by the MAPHA bulletin board.

Id. at 686 (citations omitted). Because knowledge is not an element of direct infringement, the court seems to be saying, as in Frena, that the mere creation of a BBS is sufficient to establish direct infringement liability where copyrighted material appears on the system.


[N.D.Cal.1995], District Judge Whyte departed from the reasoning of Frena and Sega. The owner of certain copyrighted religious material sued a BBS operator when the material was unlawfully copied and criticized on his BBS. The court in Netcom, however, refused to hold the BBS liable for direct infringement based simply on the creation of a space where infringing activity occurred. The court reasoned:

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. Although some of the people using the machine may directly infringe copyrights, courts analyze the machine under the rubric of contributory infringement, not direct infringement.

Id. at 1369. To impose direct infringement liability on a BBS where the operator did nothing more than provide space where information is exchanged, "would result in liability for every single ... server in the worldwide link of computers transmitting [subscriber's] message to every other computer." Id. Although the copyright statute creates a strict liability regime, the court noted that "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." Id.

D. [E.]

**Defendants' Liability for Direct Copyright Infringement**

As a legal matter, the court would agree with Judge Whyte that a finding of direct copyright infringement requires some element of direct action or participation, for two primary reasons. First, the statute is cast in terms of activities which are reserved to copyright owners. 17 U.S.C. § 106. It follows that an infringer must actually engage in one of those activities in order to directly violate the statute. Setting up a computer bulletin board is not one of those activities. Merely encouraging or facilitating those activities is not proscribed by the statute. Second, it is the area of contributory liability which allows "the imposition of liability on certain parties who have not themselves engaged in the infringing activity." Sony Corp. v. Universal Studios, Inc., 464 U.S. 417, 435, 104 S.Ct. 774, 785, 78 L.Ed.2d 574 (1984) (footnote omitted). There would be no reason to bifurcate copyright liability into the separate categories of direct and contributory if any remote causal connection
to copyright infringement could be analyzed under theories of direct infringement.

That being said, the facts in this case, unlike \textit{Frena}, \textit{Sega}, and \textit{Netcom}, are sufficient to establish that Defendants themselves engaged in two of the activities reserved to copyright owners under 17 U.S.C. \textsection{106}. The court finds that Defendants distributed and displayed copies of PEI photographs in derogation of PEI's copyrights. This finding hinges on two crucial facts: (1) Defendants' policy of encouraging subscribers to upload files, including adult photographs, onto the system, and (2) Defendants' policy of using a screening procedure in which RNE employees viewed all files in the upload file and moved them into the generally available files for subscribers.

These two facts transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement. Defendants admit that they were operating a service where the quantity of adult files available to customers increased the attractiveness of the service. Defendants actively encouraged their subscribers to upload such files. Defendants had control over which files were discarded and which files were moved into the general system. Defendants knew that there was a possibility that PEI photographs were being uploaded onto the system, but failed to adopt procedures which ensured that any and all PEI photographs would be discarded. It is inconsistent to argue that one may actively encourage and control the uploading and dissemination of adult files, but cannot hold liable for copyright violations because it is too difficult to determine which files infringe upon someone else's copyrights.

Distributing unlawful copies of a copyrighted work violates the copyright owner's distribution right and, as a result, constitutes copyright infringement. \textit{Hotaling v. Church of Jesus Christ of Latter Day Saints}, 118 F.3d 199, 203 (4th Cir.1997). In order to establish "distribution" of a copyrighted work, a party must show that an unlawful copy was disseminated "to the public." \textit{National Car Rental v. Computer Associates}, 991 F.2d 426, 434 (8th Cir.1993). The phrase "to the public," in this sense, includes paying subscribers to an otherwise publicly available service. \textit{See Thomas v. Pansy Ellen Products}, 672 F.Supp. 237, 240 (W.D.N.C.1987) (display at trade show was public even though limited to members); \textit{Ackee Music, Inc. v. Williams}, 650 F.Supp. 653 (D.Kan.1986) (performance of copyrighted songs at defendant's private club constituted public display). Defendants disseminated unlawful copies of PEI photographs to the public by adopting a policy in which RNE employees moved those copies to the generally available files instead of discarding them.

Similarly, Defendants violated PEI's right of public display. The comment to 17 U.S.C. Section106 states that a display is public if "it takes place 'at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances are gathered.' " H.R.Rep. No. 1476, 94th Cong., 2d Sess. 64 (Sept. 3, 1976), reprinted in U.S.Code Cong. & Admin. News 1976 p. 5659, 5677. "The same principles apply whenever the potential recipients of the transmission represent a limited segment of the public, such as the occupants of hotel rooms or the subscribers of a cable television service." \textit{Id}. Defendants displayed copies of PEI photographs to the public by adopting a policy which allowed their employees to place those photographs in files available to subscribers.

Defendant RNE, the corporate owner of "Rusty-N-Edie's BBS," is liable for direct copyright infringement based on its policies of active participation in the infringing activities. This summary judgment is also applicable to President Russ Hardenburgh. Mr. Hardenburgh may not use the corporate veil as a defense to this action.

In \textit{Southern Bell Tel. & Tel. v. Associated Tel. Directory Publishers}, 756 F.2d 801 (11th Cir.1985), the 11th Circuit Court of Appeals stated that "an individual, including a corporate officer, who has the
ability to supervise infringing activity and has a financial interest in that activity, or who personally participates in that activity is personally liable for the infringement." *Id.* at 811; *Vitabiotics, Inc. v. Krupa*, 606 F.Supp. 779, 785 (E.D.N.Y.1984) (holding an individual defendant jointly liable with three corporations active in marketing infringing materials). PEI has shown that Mr. Hardenburgh is the president and sole shareholder of the defendant corporation. (Hardenburgh dep. pp. 20-21.) Mr. Hardenburgh is also a paid employee of the corporation. (*Id.* at 62.) He has the sole ability to hire and fire employees on behalf of the corporation, and receives royalties paid to him by the corporation. (*Id.* at 56, 64-69.) Mr. Hardenburgh has the authority, right and ability to control the content of the BBS and its operations. (*Id.* at 73-91.) The summary judgment of direct copyright infringement is equally applicable to the corporation RNE and its President, Mr. Hardenburgh.

II.

**Contributory Copyright Infringement**

[Page 22]

A party shall be liable for contributory copyright infringement where it, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another." *Gershwin Publishing Corp. v. Columbia Artists*, 443 F.2d 1159, 1162 (2d Cir.1971). In *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984), the Supreme Court stated that:

[The 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 an individual liable for the actions of another.

*Id.* at 435.

The recent 9th circuit case of *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir.1996) is instructive. In *Fonovisa*, the District Court had granted summary judgment in favor of defendant, who operated a "swap meet" where consumers purchased merchandise from individual and independent vendors. Plaintiff sued defendant for providing the space in which its copyrighted material was illegally sold, but the District Court concluded that there was no liability for contributory infringement where defendant had neither supervised nor directly profited from the vendors' sales. *Id.* at 262. The 9th Circuit reversed the District Court's dismissal, holding that contributory liability could attach where "infringing performances enhance the attractiveness of the venue to potential customers" *Id.* at 263; *Columbia Pictures Industries Inc. v. Aveco Inc.*, 800 F.2d 59 (3rd Cir.1986) (providing the site and facilities for known infringing activity is sufficient to establish contributory liability.)

In the present case, Defendants clearly induced, caused, and materially contributed

[Page 23]

to any infringing activity which took place on their BBS. Defendants admit that they encouraged subscribers to upload information including adult files. Defendants admit that they benefitted from having more files available to their customers. Also, Defendants had at least constructive knowledge that infringing activity was likely to be occurring on their BBS. Defendants were aware that PEI was enforcing its copyrights against BBS owners. Moreover, Playboy Magazine is one of the most famous and widely distributed adult publications in the world. It seems disingenuous for Defendants to assert that they were unaware that copies of photographs from Playboy Magazine were likely to find their way onto the BBS. Defendants are liable for contributory copyright infringement.

III.
Unfair Competition

Section 43(a) of the Lanham Act, 15 U.S.C. Section 1125(a), provides:

(a)(1) Any person who, or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact which--

(A) is likely to cause confusion or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services or commercial activities by another person, or (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a). The Sixth Circuit has not addressed the elements necessary to prove a

[Page 24]

Lanham Act claim. Recent case law establishes that the following must be shown in order to prevail: (1) the advertisements at issue are false or misleading and the advertisements actually deceived or had the tendency to deceive a substantial segment of the audience, (2) the deceptive or misleading portions of the advertisement were material, in other words they were likely to influence the purchasing decision, (3) defendant caused the advertised goods to enter interstate commerce, and (4) plaintiff has been or is likely to be injured either by direct diversion of sales from itself to defendant or by lessening the goodwill or acceptability its products enjoy with the buying public. Telxon Corp. v. Symbol Technologies, Inc., 961 F.Supp. 1113, 1122 (N.D.Ohio 1996); Hobart Corp. v. Welbilt Corp., 1989 WL 449696 (Oct. 4, 1989 N.D.Ohio) (quoting Aipo Petfoods, Inc. v. Ralston Purina Co., 720 F.Supp. 194, 213 (D.D.C.1989) (citing Skil Corp. v. Rockwell Intl Corp., 375 F.Supp. 777, 783 (N.D.III.1974)); U-Haul Int'l, Inc. v. Jartran, Inc., 522 F.Supp. 1238, 1245 (D.Ariz.1981), aff'd, 681 F.2d 1159 (9th Cir.1982)).

Plaintiff has failed to satisfy at least one of these elements, that the deceptive or misleading portions of the copied photographs were material, that is, likely to influence the purchasing decision of BBS subscribers. Plaintiff has not shown that subscribers to "Rusty-N-Edie's BBS" were drawn to that system because they believed that the adult photographs contained therein were created by Defendants. Plaintiff has not shown that Defendants made any attempt, or had any incentive, to pass off PEI photographs as if they were created by "Rusty-N-Edie's," other than to avoid copyright liability. Plaintiff will need to produce further evidence at trial to prevail on its Lanham Act claim that Defendants misled consumers about the source of the images.

Conclusion

For the reasons set forth above, Plaintiff's motion for summary judgment is granted on its claims of direct and contributory copyright infringement against Defendants. Plaintiff's motion for summary judgment is denied on its claim of unfair competition under the Lanham Act. All remaining claims shall be set forth for trial. A final pre-trial conference will take place on Monday, January 26, 1998 at 1:30 p.m. Jury trial shall be scheduled to begin on February 3, 1998, with the parties on two-week standby.

IT IS SO ORDERED.
/s/Judge Sam H. Bell  
United States District Judge

FOOTNOTES:


2. Defendants have not gone so far as to say that a finding of copyright liability in this case would result in a deprivation of their rights under the First Amendment. Defendants have rather asked the court to weigh the interests protected by the First Amendment in determining the applicability of the copyright statute to the facts before it.
U.S. 4th Circuit Court of Appeals

ZERAN v AMERICA ONLINE INC

PUBLISHED UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
KENNETH M. ZERAN, Plaintiff-Appellant,

v.

AMERICA ONLINE, INCORPORATED, Defendant-Appellee. 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.

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. § 230 -- bars Zeran's claims. Zeran appeals, arguing that § 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that § 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 § 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgment 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 ways 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 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 pursuing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymous-motivated 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 relayed 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. After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. § 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. § 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 § 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 § 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. § 230(c)(1). By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 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. § 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. § 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, unfeathered by Federal or State regulation." Id. § 230(b)(2) (emphasis added).

None of this means, 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. § 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 § 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 § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, § 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 § 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 § 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 material." 47 U.S.C. § 230(b)(4). In line with this purpose, § 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 § 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 § 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 § 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected by § 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 § 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 § 558(b) (1977); Keeton et al., supra, § 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 publica-
tion. Restatement (Second) of Torts § 577; see also Tackett 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. Kee- ton et al., supra, § 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 avail-
able to others as to be regarded as publishers. They are intentionally making the contents available to others,
some- times without knowing all of the contents -- including the defamatory content -- and sometimes
without any opportu- nity 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 § 230's immunity.

Zeran contends that decisions like Stratton Oakmont and Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), recog- nize a legal distinction between publishers and distributors. He misap-
prehends, 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, § 113, at 799-800 (explaining that every party involved is charged
with pub- lication, 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 dif- ferent standards of liability. Stratton and Cubby do not, however, sug- gest 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 dis-
tributor in the eyes of the law. To the contrary, once a computer ser- vice 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 post- ing. In this respect, Zeran seeks to
impose liability on AOL for assuming the role for which § 230 specifically proscribes liability -- the
publisher role.

Our view that Zeran's complaint treats AOL as a publisher is rein- forced 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 defamatory 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 § 230 to impose liability on service providers with knowledge of
defamatory content on their ser- vices is consistent with the statutory purposes outlined in Part IIA.
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 § 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 investi- gation of the circumstances
surrounding the posted information, a legal judgment 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. Ayvaz v. CBS 60 Minutes, 806 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 discretionary calls"). 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. 267, 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 self-regulation.

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. Whenever 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 § 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 § 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. Solimeno, 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 § 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." It 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 [§ 230]," 47 U.S.C. § 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 incon- sistent 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 com- merce, 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) (cita- tions omitted). Here, Congress' command is explicitly stated. Its exer- cise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.

III.

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 § 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. Sec- tion 230 applies by its plain terms to complaints brought after the CDA became effective. As noted in Part II B, 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 sec- tion." 47 U.S.C. § 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, § 230 is addressed only to the bringing of a cause of action. Here, Zeran did not file his complaint until over two months after § 230's immunity became effective. Thus, the statute's application in this litig- ation is in fact prospective. See St. Louis v. Texas Worker's Compen- sation 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. Cas- sadega 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 frame- work would nevertheless require § 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 Prods., 511 U.S. 244, 280 (1994). This case can be resolved at this first step. In § 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. § 1997e(a), to "expressly go- vern[ ] 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. § 1915(g), to go- vern the bringing of new actions or filing of new appeals).

If we were to find a directive as plain as § 230(d)(3) to be ambigu- ous as to Congress' intent, we would be announcing a new super-clear-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 § 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

0302
right in a nonfinal tort judgment, much less an unfiled tort claim. Hammond v. United States, 786 F.2d 12 (1st Cir. 1986). Further- more, Zeran cannot point to any action he took in reliance on the law prior to § 230's enactment. Because § 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 judgment of the district court.

AFFIRMED

FOOTNOTES

1. 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.

2. 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. § 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. § 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."
Lunney v. Prodigy Services Company

New York State Court of Appeals

Text search found:

Lunney v. Prodigy Services Company

How to use WestLaw links

2 No. 164

Alexander G. Lunney, &c.,

Appellant,

v.

Prodigy Services Company, &c.,

Respondent,

et al.,

Defendants.

Thomas V. Marino, for appellant.

Michael J. Silverberg, for respondent.

National Law Center for Children and Families et al., amici curiae.

ROSENBLATT, J.:

Usurping the name of Alexander Lunney (a teenage Boy Scout and infant plaintiff in this appeal), an unknown imposter opened a number of accounts with Prodigy Services Company ("Prodigy"), an Internet Service Provider ("ISP"). The imposter posted two vulgar messages in Lunney's name on a Prodigy bulletin board and sent a threatening, profane electronic mail ("e-mail") message in Lunney's name to a third person. Lunney, by his father, has sued Prodigy, asserting that he has been stigmatized by being falsely cast as the author of these messages.[1] The principal issues before us are whether, under these circumstances, Prodigy may be held liable for defamation or negligence. For the reasons that follow, we hold
that the complaint against Prodigy was properly dismissed.

I. Background

On September 9, 1994, after opening several membership accounts with Prodigy under slightly different variants of the name Alex or Alexander Lunney, the imposter transmitted an e-mail message, under Lunney's name, to a local scoutmaster. The subject line of the message read "HOW I'M GONNA KILL U"; the body was vulgar in the extreme. After receiving the e-mail, the scoutmaster alerted the Bronxville police, as well as Lunney's scoutmaster. They investigated the matter, and readily accepted Lunney's denial of authorship, and his innocence in this episode.

While the investigation was afoot, Prodigy, by letter dated September 14, 1994, notified Lunney that it was terminating one of the accounts in his name "due to the transmission of obscene, abusive, threatening, and sexually explicit material through the Prodigy service and providing inaccurate profile information." Lunney, for his part, advised Prodigy that it was an imposter who, without authority, had opened the account and sent the message. Prodigy apologized to Lunney and also informed him that it had uncovered four more Alexander Lunney accounts and closed them all within two days after they were opened.

Lunney sued Prodigy, claiming, in essence, that Prodigy was derelict in allowing the accounts to be opened in his name, and was responsible for his having been stigmatized and defamed. During discovery Prodigy located and produced two additional vulgar messages that appeared on its electronic bulletin board with Alexander Lunney's name as sender dated September 5, 1994 and September 7, 1994. Prodigy also produced two internal memoranda pertaining to Prodigy's initial reasons for terminating the "Alexander Lunney" accounts before learning that they had been opened by an unauthorized imposter.[2]

Supreme Court denied Prodigy's three motions for summary judgment. On a consolidated appeal from the denial of the second and third motions, the Appellate Division reversed and granted summary judgment to Prodigy, holding that (i) the messages were not "of and concerning" Lunney and therefore did not defame him, (ii) although the messages were in extremely poor taste, the stigma associated with them did not amount to defamation and (iii) Prodigy was not the publisher of the messages, but even if it could be so considered, it was entitled to a qualified privilege sheltering it from liability (see, supra, Lunney v Prodigy Servs. Co., 250 AD2d 230, 233). We granted Lunney leave to appeal to this Court.

II. Analysis

As a threshold matter there is the question of whether the messages were defamatory. The Appellate Division expressed doubt on the point, considering that defamation cases most typically involve communications that directly impugn the plaintiff. Here, the messages were not about the plaintiff, but were ascribed to him. In supra Ben-Oliel v Press Pub. Co. (251 NY 250), this Court held that a
scholar stated a cause of action for libel based on the publication of a flawed article written by someone else, but improperly attributed to her (see, also, Clevenger v Baker Voorhis & Co., 8 NY2d 187). For purposes of this opinion we will assume that although he was not directly attacked, Lunney was defamed by being portrayed as the author of the foul material.

In a thoughtful opinion by Justice Bracken, the Appellate Division went on to hold that even if the material was "defamatory" Prodigy is protected by the common law privilege recognized in Anderson v New York Tel. Co. (35 NY2d 746). We agree with the Appellate Division's analysis and conclude that in the case before us the common law privilege should apply.

The E-Mail Message

We turn first to Lunney's claim stemming from the e-mail message. E-mail is the day's evolutionary hybrid of traditional telephone line communications and regular postal service mail.[3] As one commentator explained, "[t]o transmit a message, one must have access to an on-line service's e-mail system and must know the recipient's personal e-mail address" (see, Luftman, Defamation Liability for On-Line Services: The Sky is Not Falling, 65 Geo Wash L Rev 1071, 1081 [1997]). Once this is accomplished, a person may communicate by composing a message in the e-mail computer system and dispatching it telephonically (or through some other dedicated electronic line) to one or more recipients' electronic mailboxes. A recipient may forward the message or reply in like manner. Commercial on-line services, such as Prodigy, transmit the private e-mail messages but do not exercise any editorial control over them (see, Luftman, supra).

Because Lunney's defamation action is grounded in New York common law, we evaluate it in accordance with our established tort principles (see, Foster v Churchill, 87 NY2d 744, 751-752; Liberman v Gelstein, 80 NY2d 429, 434). Although they were fashioned long before the advent of e-mail, these settled doctrines accommodate the technology comfortably, and with apt analogies (see generally, Miranda, Defamation in Cyberspace: Stratton Oakmont, Inc. v Prodigy Services Co., 5 Alb LJ Sci & Tech 229, 237 [1996]).

In Anderson v New York Tel. Co., this Court was asked to determine whether a telephone company could be held liable as a publisher of a scurrilous message that a third party recorded and made available to the public by inviting anyone interested to dial in and listen (35 NY2d 746). The Court adopted the opinion of Justice Witmer in his dissent at the Appellate Division, concluding that the telephone company could not be considered a publisher, because in "no sense has * * * [i]t participated in preparing the message, exercised any discretion or control over its communication, or in any way assumed responsibility" (42 AD2d 151, 163). Anderson also holds that even if the telephone company could be counted as a publisher, it would be entitled to a qualified privilege subject to the common-law exception for malice or bad faith (42 AD2d, at 163-164).
**Anderson** emphasized the distinction between a telegraph company (in which publication may be said to have occurred through the direct participation of agents) and a telephone company, which, as far as content is concerned, plays only a passive role. The **Anderson** doctrine parallels the case before us. Prodigy's role in transmitting e-mail is akin to that of a telephone company; which one neither wants nor expects to superintend the content of its subscribers' conversations. In this respect, an ISP, like a telephone company, is merely a conduit. Thus, we conclude that under the decisional law of this State, Prodigy was not a publisher of the e-mail transmitted through its system by a third party.

Moreover, we are unwilling to deny Prodigy the common-law qualified privilege accorded to telephone and telegraph companies. The public would not be well served by compelling an ISP to examine and screen millions of e-mail communications, on pain of liability for defamation. Considering that in the case before us there is no basis upon which to defeat the qualified privilege, it should and does apply here.

**The Prodigy Bulletin Board Messages**

As distinguished from e-mail communication, there are more complicated legal questions associated with electronic bulletin board messages, owing to the generally greater level of cognizance that their operators can have over them. One commentator defines an electronic bulletin board as "storage media, e.g., computer memories or hard disks, connected to telephone lines via devices known as modems and controlled by a computer" (see, Segal, Dissemination of Digitized Music on the Internet: A Challenge to the Copyright Act, 12 Computer & High Tech LJ 97, 103 [1995]). In some instances, an electronic bulletin board could be made to resemble a newspaper's editorial page; in others it may function more like a "chat room."[4] In many respects, an ISP bulletin board may serve much the same purpose as its ancestral version, but uses electronics in place of plywood and thumbtacks. Some electronic bulletin boards post messages instantly and automatically, others briefly delay posting so as not to become "chat rooms," while still others significantly delay posting to allow their operators an opportunity to edit the message or refuse posting altogether (see, Sheridan, Zeran v AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet, 61 Alb L Rev 147, 152-153 [1997]).

Lunney argues that because Prodigy, in its membership agreements, reserves for itself broad editorial discretion to screen its bulletin board messages, it should be liable as a publisher of such messages. Prodigy, on the other hand, argues that while it reserves the right to screen its bulletin board messages, it is not required to do so, does not normally do so and therefore cannot be a publisher of electronic bulletin board messages posted on its system by third parties.

The Appellate Division aptly concluded that even if Prodigy "exercised the power to exclude certain vulgarities from the text of certain [bulletin board] messages," this would not alter its passive character in "the millions of other messages in whose transmission
it did not participate" (250 AD2d 230, 237), nor would this, in our opinion, compel it to guarantee the content of those myriad messages. We agree with the Appellate Division in its conclusion that, in this case, Prodigy was not a publisher of the electronic bulletin board messages. We see no occasion to hypothesize whether there may be other instances in which the role of an electronic bulletin board operator would qualify it as a publisher.

III. Other Issues Negligence

Lunney contends that Prodigy was negligent in failing to employ safeguards to prevent the imposter from opening the accounts in question. He would require an ISP to employ a "process for verification of the bona fides" of all applicants and any credit cards they offer so as to protect against defamatory acts. Prodigy contends that such a duty would require an ISP to perform investigations on millions of potential subscribers, so as to be guarantors against harmful transmissions. The rule plaintiff advocates would, in cases such as this, open an ISP to liability for the wrongful acts of countless potential tortfeasors committed against countless potential victims. There is no justification for such a limitless field of liability (Pulka v Edelman, 40 NY2d 781). If circumstances could be imagined in which an ISP would be liable for consequences that flow from the opening of false accounts, they do not present themselves here.

Communications Decency Act

The parties have disagreed over the applicability of the Communications Decency Act (47 USC § 230) ("CDA") and the merits of Zeran v America Online (129 F3d 327 [4th Cir 1997], cert denied 524 US 937). Prodigy has contended that the CDA should govern this case by retroactive application. It asks us to interpret the CDA to render an ISP unconditionally free from notice-based liability, insofar as the statute has been interpreted as granting federal immunity from "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" (see, Zeran v America Online, 129 F3d, at 330, supra). At this point we decline the invitation to come down on either side of this debate.[5] This case does not call for it.

We recognize of course that parties to a lawsuit, and surely others interested in the field, will look to decisions for points of guidance. For every new rule that a court sets down doubts are minimized, and practitioners are able to give counsel based on settled doctrine, rather than on open questions. While many decisions serve to establish rules that advance predictability, courts cannot go beyond the issues necessary to decide the case at hand. An ambition of that sort would entail something very much like drafting advisory opinions. Misdirected or misapplied, they can create the very kind of uncertainty, or confusion, that purposeful decisional law seeks to eliminate. These general observations apply even more compellingly when dealing with Internet law. Given the extraordinarily rapid growth of this technology and its developments, it is plainly unwise to lurch prematurely into
emerging issues, given a record that does not at all lend itself to their determination.

We have considered Lunney's remaining causes of action against Prodigy and find them to be without merit.

Accordingly, the order of the Appellate Division should be affirmed, with costs.

**FOOTNOTES**

[1]: Because this suit was commenced when Alexander Lunney was a minor, the action was brought in his name, by his father, J. Robert Lunney. Unless otherwise stated, "Lunney" refers to Alexander Lunney. Initially, Lunney named "John Doe," the unknown imposter, as a co-defendant, but that claim has been abandoned, and the case has proceeded only against Prodigy.

[2]: Lunney sought and was granted permission to amend his complaint to add claims against Prodigy based on the Prodigy bulletin board messages and the internal memoranda.

[3]: Now known colloquially as "snail mail" judging by its comparative speed (see, e.g., Salbu, Who Should Govern the Internet?: Monitoring and Supporting a New Frontier, 11 Harv J Law & Tech 429, 471-472 [1998]).

[4]: "Chat rooms" have been defined as services that allow multiple users "to 'talk' through simultaneous text postings" (see, Barrett, The Law of Diminishing Privacy Rights: Encryption Escrow and the Dilution of Associational Freedoms in Cyberspace, 15 NYL Sch J Hum Rts 115, 117 n14 [1998]).


Order affirmed, with costs. Opinion by Judge Rosenblatt. Chief Judge Kaye and Judges Smith, Levine, Ciparick and Wesley concur.

Judge Bellacosa took no part.
-CITE-

18 USC Sec. 1030

-EXPCITE-

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

-HEAD-

Sec. 1030. Fraud and related activity in connection with computers

-STATUTE-

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a
financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

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

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

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

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

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

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

(6) knowingly and with intent to defraud traffics (as defined
in section 1029) in any password or similar information through
which a computer may be accessed without authorization, if -

(A) such trafficking affects interstate or foreign commerce;

or

(B) such computer is used by or for the Government of the
United States; (FOOTNOTE 1)

(FOOTNOTE 1) So in original. Probably should be followed by
''or''.

(7) with intent to extort from any person, firm, association,
educational institution, financial institution, government
entity, or other legal entity, any money or other thing of value,
transmits in interstate or foreign commerce any communication
containing any threat to cause damage to a protected computer;
shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of
this section shall be punished as provided in subsection (c) of
this section.

(c) The punishment for an offense under subsection (a) or (b) of
this section is -

(1)(A) a fine under this title or imprisonment for not more
than ten years, or both, in the case of an offense under
subsection (a)(1) of this section which does not occur after a
conviction for another offense under this section, or an attempt
to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than
twenty years, or both, in the case of an offense under subsection
(a)(1) of this section which occurs after a conviction for
another offense under this section, or an attempt to commit an
offense punishable under this subparagraph;

(2)(A) a fine under this title or imprisonment for not more
than one year, or both, in the case of an offense under
subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section,
which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (FOOTNOTE 2)

(FOOTNOTE 2) So in original. The word ''and'' probably should not appear.

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if -

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

(FOOTNOTE 3)

(FOOTNOTE 3) So in original. Probably should be followed by ''and''.

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under
this subparagraph; and (FOOTNOTE 4)

(FOOTNOTE 4) So in original. The ';' and'' probably should be a period.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section -

(1) the term '"computer"' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term '"protected computer"' means a computer -

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication;

(3) the term '"State"' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term '"financial institution"' means -
(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) (FOOTNOTE 5) of the Federal Reserve Act. (FOOTNOTE 6)

(FOOTNOTE 5) See References in Text note below.

(FOOTNOTE 6) So in original. The period probably should be a semicolon.

(5) the term '"financial record'" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term '"exceeds authorized access'" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter;

(7) the term '"department of the United States'" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and

(FOOTNOTE 7)
(FOOTNOTE 7) So in original. The word "and" probably should not appear.

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that:

(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following