Cyberspace Law (Law 5793)
Eric Goldman and Chuck Schwab
Santa Clara University School of Law
Spring 2001

1. **SESSIONS.** The class meets on Monday nights from 7:30 to 9:10, except that the class will meet on Tuesday night on February 20. The first class meets on January 8 and the last class meets on April 23. Pursuant to University regulations, the class will not meet on January 15 (Martin Luther King birthday), February 19 (President’s Day), or February 26 (Spring break).

2. **PREREQUISITES.** This class is a general survey class and thus has no has no prerequisites other than the completion of first year courses. You also need to have some experience using the Internet.

3. **CURRICULUM OVERLAPS.** This class has significant overlaps with both Internet Law and E-Commerce Law, and we discourage you from taking this class if you’ve taken or will take those classes. There are also some overlaps with classes such as digitallaw.com, Davis/Boustani’s computer law course, and Digital Property, although students have rarely found such overlaps problematic.

4. **FINAL EXAM.** The final exam will be on April 28 at 2:30. The class is graded solely on the final exam; historically, there have been 1/3 As and 10% Cs. The final exam will probably be 1 1/2 hours long with 2 questions. The exam is very practice-oriented and will emphasize your problem-solving skills. You are strongly encouraged to review the prior years’ exams to understand the exam structure. You can find the prior years’ exams on the Web (note the law may have changed in the interim!):

<table>
<thead>
<tr>
<th>Year</th>
<th>Exam</th>
<th>Sample Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td><a href="http://members.theglobe.com/ericgoldman/2000exam.html">link</a></td>
<td><a href="http://members.theglobe.com/ericgoldman/2000examanswer.htm">link</a></td>
</tr>
<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/finals.html">link</a></td>
</tr>
</tbody>
</table>

5. **PAPERS.** A paper is not required as part of the class. However, we will be happy to assist you with your papers on an informal basis. Suggested paper topics are available at [link](http://members.theglobe.com/ericgoldman/issues.html). Additional paper resources are available from the list of cyberspace law resources at [link](http://members.theglobe.com/ericgoldman/tablecase.html).

Historically, acting as a faculty advisor for independent study has been very unsatisfying because students tend to do the minimum (despite their unanimous initial insistence to the contrary). If you want one of us to act as your faculty advisor, you will need to follow these rules:

- We will each take no more than 3 students
- All requests must be made by January 12, 2001—NO EXCEPTIONS
- With your request, you must submit a schedule of deliverables. Failure to honor this schedule will create significant tension
• You must handle all aspects of administrative compliance and paperwork
• You must be using the paper to fulfill the High Tech certificate or scheduled to publish the paper

6. **Email List.** The class has an official email list for class announcements, timely messages and occasional random postings. Subscribe to the list at cyberlaw2001-subscribe@globeclubs.com. Note that theglobe requires you to opt out of their mailing lists if you don’t want their spam—you can configure this at any time, but opt out when you sign up to minimize confusion.

The list is unmoderated, so you are free to post yourself—please do so wisely. Post to cyberlaw2001@globeclubs.com. DO NOT SEND SUBSCRIPTION MESSAGES OR PERSONAL MESSAGES TO THE LIST!!! List archives and account management are available at http://globeclubs.theglobe.com/computers_internet/law/cyberlaw2001-L/list.taf.

7. **High Tech Certificate.** The class is approved for credit towards the High Technology Law Certificate.

8. **Office Hours.** We do not hold on-campus office hours, but we are free to meet with you at our offices or otherwise by appointment. We are also always available by email for answer questions; however, we may take a few days to do so.

9. **Academic Freedom.** The class necessarily requires us to discuss the full range of human behavior. If you have any concerns about topic coverage, you should see one of us immediately.

10. **Jobs.** Eric can consult with you about your job searching efforts. He can provide you with the most help in the early part of the semester. If you want his help, email him your resume (in the text of the email, not as an attachment) and he’ll schedule a time to meet.

11. **Contact Information.**

<table>
<thead>
<tr>
<th>Eric Goldman</th>
<th>Chuck Schwab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epinions, Inc.</td>
<td>Cooley Godward LLP</td>
</tr>
<tr>
<td>8000 Marina Blvd., 5th floor</td>
<td>Mailing: 5 Palo Alto Sq., Palo Alto, CA 94306</td>
</tr>
<tr>
<td>Brisbane, CA 94005</td>
<td>Physical: 3175 Hanover, Palo Alto, CA 94043</td>
</tr>
<tr>
<td>Phone: (650) 616-6536</td>
<td>Phone: (650) 843-5347</td>
</tr>
<tr>
<td>Fax: (650) 616-6510</td>
<td>Fax: (650) 849-7400</td>
</tr>
<tr>
<td><a href="mailto:eric@epinions-inc.com">eric@epinions-inc.com</a></td>
<td><a href="mailto:cschwab@cooley.com">cschwab@cooley.com</a></td>
</tr>
<tr>
<td>Driving directions: 101N to Sierra Point</td>
<td>Driving directions: 101 to Oregon Expressway,</td>
</tr>
<tr>
<td>Parkway. Turn right. 8000 Marina Blvd. is</td>
<td>head west past El Camino, left on Hanover, left</td>
</tr>
<tr>
<td>the 8 story building behind Hitachi.</td>
<td>at the curve in Hanover</td>
</tr>
</tbody>
</table>

More materials, including an electronic copy of this syllabus, are available at http://members.theglobe.com/ericgoldman.
CLASS SCHEDULE AND READING MATERIALS

The class reader is the only required reading (except for any materials distributed during the semester). There are a number of supplementary books and treatises available on the market; all of them are out of date to some degree. If you want a supplemental reader, please contact us and we will work with you.

1. **INTRODUCTION TO CYBERSPACE** (January 8 and 22) [Eric/Chuck]

   Topics: Internet technologies, Internet business models, the Commerce Clause and state action

   ACLU v. Reno (CDA I district court ruling; facts only) page 5

2. **JURISDICTION AND VENUE** (January 29) [Chuck]

   Millennium Enterprises v. Millennium Music page 27

3. **CONTRACTS** (February 5) [Eric/Chuck]

   Topics: Clickthrough Agreements, UCITA, UETA/E-Sign

   Electronic Signatures in Global & National Commerce Act page 47
   Hill v. Gateway 2000 page 55
   Klocek v. Gateway, Inc. page 58

4. **COPYRIGHTS, TRESPASS AND THE PROTECTION OF FACTUAL DATA** (February 12 and 20) [Eric/Chuck]

   Topics: Linking, Framing, Scraping, Caching, Circumvention

   17 USC §512 page 68
   eBay v. Bidder's Edge page 78
   TicketMaster v. Tickets.com page 93
   Kelly v. Arriba Software page 96
   UMG Recordings v. MP3.com (5/4/00 ruling) page 112

5. **TRADEMARKS/DOMAIN NAMES** (March 5 and 12) [Eric]

   Topics: Domain Names Squatting and Reverse Hijacking, Metatags, Keyword Advertising

   Anticybersquatting Consumer Protection Act page 117
   ICANN Domain Name Dispute Resolution Policy (and associated rules) page 132
   Avery Dennison v. Sumpton (9th Circuit) page 150
6. **Privacy** (March 19) [Eric/Chuck]

Children’s Online Privacy Protection Act  
16 CFR Part 312 (implementing COPPA)  
Internet Privacy Policies handout  
*In re Toysmart Stipulation and Order Establishing Conditions on Sale of Customer Information*  

7. **Porn** (March 26) [Eric]

Topics: Obscenity, Child Pornography, "Indecent” Speech, “Harmful to Minors” Speech  

ACLU v. Reno (Supreme Court)  

8. **Selected Information Torts** (April 2) [Chuck]

Topics: CFAA, Spam, Defamation, Publicity/Privacy Rights, Harmful/Inaccurate Information  

18 USC §1030  
AOL v. Christian Brothers  

9. **Intermediary Liability for User Content/Actions** (April 9 and 16) [Eric]

17 USC §512  
47 USC §230  
Cooley Godward Alert on Website Provider Liability for User Content & Actions  
Zeran v. America Online (4th Circuit)  
Stoner v. eBay  
A&M Records v. Napster (Ninth circuit ruling) [ruling is not available at press time; case will be distributed electronically during the semester]  
Lockheed Martin v. Network Solutions (9th Circuit)  

10. **ECPA and Catch-Up** (April 23) [Chuck]

Topics: ECPA  

Note: Most of the cases and statutes above are available from  
http://members.theglobe.com/ericgoldman/tablecase.html  
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, 1996. (1) Telecommunications Act of 1996, Pub. L.
No. 104-104, § 502, 110 Stat. 56, 133-35. Plaintiffs include various organizations and

http://www.aclu.org/court/cdadc.html

11/26/00
(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 in turn connected to other networks in a manner which permits each computer in any
network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.

3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.

4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole.

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

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

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

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

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

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

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

How Individuals Access the Internet

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

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

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

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

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

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

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

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

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

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

Methods to Communicate Over the Internet

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

(1) one-to-one messaging (such as "e-mail"),

(2) one-to-many messaging (such as "listserv"),
(3) distributed message databases (such as "USENET newsgroups"),

(4) real time communication (such as "Internet Relay Chat"),

(5) real time remote computer utilization (such as "telnet"), and

(6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web").

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

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

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

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

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

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

28. In addition, commercial online services such as America Online, CompuServe, the Microsoft Network, and Prodigy have their own "chat" systems allowing their members to converse.

29. Real time remote computer utilization. Another method to use information on the Internet is to access and control remote computers in "real time" using "telnet." For example, using telnet, a researcher at a university would be able to use the computing power of a supercomputer located at a different university. A student can use telnet to connect to a remote library to access the library's online card catalog program.

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

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

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

The World Wide Web

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

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

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

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

38. As an example of the use of links, if these Findings were to be put on a World Wide Web site, its home page might contain links such as those:

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

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

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

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

42. Information to be published on the Web must also be formatted according to the rules of the Web standards. These standardized formats assure that all Web users who want to read the material will be able to view it. Web standards are sophisticated and flexible enough that they have grown to meet the publishing needs of many large corporations, banks, brokerage houses, newspapers and magazines which now publish "online" editions of their material, as well as government agencies, and even courts, which use the Web to disseminate information to the public. At the same time, Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal "home pages," the equivalent of individualized newsletters about that person or organization, which are available to everyone on the Web.
43. Web publishers have a choice to make their Web sites open to the general pool of all Internet users, or close them, thus making the information accessible only to those with advance authorization. Many publishers choose to keep their sites open to all in order to give their information the widest potential audience. In the event that the publishers choose to maintain restrictions on access, this may be accomplished by assigning specific user names and passwords as a prerequisite to access to the site. Or, in the case of Web sites maintained for internal use of one organization, access will only be allowed from other computers within that organization's local network.(11)

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

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

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

47. Contrast to closed databases. The Web's open, distributed, decentralized nature stands in sharp contrast to most information systems that have come before it. Private information services such as Westlaw, Lexis/Nexis, and Dialog, have contained large storehouses of knowledge, and can be accessed from the Internet with the appropriate passwords and access software. However, these databases are not linked together into a single whole, as is the World Wide Web.
48. Success of the Web in research, education, and political activities. The World Wide
Web has become so popular because of its open, distributed, and easy-to-use nature.
Rather than requiring those who seek information to purchase new software or hardware,
and to learn a new kind of system for each new database of information they seek to
access, the Web environment makes it easy for users to jump from one set of information
to another. By the same token, the open nature of the Web makes it easy for publishers to
reach their intended audiences without having to know in advance what kind of computer
each potential reader has, and what kind of software they will be using.

Restricting Access to Unwanted On-Line
Material(12)

PICS

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

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

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

Adobe Systems, Inc.
Apple Computer
America Online
AT&T
Center for Democracy and Technology
CompuServe

http://www.aclu.org/court/cdadec.html
control options free of charge to their members. AOL has established an online area designed specifically for children. The "Kids Only" parental control feature allows parents to establish an AOL account for their children that accesses only the Kids Only channel on America Online.

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 board 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 rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert Dr. Olsen agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list.

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

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

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

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

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

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

The Practicalities of the Proffered Defenses

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

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

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

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

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

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

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

Adult Verification by Password

http://www.aclu.org/court/cdadcem.html
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 Kirosi
Kuromiya testified that it would be impossible for his organization, Critical Path, to
review all of its material because it has only one full and one part-time employee.

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

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

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

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

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

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

The Problems of Offshore Content and
Caching

117. A large percentage, perhaps 40% or more, of content on the Internet originates outside the United States. At the hearing, a witness demonstrated how an Internet user could access a Web site of London (which presumably is on a server in England), and then link to other sites of interest in England. A user can sometimes discern from a URL that content is coming from overseas, since InterNIC allows a content provider to imbed a country code in a domain name. 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.

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
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 P.2d 69, 72 (3d Cir.), cert. denied, 493 U.S. 848 (1989); Acierno v. New Castle County, 40 P.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.

SLOVITER, Chief Judge, Court of Appeals for the Third Circuit:

A.
Statutory Provisions

As noted in Part I, Introduction, the plaintiffs' motion for a preliminary injunction is confined to portions of two provisions of the Communications Decency Act of 1996, § 223(a) and § 223(d), which they contend violate their First Amendment free speech and Fifth Amendment due process rights. To facilitate reference, I set forth those provisions in full. Section 223(a), the "indecency" provision, subjects to criminal penalties of
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
UNITED STATES DISTRICT COURT FOR THE DISTRICT OF OREGON
January 4, 1999, Decided
January 4, 1999, Filed

OPINION:

OPINION AND ORDER

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


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. n1 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, 90 L. Ed. 95, 66 S. Ct. 154 (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, 104 S. Ct. 1868, 80 L. Ed. 2d 404 (1984). Plaintiff bears the burden of establishing personal jurisdiction through a prima facie showing of jurisdictional facts. American Telephone & Telegraph Co. v. Compagnie Bruxelles Lambert, 94 F.3d 586, 588 (9th Cir. 1996); Farmers Ins. Exchange v. Portage La Prairie Mut. Ins. Co., 907 F.2d 911, 912 (9th Cir. 1990).
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., 1996 U.S. Dist. LEXIS 15139, 40 U.S.P.Q.2D (BNA) 1826, 1996 WL 753991 (S.D. Cal. 1996)*. The court reasoned that "allowing computer interaction via the web to supply sufficient contracts to establish jurisdiction would eviscerate the personal jurisdiction requirement as it currently exists." *1997 WL 753991 at *3; c.f. Mieczkowski v. Masco 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 (9th Cir. 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, 85 L. Ed. 2d 528, 105 S. Ct. 2174 (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 availing 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, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (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 availing 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." *Shakeys, 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, P 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.

A "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 Ore. 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 Ore. 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 for 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. n2

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 indubitable, 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 used 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, 62 L. Ed. 2d 490, 100 S. Ct. 559 (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), aff'd 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 Bensusan'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.*

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 v. An Apple a Day_, 977 F. Supp. 404 (E.D. Va. 1997) (defamatory press releases on passive Web site); _EDIAS Software v. Basis International_, 947 F. Supp. 413 (D. Ariz. 1996) (defamatory messages directed at forum). These cases are based on the "effects test" articulated in _Calder v. Jones_, 465 U.S. 783, 788-90, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (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 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 include 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. Ameritech 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. n4

Finally, in Vitullo v. Velocity Powerboats, Inc., 1998 U.S. Dist. LEXIS 7120, 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. at 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 along 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 U.S. Dist. LEXIS 8531, 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*,

http://www.kentlaw.edu/classes/rwarner/legalaspects/millennium.html
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 "purposely directed" at plaintiff, whom defendant knew to reside in Massachusetts. Id. at 470. The court emphasized that "there 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 and an invitation for companies to communications via electronic mail to Cybersell FL, as well as 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:

No 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 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 establishes 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, the 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 of Internet contacts as described in Zippo needs further refinement to include the fundamental requirement of personal jurisdiction: "deliberate action" within the forum state in the form of transactions between the defendant and residents of the forum or conduct of the defendant purposefully directed at residents of the forum state. See Calder, 465 U.S. at 788-90; Ballard, 65 F.3d at 1498. 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." Id. 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. Compuserve 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, 62 L. Ed. 2d 490, 100 S. Ct. 559 (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 113-14; Park Inns, 5 F. Supp. 2d at 763 (interpreting and applying Cyberell); 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; see also *Panavision v. Toeppen*, 141 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 cases 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.
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. 2d 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.3d 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 97097 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 4 day of January, 1999.

Ann Aiken

United States District Judge
One Hundred Sixth Congress of the United States of America

AT THE SECOND SESSION

_Began and held at the City of Washington on Monday, the twenty-fourth day of January, two thousand_

An Act

To facilitate the use of electronic records and signatures in interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Signatures in Global and National Commerce Act".

TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE

SEC. 101. GENERAL RULE OF VALIDITY.

(a) In General.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

(b) Preservation of Rights and Obligations.—This title does not—

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

(c) Consumer Disclosures.—

(1) Consent to Electronic Records.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever
is required) such information satisfies the requirement that such information be in writing if—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) OTHER RIGHTS.—

(A) PRESERVATION OF CONSUMER PROTECTIONS.—Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made
available to any consumer under any statute, regulation, or other rule of law.

(B) VERIFICATION OR ACKNOWLEDGMENT.—If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt ( whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT.—The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT.—Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT.—This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS.—An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) RETENTION OF CONTRACTS AND RECORDS.—

(1) ACCURACY AND ACCESSIBILITY.—If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that—

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) EXCEPTION.—A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) ORIGINALS.—If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided,
available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

(4) CHECKS.—If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with paragraph (1).

(e) ACCURACY AND ABILITY TO RETAIN CONTRACTS AND OTHER RECORDS.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(f) PROXIMITY.—Nothing in this title affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed.

(g) NOTARIZATION AND ACKNOWLEDGMENT.—If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) ELECTRONIC AGENTS.—A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) INSURANCE.—It is the specific intent of the Congress that this title and title II apply to the business of insurance.

(j) INSURANCE AGENTS AND BROKERS.—An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if—

1. the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct;
2. the agent or broker was not involved in the development or establishment of such electronic procedures; and
3. the agent or broker did not deviate from such procedures.

SEC. 102. EXEMPTION TO PREEMPTION.

(a) IN GENERAL.—A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law—
S. 761—5

(1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or

(2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—

(i) such alternative procedures or requirements are consistent with this title and title II; and

(ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures; and

(B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.

(b) EXCEPTIONS FOR ACTIONS BY STATES AS MARKET PARTICIPANTS.—Subsection (a)(2)(A)(ii) shall not apply to the statutes, regulations, or other rules of law governing procurement by any State, or any agency or instrumentality thereof.

(c) PREVENTION OF CIRCUMVENTION.—Subsection (a) does not permit a State to circumvent this title or title II through the imposition of nonelectronic delivery methods under section 8(b)(2) of the Uniform Electronic Transactions Act.

SEC. 103. SPECIFIC EXCEPTIONS.

(a) EXCEPTED REQUIREMENTS.—The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—

(1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any State, other than sections 1–107 and 1–206 and Articles 2 and 2A.

(b) ADDITIONAL EXCEPTIONS.—The provisions of section 101 shall not apply to—

(1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;

(2) any notice of—

(A) the cancellation or termination of utility services (including water, heat, and power);

(B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
(C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or

(D) recall of a product, or material failure of a product, that risks endangering health or safety; or

(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

(c) REVIEW OF EXCEPTIONS.—

(1) EVALUATION REQUIRED.—The Secretary of Commerce, acting through the Assistant Secretary for Communications and Information, shall review the operation of the exceptions in subsections (a) and (b) to evaluate, over a period of 3 years, whether such exceptions continue to be necessary for the protection of consumers. Within 3 years after the date of enactment of this Act, the Assistant Secretary shall submit a report to the Congress on the results of such evaluation.

(2) DETERMINATIONS.—If a Federal regulatory agency, with respect to matter within its jurisdiction, determines after notice and an opportunity for public comment, and publishes a finding, that one or more such exceptions are no longer necessary for the protection of consumers and eliminating such exceptions will not increase the material risk of harm to consumers, such agency may extend the application of section 101 to the exceptions identified in such finding.

SEC. 104.—APPLICABILITY TO FEDERAL AND STATE GOVERNMENTS.

(a) FILING AND ACCESS REQUIREMENTS.—Subject to subsection (c)(2), nothing in this title limits or supersedes any requirement by a Federal regulatory agency, self-regulatory organization, or State regulatory agency that records be filed with such agency or organization in accordance with specified standards or formats.

(b) PRESERVATION OF EXISTING RULEMAKING AUTHORITY.—

(1) USE OF AUTHORITY TO INTERPRET.—Subject to paragraph (2) and subsection (c), a Federal regulatory agency or State regulatory agency that is responsible for rulemaking under any other statute may interpret section 101 with respect to such statute through—

(A) the issuance of regulations pursuant to a statute; or

(B) to the extent such agency is authorized by statute to issue orders or guidance, the issuance of orders or guidance of general applicability that are publicly available and published (in the Federal Register in the case of an order or guidance issued by a Federal regulatory agency). This paragraph does not grant any Federal regulatory agency or State regulatory agency authority to issue regulations, orders, or guidance pursuant to any statute that does not authorize such issuance.

(2) LIMITATIONS ON INTERPRETATION AUTHORITY.—Notwithstanding paragraph (1), a Federal regulatory agency shall not adopt any regulation, order, or guidance described in paragraph (1), and a State regulatory agency is preempted by section 101 from adopting any regulation, order, or guidance described in paragraph (1), unless—

(A) such regulation, order, or guidance is consistent with section 101;
SEC. 106. DEFINITIONS.

For purposes of this title:

(1) CONSUMER.—The term "consumer" means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.

(2) ELECTRONIC.—The term "electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(3) ELECTRONIC AGENT.—The term "electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.

(4) ELECTRONIC RECORD.—The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

(5) ELECTRONIC SIGNATURE.—The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

(6) FEDERAL REGULATORY AGENCY.—The term "Federal regulatory agency" means an agency, as that term is defined in section 552(f) of title 5, United States Code.

(7) INFORMATION.—The term "information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(8) PERSON.—The term "person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(9) RECORD.—The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(10) REQUIREMENT.—The term "requirement" includes a prohibition.

(11) SELF-REGULATORY ORGANIZATION.—The term "self-regulatory organization" means an organization or entity that is not a Federal regulatory agency or a State, but that is under the supervision of a Federal regulatory agency and is authorized under Federal law to adopt and administer rules applicable to its members that are enforced by such organization or entity, by a Federal regulatory agency, or by another self-regulatory organization.

(12) STATE.—The term "State" includes the District of Columbia and the territories and possessions of the United States.

(13) TRANSACTION.—The term "transaction" means an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct—

(A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and
(B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

SEC. 107. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title shall be effective on October 1, 2000.

(b) EXCEPTIONS.—

(1) RECORD RETENTION.—

(A) IN GENERAL.—Subject to subparagraph (B), this title shall be effective on March 1, 2001, with respect to a requirement that a record be retained imposed by—

(i) a Federal statute, regulation, or other rule of law, or

(ii) a State statute, regulation, or other rule of law administered or promulgated by a State regulatory agency.

(B) DELAYED EFFECT FOR PENDING RULEMAKINGS.—If on March 1, 2001, a Federal regulatory agency or State regulatory agency has announced, proposed, or initiated, but not completed, a rulemaking proceeding to prescribe a regulation under section 104(b)(3) with respect to a requirement described in subparagraph (A), this title shall be effective on June 1, 2001, with respect to such requirement.

(2) CERTAIN GUARANTEED AND INSURED LOANS.—With regard to any transaction involving a loan guarantee or loan guarantee commitment (as those terms are defined in section 502 of the Federal Credit Reform Act of 1990), or involving a program listed in the Federal Credit Supplement, Budget of the United States, FY 2001, this title applies only to such transactions entered into, and to any loan or mortgage made, insured, or guaranteed by the United States Government thereafter, on and after one year after the date of enactment of this Act.

(3) STUDENT LOANS.—With respect to any records that are provided or made available to a consumer pursuant to an application for a loan, or a loan made, pursuant to title IV of the Higher Education Act of 1965, section 101(c) of this Act shall not apply until the earlier of—

(A) such time as the Secretary of Education publishes revised promissory notes under section 432(m) of the Higher Education Act of 1965; or

(B) one year after the date of enactment of this Act.

TITLE II—TRANSFERABLE RECORDS

SEC. 201. TRANSFERABLE RECORDS.

(a) DEFINITIONS.—For purposes of this section:

(1) TRANSFERABLE RECORD.—The term "transferable record" means an electronic record that—

(A) would be a note under Article 3 of the Uniform Commercial Code if the electronic record were in writing;

(B) the issuer of the electronic record expressly has agreed is a transferable record; and

(C) relates to a loan secured by real property.
Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997)

Before CUMMINGS, WOOD, Jr., and EASTERBROOK, Circuit Judges.

EASTERBROOK, Circuit Judge.

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

One of the terms in the box containing a Gateway 2000 system was an arbitration clause. Rich and Enza Hill, the customers, kept the computer more than 30 days before complaining about its components and performance. They filed suit in federal court arguing, among other things, that the product's shortcomings make Gateway a racketeer (mail and wire fraud are said to be the predicate offenses), leading to treble damages under RICO for the Hills and a class of all other purchasers. Gateway asked the district court to enforce the arbitration clause; the judge refused, writing that "[t]he present record is insufficient to support a finding of a valid arbitration agreement between the parties or that the plaintiffs were given adequate notice of the arbitration clause." Gateway took an immediate appeal, as is its right. 9 U.S.C. § 16(a) (1)(A).

The Hills say that the arbitration clause did not stand out: they concede noticing the statement of terms but deny reading it closely enough to discover the agreement to arbitrate, and they ask us to conclude that they therefore may go to court. Yet an agreement to arbitrate must be enforced "save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2. Doctor's Associates, Inc. v. Casarotto, --- U.S. ----, 116 S.Ct. 1652, 134 L.Ed.2d 902 (1996), holds that this provision of the Federal Arbitration Act is inconsistent with any requirement that an arbitration clause be prominent. A contract need not be read to be effective; people who accept take the risk that the unread terms may in retrospect prove unwelcome. Carr v. CIGNA Securities, Inc., 95 F.3d 544, 547 (7th Cir.1996); Chicago Pacific Corp. v. Canada Life Assurance Co., 850 F.2d 334 (7th Cir.1988). Terms inside Gateway's box stand or fall together. If they constitute the parties' contract because the Hills had an opportunity to return the computer after reading them, then all must be enforced.

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

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

For their second sally, the Hills contend that ProCD should be limited to executory contracts (to licenses in particular), and therefore does not apply because both parties' performance of this contract was complete when the box arrived at their home. This is legally and factually wrong: legally because the question at hand concerns the formation of the contract rather than its performance, and factually because both contracts were incompletely performed. ProCD did not depend on the fact that the seller characterized the transaction as a license rather than as a contract; we treated it as a contract for the sale of goods and reserved the question whether for other purposes a "license" characterization might be preferable. 86 F.3d at 1450. All debates about characterization to one side, the transaction in ProCD was no more executory than the one here: Zeidenberg paid for the software and walked out of the store with a box under his arm, so if arrival of the box with the product ends the time for revelation of contractual terms, then the time ended in ProCD before Zeidenberg opened the box. But of course ProCD had not completed performance with delivery of the box, and neither had Gateway. One element of the transaction was the warranty, which oblige sellers to fix defects in their products. The Hills have invoked Gateway's warranty and are not satisfied with its response, so they are not well positioned to say that Gateway's obligations were fulfilled when the motor carrier unloaded the box. What is more, both ProCD and Gateway promised to help customers to use their products. Long-term service and information obligations are common in the computer business, on both hardware and software sides. Gateway offers "lifetime service" and has a round-the-clock telephone hotline to fulfill this promise. Some vendors spend more money helping customers use their products than on developing and manufacturing them. The document in Gateway's box includes promises of future performance that some consumers value highly; these promises bind Gateway just as the arbitration clause binds the Hills.

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

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

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

The Hills' remaining arguments, including a contention that the arbitration clause is unenforceable as part of a scheme to defraud, do not require more than a citation to Prima Paint Corp. v. Flood & Conklin Mfg. Co., 388 U.S. 395, 87 S.Ct. 1801, 18 L.Ed.2d 1270 (1967). Whatever may be said pro and con about the cost and efficacy of arbitration (which the Hills disparage) is for Congress and the contracting parties to consider. Claims based on RICO are no less arbitrable than those founded on the contract or the law of torts. Shearson/American Express, Inc. v. McMahon, 482 U.S. 220, 238-42, 107 S.Ct. 2332, 2343-46, 96 L.Ed.2d 185 (1987). The decision of the district court is vacated, and this case is remanded with instructions to compel the Hills to submit their dispute to arbitration.
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

WILLIAM S. KLOCEK,

Plaintiff,

v.

GATEWAY, INC., et al.,

Defendants.

CIVIL ACTION

No. 99-2499-KHV

MEMORANDUM AND ORDER

William S. Klocek brings suit against Gateway, Inc. and Hewlett-Packard, Inc. on claims arising from purchases of a Gateway computer and a Hewlett-Packard scanner. This matter comes before the Court on the Motion to Dismiss (Doc. # 6) which Gateway filed November 22, 1999 and Defendant Hewlett-Packard, Inc.'s Motion To Dismiss, Or In The Alternative For Stay Of Proceedings (Doc. # 16) filed December 22, 1999, the Motion (Doc. # 2) to certify a class which plaintiff filed October 29, 1999, the Motion For Sanctions, Expenses and Punitives [sic] (Doc. # 11) which plaintiff filed December 3, 1999, the Motion for a Writ of Certiorari (Doc. # 12) which plaintiff filed December 6, 1999, and the Motion for Verification (Doc. # 24) which plaintiff filed January 25, 2000. For reasons stated below, the Court overrules Gateway's motion to dismiss, sustains Hewlett-Packard's motion to dismiss, and overrules the motions filed by plaintiff.

A. Gateway's Motion to Dismiss

Plaintiff brings individual and class action claims against Gateway, alleging that it induced him and other consumers to purchase computers and special support packages by making false promises of technical support. Complaint, ¶¶ 3 and 4. Individually, plaintiff also claims breach of contract and breach of warranty, in that Gateway breached certain warranties that its computer would be compatible with standard peripherals and standard internet services. Complaint, ¶¶ 2, 5, and 6. Gateway asserts that plaintiff must arbitrate his claims under Gateway's Standard Terms and Conditions Agreement ("Standard Terms"). Whenever it sells a computer, Gateway includes a copy of the Standard Terms in the box which contains the computer battery power cables and instruction manuals. At the top of the first page, the Standard Terms include the following notice:

NOTE TO THE CUSTOMER:

This document contains Gateway 2000's Standard Terms and Conditions. By keeping your Gateway 2000 computer system beyond five (5) days after the date of delivery, you accept these Terms and
Conditions.

The notice is in emphasized type and is located inside a printed box which sets it apart from other provisions of the document. The Standard Terms are four pages long and contain 16 numbered paragraphs. Paragraph 10 provides the following arbitration clause:

DISPUTE RESOLUTION. Any dispute or controversy arising out of or relating to this Agreement or its interpretation shall be settled exclusively and finally by arbitration. The arbitration shall be conducted in accordance with the Rules of Conciliation and Arbitration of the International Chamber of Commerce. The arbitration shall be conducted in Chicago, Illinois, U.S.A. before a sole arbitrator. Any award rendered in any such arbitration proceeding shall be final and binding on each of the parties, and judgment may be entered thereon in a court of competent jurisdiction.¹


FAA Section 3 states:

If any suit or proceeding be brought in any of the courts of the United States upon any issue referable to arbitration under an agreement in writing for such arbitration, the court in which such suit is pending, upon being satisfied that the issue involved in such suit or proceeding is referable to arbitration under such agreement, shall on application of one of the parties stay the trial of the action until such arbitration has been had in accordance with the terms of the agreement, providing the applicant for the stay is not in default in proceeding with such arbitration.

9 U.S.C. § 3. Although the FAA does not expressly provide for dismissal, the Tenth Circuit has affirmed dismissal where the applicant did not request a stay. See Armijo v. Prudential Ins. Co. of Am., 72 F.3d 793, 797 (10th Cir. 1995). Here, neither Gateway nor plaintiff requests a stay. Accordingly, the Court concludes that dismissal is appropriate if plaintiff's claims are arbitrable.³ Accord Fedmet Corp. v. M/V BUYALYK, 194 F.3d 674, 678 (5th Cir. 1999) (dismissal appropriate if all issues raised before court are arbitrable); Sparling v. Hoffman Constr. Co., 864 F.2d 635, 638 (9th Cir. 1988); (district court had discretion to dismiss arbitrable claims); see also Black & Veatch Intl Co. v. Wartsila NSD North Am., Inc., 1998 WL 953966, Case No. 97-2556-GTV (D. Kan. Dec. 17, 1998) (dismissing case and compelling arbitration).

Gateway bears an initial summary-judgment-like burden of establishing that it is entitled to arbitration. See, e.g., Par-Knit Mills, Inc. v. Stockbridge Fabrics Co., 636 F.2d 51, 54 n.9 (3d Cir. 1980) (standard on motion to compel arbitration is same as summary judgment standard); Doctor's Assoc., Inc. v. Distajo, 944 F. Supp. 1010, 1014 (D. Conn. 1996), aff'd, 107 F.3d 126 (2d Cir. 1997) (same); Dougherty v. Mieczkowski, 661 F. Supp. 267, 270 n.1 (D. Del. 1987). Thus, Gateway must present evidence sufficient to demonstrate the existence of an enforceable agreement to arbitrate. See, e.g., Oppenheimer & Co. v. Neidhardt, 56 F.3d 352, 358 (2d Cir. 1995). If Gateway makes such a showing, the burden shifts to plaintiff to submit evidence demonstrating a genuine issue for trial. Id., see also Naddy v. Piper Jaffray, Inc., 1997 WL 749261, *2, Case Nos. 15431-9-III, 15681-8-III.


11/26/00
In this case, Gateway fails to present evidence establishing the most basic facts regarding the transaction. The gaps in the evidentiary record preclude the Court from determining what state law controls the formation of the contract in this case and, consequently, prevent the Court from agreeing that Gateway's motion is well taken.

Before granting a stay or dismissing a case pending arbitration, the Court must determine that the parties have a written agreement to arbitrate. See 9 U.S.C. §§ 3 and 4; Avedon Engineering, Inc. v. Seatex, 126 F.3d 1279, 1283 (10th Cir. 1997). When deciding whether the parties have agreed to arbitrate, the Court applies ordinary state law principles that govern the formation of contracts. First Options of Chicago, Inc. v. Kaplan, 514 U.S. 938, 944 (1995). The existence of an arbitration agreement "is simply a matter of contract between the parties; [arbitration] is a way to resolve those disputes - but only those disputes - that the parties have agreed to submit to arbitration." Avedon, 126 F.3d at 1283 (quoting Kaplan, 514 U.S. at 943-945). If the parties dispute making an arbitration agreement, a jury trial on the existence of an agreement is warranted if the record reveals genuine issues of material fact regarding the parties' agreement. See Avedon, 126 F.3d at 1283.

Before evaluating whether the parties agreed to arbitrate, the Court must determine what state law controls the formation of the contract in this case. See id. at 1284. In diversity actions, the Court applies the substantive law, including choice of law rules, that Kansas state courts would apply. See Moore v. Subaru of Am., 891 F.2d 1445, 1448 (10th Cir. 1989). Kansas courts apply the doctrine of lex loci contractus, which requires that the Court interpret the contract according to the law of the state in which the parties performed the last act necessary to form the contract. See Missouri Pac. R.R. Co. v. Kansas Gas and Elec. Co., 862 F.2d 796, 798 n.1 (10th Cir. 1988) (citing Simms v. Metropolitan Life Ins. Co., 9 Kan.App.2d 640, 642-43, 685 P.2d 321 (1984)).

The parties do not address the choice of law issue, and the record is unclear where they performed the last act necessary to complete the contract. Gateway presents affidavit testimony that it shipped a computer to plaintiff on or about August 31, 1997, Affidavit of David Blackwell, ¶ 5 (attached to Memorandum in Support of Motion to Dismiss (Doc. # 8)), but it provides no details regarding the transaction. Plaintiff's complaint alleges that plaintiff lives in Missouri and, if Gateway shipped his computer, it presumably shipped it to Missouri. See Complaint, p. 1 (Doc. # 1). In his response to Gateway's motion, however, plaintiff states that on August 27, 1997 he purchased the computer in person at the Gateway store in Overland Park, Kansas, and took it with him at that time. Response to Motion to Dismiss, ¶¶ 2(b) and 2(d) (Doc. # 9). Depending on which factual version is correct, it appears that the parties may have performed the last act necessary to form the contract in Kansas (with plaintiff purchasing the computer in Kansas), Missouri (with Gateway shipping the computer to plaintiff in Missouri), or some unidentified other states (with Gateway agreeing to ship plaintiff's catalog order and/or Gateway actually shipping the order). (4) The Court discerns no material difference between the applicable substantive law in Kansas and Missouri and - as to those two states - it perhaps would not need to resolve the choice of law issue at this time. See Avelon, 126 F.3d at 1284 (choice of law analysis unnecessary if relevant states have enacted identical controlling statutes); see also Missouri Pacific, 862 F.2d at 798 n.1 (applying Kansas law where record did not indicate where final act occurred and parties did not raise issue); Phillips Petrol. Co. v. Shutts, 472 U.S. 797, 816 (1985) ("There can be no injury in applying Kansas law if it is not in conflict with that of any other jurisdiction connected to this suit"). (5) The Uniform Commercial Code ("UCC") governs the parties' transaction under both Kansas and Missouri law. See K.S.A. § 84-2-102; V.A.M.S. § 400.2-102 (UCC applies to "transactions in goods"); Kansas Comment 1 (main thrust of Article 2 is limited to sales); K.S.A. § 84-2-105(1) V.A.M.S. § 400.2-105(1) ("'Goods' means all things ... which are movable at the time of identification to the contract for sale ... "). Regardless whether plaintiff...
purchased the computer in person or placed an order and received shipment of the computer, the parties agree that plaintiff paid for and received a computer from Gateway. This conduct clearly demonstrates a contract for the sale of a computer. See, e.g., Step-Saver Data Sys., Inc. v. Wyse Techn., 939 F.2d 91, 98 (3d Cir. 1991). Thus the issue is whether the contract of sale includes the Standard Terms as part of the agreement.

State courts in Kansas and Missouri apparently have not decided whether terms received with a product become part of the parties' agreement. Authority from other courts is split. Compare Step-Saver, 939 F.2d 91 (printed terms on computer software package not part of agreement); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993) (license agreement shipped with computer software not part of agreement); and U.S. Surgical Corp. v. Orris, Inc., 5 F. Supp. 2d 1201 (D. Kan. 1998) (single use restriction on product package not binding agreement); with Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir.), cert. denied, 522 U.S. 808 (1997) (arbitration provision shipped with computer binding on buyer); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996) (shrinkwrap license binding on buyer); and M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000) (following Hill and ProCD on license agreement supplied with software). It appears that at least in part, the cases turn on whether the court finds that the parties formed their contract before or after the vendor communicated its terms to the purchaser. Compare Step-Saver, 939 F.2d at 98 (parties' conduct in shipping, receiving and paying for product demonstrates existence of contract; box top license constitutes proposal for additional terms under § 2-207 which requires express agreement by purchaser); Arizona Retail, 831 F. Supp. at 765 (vendor entered into contract by agreeing to ship goods, or at latest by shipping goods to buyer; license agreement constitutes proposal to modify agreement under § 2-209 which requires express assent by buyer); and Orris, 5 F. Supp. 2d at 1206 (sales contract concluded when vendor received consumer orders; single-use language on product's label was proposed modification under § 2-209 which requires express assent by purchaser); with ProCD, 86 F.3d at 1452 (under § 2-204 vendor, as master of offer, may propose limitations on kind of conduct that constitutes acceptance; § 2-207 does not apply in case with only one form); Hill, 105 F.3d at 1148-49 (same); and Mortenson, 998 P.2d at 311-314 (where vendor and purchaser utilized license agreement in prior course of dealing, shrinkwrap license agreement constituted issue of contract formation under § 2-204, not contract alteration under § 2-207).

Gateway urges the Court to follow the Seventh Circuit decision in Hill. That case involved the shipment of a Gateway computer with terms similar to the Standard Terms in this case, except that Gateway gave the customer 30 days - instead of 5 days - to return the computer. In enforcing the arbitration clause, the Seventh Circuit relied on its decision in ProCD, where it enforced a software license which was contained inside a product box. See Hill, 105 F.3d at 1148-50. In ProCD, the Seventh Circuit noted that the exchange of money frequently precedes the communication of detailed terms in a commercial transaction. See ProCD, 86 F.3d at 1451. Citing UCC § 2-204, the court reasoned that by including the license with the software, the vendor proposed a contract that the buyer could accept by using the software after having an opportunity to read the license. ProCD, 86 F.3d at 1452. Specifically, the court stated:

A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance.

ProCD, 86 F.3d at 1452. The Hill court followed the ProCD analysis, noting that "[p]ractical considerations support allowing vendors to enclose the full legal terms with their products." Hill, 105
F.3d at 1149. (9)

The Court is not persuaded that Kansas or Missouri courts would follow the Seventh Circuit reasoning in Hill and ProCD. In each case the Seventh Circuit concluded without support that UCC § 2-207 was irrelevant because the cases involved only one written form. See ProCD, 86 F.3d at 1452 (citing no authority); Hill, 105 F.3d at 1150 (citing ProCD). This conclusion is not supported by the statute or by Kansas or Missouri law. Disputes under § 2-207 often arise in the context of a "battle of forms," see, e.g., Diatom, Inc. v. Pennwalt Corp., 741 F.2d 1569, 1574 (10th Cir. 1984), but nothing in its language precludes application in a case which involves only one form. The statute provides:

Additional terms in acceptance or confirmation.

(1) A definite and seasonable expression of acceptance or a written confirmation which is sent within a reasonable time operates as an acceptance even though it states terms additional to or different from those offered or agreed upon, unless acceptance is expressly made conditional on assent to the additional or different terms.

(2) The additional terms are to be construed as proposals for addition to the contract [if the contract is not between merchants] . . . .

K.S.A. § 84-2-207; V.A.M.S. § 400.2-207. By its terms, § 2-207 applies to an acceptance or written confirmation. It states nothing which requires another form before the provision becomes effective. In fact, the official comment to the section specifically provides that §§ 2-207(1) and (2) apply "where an agreement has been reached orally . . . and is followed by one or both of the parties sending formal memoranda embodying the terms so far agreed and adding terms not discussed." Official Comment 1 of UCC § 2-207. Kansas and Missouri courts have followed this analysis. See Southwest Engineering Co. v. Martin Tractor Co., 205 Kan. 684, 695, 473 P.2d 18, 26 (1970) (stating in dicta that § 2-207 applies where open offer is accepted by expression of acceptance in writing or where oral agreement is later confirmed in writing); Central Bag Co. v. W. Scott and Co., 647 S.W.2d 828, 830 (Mo. App. 1983) (§§ 2-207(1) and (2) govern cases where one or both parties send written confirmation after oral contract). Thus, the Court concludes that Kansas and Missouri courts would apply § 2-207 to the facts in this case. Accord Avedon, 126 F.2d at 1283 (parties agree that § 2-207 controls whether arbitration clause in sales confirmation is part of contract).

In addition, the Seventh Circuit provided no explanation for its conclusion that "the vendor is the master of the offer." See ProCD, 86 F.3d at 1452 (citing nothing in support of proposition); Hill, 105 F.3d at 1149 (citing ProCD). In typical consumer transactions, the purchaser is the offeror, and the vendor is the offeree. See Brown Mach., Div. of John Brown, Inc. v. Hercules, Inc., 770 S.W.2d 416, 419 (Mo. App. 1989) (as general rule orders are considered offers to purchase); Rich Prods. Corp. v. Kemutec Inc., 66 F. Supp.2d 937, 956 (E.D. Wis. 1999) (generally price quotation is invitation to make offer and purchase order is offer). While it is possible for the vendor to be the offeror, see Brown Machine, 770 S.W.2d at 419 (price quote can amount to offer if it reasonably appears from quote that assent to quote is all that is needed to ripen offer into contract), Gateway provides no factual evidence which would support such a finding in this case. The Court therefore assumes for purposes of the motion to dismiss that plaintiff offered to purchase the computer (either in person or through catalog order) and that Gateway accepted plaintiff's offer (either by completing the sales transaction in person or by agreeing to ship and/or shipping the computer to plaintiff). Accord Arizona Retail, 831 F. Supp. at 765 (vendor entered into contract by agreeing to ship goods, or at latest, by shipping goods).


11/26/00
Under § 2-207, the Standard Terms constitute either an expression of acceptance or written confirmation. As an expression of acceptance, the Standard Terms would constitute a counter-offer only if Gateway expressly made its acceptance conditional on plaintiff's assent to the additional or different terms. K.S.A. § 84-2-207(1); V.A.M.S. § 400.2-207(1). "[T]he conditional nature of the acceptance must be clearly expressed in a manner sufficient to notify the offeror that the offeree is unwilling to proceed with the transaction unless the additional or different terms are included in the contract." Brown Machine, 770 S.W.2d at 420. Gateway provides no evidence that at the time of the sales transaction, it informed plaintiff that the transaction was conditioned on plaintiff's acceptance of the Standard Terms. Moreover, the mere fact that Gateway shipped the goods with the terms attached did not communicate to plaintiff any unwillingness to proceed without plaintiff's agreement to the Standard Terms. See, e.g., Arizona Retail, 831 F. Supp. at 765 (conditional acceptance analysis rarely appropriate where contract formed by performance but goods arrive with conditions attached); Lighton Indus., Inc. v. Callier Steel Pipe & Tube, Inc., 1991 WL 18415, *6, Case No. 89-C-8235 (N.D. Ill. Feb. 6, 1991) (applying Missouri law) (preprinted forms insufficient to notify offeror of conditional nature of acceptance, particularly where form arrives after delivery of goods).

Because plaintiff is not a merchant, additional or different terms contained in the Standard Terms did not become part of the parties' agreement unless plaintiff expressly agreed to them. See K.S.A. § 84-2-207, Kansas Comment 2 (if neither party is not a merchant, additional terms are proposals for addition to the contract that do not become part of the contract unless the original offeror expressly agrees). Gateway argues that plaintiff demonstrated acceptance of the arbitration provision by keeping the computer more than five days after the date of delivery. Although the Standard Terms purport to work that result, Gateway has not presented evidence that plaintiff expressly agreed to those Standard Terms. Gateway states only that it enclosed the Standard Terms inside the computer box for plaintiff to read afterwards. It provides no evidence that it informed plaintiff of the five-day review-and-return period as a condition of the sale transaction, or that the parties contemplated additional terms to the agreement. See Step-Saver, 939 F.2d at 99 (during negotiations leading to purchase, vendor never mentioned box-top license or obtained buyer's express assent thereto). The Court finds that the act of keeping the computer past five days was not sufficient to demonstrate that plaintiff expressly agreed to the Standard Terms. Accord Brown Machine, 770 S.W.2d at 421 (express assent cannot be presumed by silence or mere failure to object). Thus, because Gateway has not provided evidence sufficient to support a finding under Kansas or Missouri law that plaintiff agreed to the arbitration provision contained in Gateway's Standard Terms, the Court overrules Gateway's motion to dismiss.

The motion also must be overruled because Kansas and Missouri law may not apply. As noted above, the Court must interpret the contract according to the law of the state in which the parties performed the last act necessary to form the contract. Gateway's motion does not address the choice of law issue, and the record is woefully unclear where the parties performed the last act necessary to complete the contract. Gateway therefore has not established that its motion is meritorious. If Gateway contends that the issue of contract formation is governed by some law other than that of Kansas or Missouri, it shall file a supplemental motion which cites the factual and legal basis for its position. The Court will review that submission and decide whether to order a jury trial on the existence of an agreement to arbitrate. See Avedon, 126 F.3d at 1283.

~B. Hewlett-Packard's Motion to Dismiss~
IT IS THEREFORE ORDERED that the Motion to Dismiss (Doc. # 6) which defendant Gateway filed November 22, 1999 be and hereby is OVERRULED. If Gateway contends that the issue of contract formation is governed by some law other than that of Kansas or Missouri, on or before June 30, 2000, it shall file a supplemental motion to dismiss and compel arbitration and cite the factual and legal basis for its position. Plaintiff no later than July 24, 2000 shall file any response. Gateway's reply, if any, shall be filed no later than August 7, 2000. The Court will review those submissions and decide whether to order a jury trial on the existence of an agreement to arbitrate. In presenting these materials, however, the parties are ordered to brief the matter in a summary judgment motion format and scrupulously follow Rule 56, Fed. R. Civ. P., D. Kan. Rule 56.1.

IT IS FURTHER ORDERED that Defendant Hewlett-Packard, Inc.'s Motion To Dismiss, Or In The Alternative For Stay Of Proceedings (Doc. # 16) filed December 22, 1999 be and hereby is SUSTAINED in part, in that plaintiff's complaint against Hewlett-Packard is dismissed for lack of subject matter jurisdiction.

IT IS FURTHER ORDERED that the Motion (Doc. # 2) to certify a class which plaintiff filed October 29, 1999 be and hereby is OVERRULED; the Motion For Sanctions, Expenses and Punitives [sic] (Doc. # 11) which plaintiff filed December 3, 1999 be and hereby is OVERRULED; the Motion for a Writ of Certiorari (Doc. # 12) which plaintiff filed December 6, 1999 be and hereby is OVERRULED, and the Motion for Verification (Doc. # 24) which plaintiff filed January 25, 2000 be and hereby is OVERRULED.

Dated this 15th day of June, 2000, at Kansas City, Kansas.

Kathryn H. Vratil

United States District Judge

1. Gateway states that after it sold plaintiff's computer, it mailed all existing customers in the United States a copy of its quarterly magazine, which contained notice of a change in the arbitration policy set forth in the Standard Terms. The new arbitration policy afforded customers the option of arbitrating before the International Chamber of Commerce ("ICC"), the American Arbitration Association ("AAA"), or the National Arbitration Forum ("NAF") in Chicago, Illinois, or any other location agreed upon by the parties. Plaintiff denies receiving notice of the amended arbitration policy. Neither party explains why - if the arbitration agreement was an enforceable contract - Gateway was entitled to unilaterally amend it by sending a magazine to computer customers.

2. The FAA does not create independent federal-question jurisdiction; rather, "there must be diversity of citizenship or some other independent basis for federal jurisdiction" before the Court may act. Moses H. Cone Memorial Hosp. v. Mercury Const. Corp., 460 U.S. 1, 25 n.32 (1983). In this case, plaintiff asserts diversity jurisdiction.

3. It is not clear whether Gateway asks the Court to compel arbitration in addition to dismissal. Compare Motion to Dismiss (Doc. # 6), p. 2 (Gateway "requests this Court to dismiss the complaint . . . so that [plaintiff] can pursue his arbitration remedy"); Memorandum in Support of Motion to
4. While Gateway may have shipped the computer to plaintiff in Missouri, the record contains no evidence regarding how plaintiff communicated his order to Gateway, where Gateway received plaintiff's order or where the shipment originated.

5. Paragraph 9 of the Standard Terms provides that "[t]his Agreement shall be governed by the laws of the State of South Dakota, without giving effect to the conflict of laws rules thereof." Both Kansas and Missouri recognize choice-of-law provisions, so long as the transaction at issue has a "reasonable relation" to the state whose law is selected. K.S.A. § 84-1-105(1); Mo. Rev. Stat. § 400.1-105(1). At this time, because it must first determine whether the parties ever agreed to the Standard Terms, the Court does not decide whether Kansas or Missouri (or some other unidentified state) would recognize the choice of law provision contained in the Standard Terms.

6. The term "shrinkwrap license" gets its name from retail software packages that are covered in plastic or cellophane "shrinkwrap" and contain licenses that purport to become effective as soon as the customer tears the wrapping from the package. See ProCD, 86 F.3d at 1449.

7. The Mortenson court also found support for its holding in the proposed Uniform Computer Information Transactions Act ("UCITA") (formerly known as proposed UCC Article 2B) (text located at www.law.upenn.edu/library/ulc/ucita/UCITA_99.htm), which the National Conference of Commissioners on Uniform State Laws approved and recommended for enactment by the states in July 1999. See Mortenson, 998 P.2d at 310 n.6, 313 n.10. The proposed UCITA, however, would not apply to the Court's analysis in this case. The UCITA applies to computer information transactions, which are defined as agreements "to create, modify, transfer, or license computer information or informational rights in computer information." UCITA, §§ 102(11) and 103. In transactions involving the sale of computers, such as our case, the UCITA applies only to the computer programs and copies, not to the sale of the computer itself. See UCITA § 103(c)(2).

8. Section 2-204 provides: "A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such contract." K.S.A. § 84-2-204; V.A.M.S. § 400.2-204.

9. Legal commentators have criticized the reasoning of the Seventh Circuit in this regard. See, e.g., Jean R. Sternlight, Gateway Widens Doorway to Imposing Unfair Binding Arbitration on Consumers, Fla. Bar J., Nov. 1997, at 8, 10-12 (outcome in Gateway is questionable on federal statutory, common law and constitutional grounds and as a matter of contract law and is unwise as a matter of policy because it unreasonably shifts to consumers search cost of ascertaining existence of arbitration clause and return cost to avoid such clause); Thomas J. McCarthy et al., Survey: Uniform Commercial Code, 53 Bus. Law. 1461, 1465-66 (Seventh Circuit finding that UCC § 2-207 did not apply is inconsistent with official comment); Batya Goodman, Honey, I Shrink-Wrapped the Consumer: the Shrinkwrap Agreement as an Adhesion Contract, 21 Cardozo L. Rev. 319, 344-352 (Seventh Circuit failed to consider principles of adhesion contracts); Jeremy Senderowitz, Consumer Arbitration and Freedom of Contract: A Proposal to Facilitate Consumers' Informed Consent to Arbitration Clauses in Form Contracts, 32 Colum. J.L. & Soc. Probs. 275, 296-299 (judiciary (in multiple decisions, including Hill) has ignored issue of consumer consent to an arbitration clause). Nonetheless, several courts have followed the Seventh Circuit decisions in Hill and ProCD. See, e.g., Mortenson, 2000...

10. In Southwest Engineering, the court was concerned with the existence of an enforceable contract under the UCC statute of frauds and it determined that the parties' notes satisfied the writing requirement. It found that a subsequent letter which contained additional material terms did not become part of the agreement under § 2-207, however, because the parties did not expressly agree to the change in terms. See Southwest Engineering, 205 Kan. at 693-94, 473 P.2d at 25. The court further found that § 2-207 did not apply to its analysis because at the time of the letter, the parties had already memorialized the agreement in writing and there was no outstanding offer to accept or oral agreement to confirm. See Southwest Engineering, 205 Kan. at 695, 473 P.2d at 26.

11. UCC § 2-206(b) provides that "an order or other offer to buy goods for prompt or current shipment shall be construed as inviting acceptance either by a prompt promise to ship or by the prompt or current shipment . . . ." The official comment states that "[e]ither shipment or a prompt promise to ship is made a proper means of acceptance of an offer looking to current shipment." UCC § 2-206, Official Comment 2.

12. Courts are split on the standard for a conditional acceptance under § 2-207. See Daitom, 741 F.2d at 1576 (finding that Pennsylvania would most likely adopt "better" view that offeree must explicitly communicate unwillingness to proceed with transaction unless additional terms in response are accepted by offeror). On one extreme of the spectrum, courts hold that the offeree's response stating a materially different term solely to the disadvantage of the offeror constitutes a conditional acceptance. See Daitom, 741 F.2d at 1569 (citing Roto-Lith, Ltd. v. F. P. Bartlett & Co., 297 F.2d 497 (1st Cir. 1962)). At the other end of the spectrum, courts hold that the conditional nature of the acceptance should be so clearly expressed in a manner sufficient to notify the offeror that the offeree is unwilling to proceed without the additional or different terms. See Daitom, 741 F.2d at 1569 (citing Dorton v. Collins & Aikman Corp., 453 F.2d 1161 (6th Cir. 1972)). The middle approach requires that the response predicate acceptance on clarification, addition or modification. See Daitom, 741 F.2d at 1569 (citing Construction Aggregates Corp. v. Hewitt-Robins, Inc., 404 F.2d 505 (7th Cir. 1968)). The First Circuit has since overruled its decision in Roto-Lith, see Ironics, Inc. v. Elmwood Sensors, Inc., 110 F.3d 184, and the Court finds that neither Kansas nor Missouri would apply the standard set forth therein. See Boese-Hilburn Co. v. Dean Machinery Co., 616 S.W.2d 520, (Mo. App. 1981) (rejecting Roto-Lith standard); Owens-Corning Fiberglas Corp. v. Sonic Dev. Corp., 546 F. Supp. 533, 538 (D. Kan. 1982) (acceptance is not counteroffer under Kansas law unless it is made conditional on assent to additional or different terms (citing Roto-Lith as comparison)); Daitom, 741 F.2d at 1569 (finding that Dorton is "better" view). Because Gateway does not satisfy the standard for conditional acceptance under either of the remaining standards (Dorton or Construction Aggregates), the Court does not decide which of the remaining two standards would apply in Kansas and/or Missouri.

13. The Court's decision would be the same if it considered the Standard Terms as a proposed modification under UCC § 2-209. See, e.g., Orris, 5 F. Supp.2d at 1206 (express assent analysis is same under §§ 2-207 and 2-209).
14. The Court is mindful of the practical considerations which are involved in commercial transactions, but it is not unreasonable for a vendor to clearly communicate to a buyer - at the time of sale - either the complete terms of the sale or the fact that the vendor will propose additional terms as a condition of sale; if that be the case.

15. While the Court holds pro se pleadings to less stringent standards than pleadings drafted by lawyers, pro se litigants must follow the same procedural rules as any other litigant. See Hughes v. Rowe, 449 U.S. 5, 9 (1980); Green v. Dorrell, 969 F.2d 915, 917 (10th Cir. 1992). The Court may not assume the role of advocate for a pro se litigant. Hall v. Bellmon, 935 F.2d 1106, 1110 (10th Cir. 1991).

16. Plaintiff does not address the amount of damages claimed in Plaintiff's Response to Defendant Hewlett-Packard's Motion to Dismiss or Stay (Doc. # 20) filed January 5, 2000 or Plaintiff's Adendum [sic] to his Memoranda in Support (Doc. # 21) filed January 6, 2000.

17. Plaintiff further claims that the "class of consumers who've purchased Gateway Computers and Hewlett-Packard scanners are owed damages plus punitives [sic] as can be shown." Complaint, p. 7. Plaintiff may not aggregate the claims of the class members, however, to meet the amount in controversy requirement. See Zahn v. Int'l Paper Co., 414 U.S. 291, 294-95 (1973); Leonhardt v. Western Sugar Co., 160 F.3d 631, 637-38 (10th Cir. 1998) (each plaintiff in class action diversity action must meet jurisdictional amount in controversy; aggregation allowed only if plaintiffs unite to enforce a single title or right in which they have a common and undivided interest).

18. Because the Court concludes that it lacks subject matter jurisdiction, it does not reach Hewlett-Packard's claim that plaintiff has failed to state a claim upon which relief may be granted.

19. Neither defendant has filed a response to the motion to certify. On January 4, 2000, the Court entered an order staying Hewlett-Packard's time to file a response to 30 days after defendant receives a transcript of plaintiff's deposition. The record does not reveal the status of plaintiff's deposition or the transcript thereof.

20. A "certiorari" is "[a]n extraordinary writ issued by an appellate court, at its discretion, directing a lower court to deliver the record in the case for review." Black's Law Dictionary (1996). This Court does not have appellate jurisdiction over the District Court of Johnson County, Kansas.
Sec. 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:
  o (1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
  o (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;
  o (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
  o (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
  o (5) the material is transmitted through the system or network without modification of its content.

- (b) System Caching. -
  o (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.
  o (2) Conditions. - The conditions referred to in paragraph (1)
are that -

■ (A) the material described in paragraph (1) is transmitted to
the 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 (i), 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.

■ (l) 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.
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

NO. C-99-21200 RMW

ORDER GRANTING PRELIMINARY
INJUNCTION

[Docket Nos. 6, 12]

EBAY, INC.,

Plaintiff,

vs.

BIDDER'S EDGE, INC.,

Defendant.

Plaintiff eBay, Inc.'s ("eBay") motion for preliminary injunction was heard by the court on April 14, 2000. The court has read the moving and responding papers and heard the argument of counsel. For the reasons set forth below, the court preliminarily enjoins defendant Bidder's Edge, Inc. ("BE") from accessing eBay's computer systems by use of any automated querying program without eBay's written authorization.

I. BACKGROUND

eBay is an Internet-based, person-to-person trading site. (Jordan Decl. ¶ 3.) eBay offers sellers the ability to list items for sale and prospective buyers the ability to search those listings and bid on items. (Id.) The seller can set the terms and conditions of the auction. (Id.) The item is sold to the highest bidder. (Id.) The transaction is consummated directly between the buyer and seller without eBay's involvement. (Id.) A potential purchaser looking for a particular item can access the eBay site and perform a key word search for relevant auctions and bidding status. (Id.) eBay has also created category listings which identify items in over 2500 categories, such as antiques, computers, and dolls. (Id.)

Users may browse these category listing pages to identify items of interest. (Id.) Users of the eBay site must register and agree to the eBay User Agreement. (Id. ¶ 4.) Users agree to the seven page User Agreement by clicking on an "I Accept" button located at the end of the User Agreement. (Id. Ex. D.) The current version of the User Agreement prohibits the use of "any robot, spider, other automatic device, or manual process to monitor or copy our web pages or the content contained herein without our prior expressed written permission." (Id.) It is not clear that the version of the User Agreement in effect at the time BE began searching the eBay site prohibited such activity, or that BE ever agreed to comply with the User Agreement.

eBay currently has over 7 million registered users. (Jordan Decl. ¶ 4.) Over 400,000 new items are added to the site every day. (Id.) Every minute, 600 bids are placed on almost 3 million items. (Id.) Users currently perform, on average, 10 million searches per day on eBay's database. Bidding for and sales of items are continuously ongoing in millions of separate auctions. (Id.) A software robot is a
computer program which operates across the Internet to perform searching, copying and retrieving functions on the web sites of others.2 (Maynor Decl. ¶ 3; Johnson-Laird Decl. ¶ 15.)

A software robot is capable of executing thousands of instructions per minute, far in excess of what a human can accomplish. (Maynor Decl. ¶ 3) Robots consume the processing and storage resources of a system, making that portion of the system's capacity unavailable to the system owner or other users. (Id.) Consumption of sufficient system resources will slow the processing of the overall system and can overload the system such that it will malfunction or "crash." (Id.) A severe malfunction can cause a loss of data and an interruption in services. (Id.)

The eBay site employs "robot exclusion headers." (Id. ¶ 5.) A robot exclusion header is a message, sent to computers programmed to detect and respond to such headers, that eBay does not permit unauthorized robotic activity. (Id.) Programmers who wish to comply with the Robot Exclusion Standard design their robots to read a particular data file, "robots.txt," and to comply with the control directives it contains. (Johnson-Laird Decl. ¶ 20.)

To enable computers to communicate with each other over the Internet, each is assigned a unique Internet Protocol ("IP") address. (Maynor Decl. ¶ 6.) When a computer requests information from another computer over the Internet, the requesting computer must offer its IP address to the responding computer in order to allow a response to be sent. (Id.) These IP addresses allow the identification of the source of incoming requests. (Id.) eBay identifies robotic activity on its site by monitoring the number of incoming requests from each particular IP address. (Id. ¶ 7.) Once eBay identifies an IP address believed to be involved in robotic activity, an investigation into the identity, origin and owner of the IP address may be made in order to determine if the activity is legitimate or authorized. (Id. ¶ 8.) If an investigation reveals unauthorized robotic activity, eBay may attempt to ignore ("block") any further requests from that IP address. (Id.) Attempts to block requests from particular IP addresses are not always successful. (Id. ¶ 9; Johnson-Laird Decl. ¶ 27.)

Organizations often install "proxy server" software on their computers. (Johnson-Laird Decl. ¶ 12.) Proxy server software acts as a focal point for outgoing Internet requests. (Id.) Proxy servers conserve system resources by directing all outgoing and incoming data traffic through a centralized portal. (Id.) Typically, organizations limit the use of their proxy servers to local users. (Id.) However, some organizations, either as a public service or because of a failure to properly protect their proxy server through the use of a "firewall," allow their proxy servers to be accessed by remote users. (Id. ¶ 13.) Outgoing requests from remote users can be routed through such unprotected proxy servers and appear to originate from the proxy server. (Id.) Incoming responses are then received by the proxy server and routed to the remote user. (Id.) Information requests sent through such proxy servers cannot easily be traced back to the originating IP address and can be used to circumvent attempts to block queries from the originating IP address. (Id. ¶ 14.) Blocking queries from innocent third party proxy servers is both inefficient, because it creates an endless game of hide-and-seek, and potentially counterproductive, as it runs a substantial risk of blocking requests from legitimate, desirable users who use that proxy server. (Id. ¶ 22.)

BE is a company with 22 employees that was founded in 1997. (Carney Decl. ¶ 2.) The BE web site debuted in November 1998. (Id. ¶ 3.) BE does not host auctions. (Id. ¶ 2.) BE is an auction aggregation site designed to offer on-line auction buyers the ability to search for items across numerous on-line auctions without having to search each host site individually. (Id.) As of March 2000, the BE web site contained information on more than five million auction items being auctioned on more than one hundred auction sites. (Id. ¶ 3.) BE also provides its users with additional auction-related
services and information. (Id. ¶ 2.) The information available on the BE site is contained in a database of information that BE compiles through access to various auction sites such as eBay. (Id. ¶ 4.) When a user enters a search for a particular item at BE, BE searches its database and generates a list of every item in the database responsive to the search, organized by auction closing date and time. (Id. ¶ 5.) Rather than going to each host auction site one at a time, a user who goes to BE may conduct a single search to obtain information about that item on every auction site tracked by BE. (Id. ¶ 6.) It is important to include information regarding eBay auctions on the BE site because eBay is by far the biggest consumer to consumer on-line auction site. (Id.)

On June 16, 1997, over a year before the BE web site debuted, Peter Leeds\(^3\) wrote an email in response to an email from Kimbo Mundy, co-founder of BE. (Ritchey Decl. Ex 6.) Mundy's email said, "I think the magazines may be overrating sites' ability to block. The early agent experiments, like Arthur Anderson's BargainFinder were careful to check the robots.txt file on every site and desist if asked." (Id.) (underline in original). Mundy wrote back: "I believe well-behaved robots are still expected to check the robots.txt file... Our other concern was also legal. It is one thing for customers to use a tool to check a site and quite another for a single commercial enterprise to do so on a repeated basis and then to distribute that information for profit." (Id.) In early 1998, eBay gave BE permission to include information regarding eBay-hosted auctions for Beanie Babies and Furbies in the BE database. (Id. ¶ 7.)

In early 1999, BE added to the number of person-to-person auction sites it covered and started covering a broader range of items hosted by those sites, including eBay. (Id. ¶ 8.) On April 24, 1999, eBay verbally approved BE crawling the eBay web site for a period of 90 days. (Id.) The parties contemplated that during this period they would reach a formal licensing agreement. (Id.) They were unable to do so.

It appears that the primary dispute was over the method BE uses to search the eBay database. eBay wanted BE to conduct a search of the eBay system only when the BE system was queried by a BE user. (Ploen Decl. Ex. 9.) This reduces the load on the eBay system and increases the accuracy of the BE data. (Id.) BE wanted to recursively crawl the eBay system to compile its own auction database. (Carney Decl. ¶ 18.) This increases the speed of BE searches and allows BE to track the auctions generally and automatically update its users when activity occurs in particular auctions, categories of auctions, or when new items are added. (Id.)

In late August or early September 1999, eBay requested by telephone that BE cease posting eBay auction listings on its site. (Id. ¶ 9; Rock Decl. ¶ 5.) BE agreed to do so. (Rock Decl. ¶ 5.) In October 1999, BE learned that other auction aggregations sites were including information regarding eBay auctions. (Carney Decl. ¶ 12.) On November 2, 1999, BE issued a press release indicating that it had resumed including eBay auction listings on its site. (Rock Decl. Ex. H.) On November 9, 1999, eBay sent BE a letter reasserting that BE's activities were unauthorized, insisting that BE cease accessing the eBay site, alleging that BE's activities constituted a civil trespass and offering to license BE's activities. (Id. Ex. I.) eBay and BE were again unable to agree on licensing terms. As a result, eBay attempted to block BE from accessing the eBay site; by the end of November, 1999, eBay had blocked a total of 169 IP addresses it believed BE was using to query eBay's system. (Maynor Decl. ¶ 12.) BE elected to continue crawling eBay's site by using proxy servers to evade eBay's IP blocks. (Mundy Depo. at 271:18-19 ("We eventually adopted the rotating proxy servers."))

Approximately 69% of the auction items contained in the BE database are from auctions hosted on eBay. (Carney Decl. ¶ 17.) BE estimates that it would lose one-third of its users if it ceased to cover

http://pub.bna.com/lw/21200.htm

11/26/00
the eBay auctions. (Id.)

The parties agree that BE accessed the eBay site approximately 100,000 times a day. (Felton Decl. ¶ 33.) eBay alleges that BE activity constituted up to 1.53% of the number of requests received by eBay, and up to 1.10% of the total data transferred by eBay during certain periods in October and November of 1999. (Johnson-Laird Decl. ¶ 64.) BE alleges that BE activity constituted no more than 1.11% of the requests received by eBay, and no more than 0.70% of the data transferred by eBay. (Felton Decl. ¶ 60.) eBay alleges that BE activity had fallen 27%, to 0.74% of requests and 0.61% of data, by February 20, 2000. (Johnson-Laird Decl. ¶¶ 70-71.) eBay alleges damages due to BE's activity totaling between $45,323 and $61,804 for a ten month period including seven months in 1999 and the first three months in 2000. (Meyer Decl. ¶ 28.) However, these calculations appear flawed in that they assume the maximal BE usage of eBay resources continued over all ten months. (Id.) Moreover, the calculations attribute a pro rata share of eBay expenditures to BE activity, rather than attempting to calculate the incremental cost to eBay due to BE activity. (Id.) eBay has not alleged any specific incremental damages due to BE activity. (See Rock Depo., 192:8-10.)

It appears that major Internet search engines, such as Yahoo!, Google, Excite and AltaVista, respect the Robot Exclusion Standard. (Johnson-Laird Decl. ¶¶ 81-85.)

eBay now moves for preliminary injunctive relief preventing BE from accessing the eBay computer system based on nine causes of action: trespass, false advertising, federal and state trademark dilution, computer fraud and abuse, unfair competition, misappropriation, interference with prospective economic advantage and unjust enrichment. However, eBay does not move, either independently or alternatively, for injunctive relief that is limited to restricting how BE can use data taken from the eBay site.

II. LEGAL STANDARD

To obtain preliminary injunctive relief, a movant must demonstrate "either a likelihood of success on the merits and the possibility of irreparable injury, or that serious questions going to the merits were raised and the balance of hardships tips sharply in its favor." Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1517 (9th Cir. 1992) (citations omitted). The alternatives in the above standard represent "extremes of a single continuum," rather than two separate tests. Benda v. Grand Lodge of Int'l Ass'n of Machinists & Aerospace Workers, 584 F.2d 308, 315 (9th Cir. 1978). "The critical element in determining the test to be applied is the relative hardship to the parties. If the balance of harm tips decidedly toward the plaintiff, then the plaintiff need not show as robust a likelihood of success on the merits as when the balance tips less decidedly." Alaska v. Native Village of Venetie, 856 F.2d 1384, 1389 (9th Cir. 1988). A "serious question" is one on which the movant has a "fair chance of success on the merits." Sierra On-Line, Inc. v. Phoenix Software, Inc., 739 F.2d 1415, 1421 (9th Cir. 1984). Generally, the "balance of harm" evaluation should precede the "likelihood of success analysis" because until the balance of harm has been evaluated the court cannot know how strong and substantial the plaintiff's showing of the likelihood of success must be. See Village of Venetie, 856 F.2d at 1389.

III. ANALYSIS

A. Balance of Harm
eBay asserts that it will suffer four types of irreparable harm if preliminary injunctive relief is not granted: (1) lost capacity of its computer systems resulting from to BE's use of automated agents; (2) damage to eBay's reputation and goodwill caused by BE's misleading postings; (3) dilution of the eBay mark; and (4) BE's unjust enrichment. The harm eBay alleges it will suffer can be divided into two categories. The first type of harm is harm that eBay alleges it will suffer as a result of BE's automated query programs burdening eBay's computer system ("system harm"). The second type of harm is harm that eBay alleges it will suffer as a result of BE's misrepresentations regarding the information that BE obtains through the use of these automated query programs ("reputational harm").

As noted above, eBay does not seek an injunction that is tailored to independently address the manner in which BE uses the information it obtains from eBay. Even without accessing eBay's computer systems by robot, BE could inflict reputational harm by misrepresenting the contents of eBay's auction database or by misusing eBay's trademark. Moreover, allowing frequent and complete recursive searching of eBay's database (which would presumably exacerbate the system harm), requiring appropriate disclaimers regarding the accuracy of BE's listings, or limiting BE's use of the eBay mark would all reduce or eliminate the possibility of reputational harm, without requiring the drastic remedy of enjoining BE from accessing eBay's database. Since eBay does not move independently or alternatively for injunctive relief tailored toward the alleged reputational harm, the court does not include the alleged reputational harm in the balance of harm analysis, nor does the court address the merits of the causes of action based on the alleged reputational harm in the likelihood of success analysis.

According to eBay, the load on its servers resulting from BE's web crawlers represents between 1.11% and 1.53% of the total load on eBay's listing servers. eBay alleges both economic loss from BE's current activities and potential harm resulting from the total crawling of BE and others. In alleging economic harm, eBay's argument is that eBay has expended considerable time, effort and money to create its computer system, and that BE should have to pay for the portion of eBay's system BE uses. eBay attributes a pro rata portion of the costs of maintaining its entire system to the BE activity. However, eBay does not indicate that these expenses are incrementally incurred because of BE's activities, nor that any particular service disruption can be attributed to BE's activities. eBay provides no support for the proposition that the pro rata costs of obtaining an item represent the appropriate measure of damages for unauthorized use. In contrast, California law appears settled that the appropriate measure of damages is the actual harm inflicted by the conduct:

Where the conduct complained of does not amount to a substantial interference with possession or the right thereto, but consists of intermeddling with or use of or damages to the personal property, the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.

Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946). Moreover, even if BE is inflicting incremental maintenance costs on eBay, potentially calculable monetary damages are not generally a proper foundation for a preliminary injunction. See e.g., Sampson v. Murray, 415 U.S. 61, 90 (1974). Nor does eBay appear to have made the required showing that this is the type of extraordinary case in which monetary damages may support equitable relief. See In re Estate of Ferdinand Marcos, Human Rights Litigation, 25 F.3d 1467, 1480 (9th Cir. 1994) ("a district court has authority to issue a
preliminary injunction where the plaintiffs can establish that money damages will be an inadequate remedy due to impending insolvency of the defendant or that defendant has engaged in a pattern of secreting or dissipating assets to avoid judgment.

eBay's allegations of harm are based, in part, on the argument that BE's activities should be thought of as equivalent to sending in an army of 100,000 robots a day to check the prices in a competitor's store. This analogy, while graphic, appears inappropriate. Although an admittedly formalistic distinction, unauthorized robot intruders into a "brick and mortar" store would be committing a trespass to real property. There does not appear to be any doubt that the appropriate remedy for an ongoing trespass to business premises would be a preliminary injunction. See e.g., State v. Carriker, 214 N.E.2d 809, 811-12 (Ohio App. 1964) (interpreting Ohio criminal trespass law to cover a business invitee who, with no intention of making a purchase, uses the business premises of another for his own gain after his invitation has been revoked); General Petroleum Corp. v. Beilby, 213 Cal. 601, 605 (1931). More importantly, for the analogy to be accurate, the robots would have to make up less than two out of every one-hundred customers in the store, the robots would not interfere with the customers' shopping experience, nor would the robots even be seen by the customers. Under such circumstances, there is a legitimate claim that the robots would not pose any threat of irreparable harm. However, eBay's right to injunctive relief is also based upon a much stronger argument.

If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses. (See Spafford Decl. ¶ 32;12 Parker Decl. ¶ 19,13 Johnson-Laird Decl. ¶ 85.14) BE does not appear to seriously contest that reduced system performance, system unavailability or data loss would inflict irreparable harm on eBay consisting of lost profits and lost customer goodwill. Harm resulting from lost profits and lost customer goodwill is irreparable because it is neither easily calculable, nor easily compensable and is therefore an appropriate basis for injunctive relief. See, e.g., People of State of California ex rel. Van De Kamp v. Tahoe Reg'l Planning Agency, 766 F.2d 1316, 1319 (9th Cir. 1985). Where, as here, the denial of preliminary injunctive relief would encourage an increase in the complained of activity, and such an increase would present a strong likelihood of irreparable harm, the plaintiff has at least established a possibility of irreparable harm.15

In the patent infringement context, the Federal Circuit has held that a preliminary injunction may be based, at least in part, on the harm that would occur if a preliminary injunction were denied and infringers were thereby encouraged to infringe a patent during the course of the litigation. See Atlas Powder Co. v. Ireco Chems, 773 F.2d 1230, 1233 (Fed. Cir. 1985). In the absence of preliminary injunctive relief, "infringers could become compulsory licensees for as long as the litigation lasts." Id. The Federal Circuit's reasoning is persuasive. "The very nature of the patent right is the right to exclude others. . . . We hold that where validity and continuing infringement have been clearly established, as in this case, immediate irreparable harm is presumed. To hold otherwise would be contrary to the public policy underlying the patent laws." Smith Intern., Inc. v. Hughes Tool Co., 718 F.2d 1573, 1581 (Fed. Cir. 1983) (footnotes omitted). Similarly fundamental to the concept of ownership of personal property is the right to exclude others. See Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (characterizing "the right to exclude others" as "one of the most essential sticks in the bundle of rights that are commonly characterized as property"). If preliminary injunctive relief against an ongoing trespass to chattels were unavailable, a trespasser could take a compulsory license to use another's personal property for as long as the trespasser could perpetuate the litigation.

BE correctly observes that there is a dearth of authority supporting a preliminary injunction based on
an ongoing to trespass to chattels. In contrast, it is black letter law in California that an injunction is an appropriate remedy for a continuing trespass to real property. See Allred v. Harris, 14 Cal. App. 4th 1386, 1390 (1993) (citing 5 B.E. Witkin, Summary of California Law, Torts § 605 (9th ed. 1988)). If eBay were a brick and mortar auction house with limited seating capacity, eBay would appear to be entitled to reserve those seats for potential bidders, to refuse entrance to individuals (or robots) with no intention of bidding on any of the items, and to seek preliminary injunctive relief against non-customer trespassers eBay was physically unable to exclude. The analytic difficulty is that a wrongdoer can commit an ongoing trespass of a computer system that is more akin to the traditional notion of a trespass to real property, than the traditional notion of a trespass to chattels, because even though it is ongoing, it will probably never amount to a conversion. The court concludes that under the circumstances present here, BE's ongoing violation of eBay's fundamental property right to exclude others from its computer system potentially causes sufficient irreparable harm to support a preliminary injunction.

BE argues that even if eBay is entitled to a presumption of irreparable harm, the presumption may be rebutted. The presumption may be rebutted by evidence that a party has engaged in a pattern of granting licenses to engage in the complained of activity such that it may be reasonable to expect that invasion of the right can be recompensed with a royalty rather than with an injunction, or by evidence that a party has unduly delayed in bringing suit, thereby negating the idea of irreparability. See Polymer Technologies, Inc. v. Bridwell, 103 F.3d 970, 974 (Fed. Cir. 1996) (discussing presumption of irreparable harm in patent infringement context). BE alleges that eBay has both engaged in a pattern of licensing aggregators to crawl its site as well as delayed in seeking relief. For the reasons set forth below, the court finds that neither eBay's limited licensing activities nor its delay in seeking injunctive relief while it attempted to resolve the matter without judicial intervention are sufficient to rebut the possibility of irreparable harm.

If eBay's irreparable harm claim were premised solely on the potential harm caused by BE's current crawling activities, evidence that eBay had licensed others to crawl the eBay site would suggest that BE's activity would not result in irreparable harm to eBay. However, the gravamen of the alleged irreparable harm is that if eBay is allowed to continue to crawl the eBay site, it may encourage frequent and unregulated crawling to the point that eBay's system will be irreparably harmed. There is no evidence that eBay has indiscriminately licensed all comers. Rather, it appears that eBay has carefully chosen to permit crawling by a limited number of aggregation sites that agree to abide by the terms of eBay's licensing agreement. "The existence of such a [limited] license, unlike a general license offered to all comers, does not demonstrate a decision to relinquish all control over the distribution of the product in exchange for a readily computable fee." Ty, Inc. v. GMA Accessories, Inc., 132 F.3d 1167, 1173 (7th Cir. 1997) (discussing presumption of irreparable harm in copyright infringement context). eBay's licensing activities appear directed toward limiting the amount and nature of crawling activity on the eBay site. Such licensing does not support the inference that carte blanche crawling of the eBay site would pose no threat of irreparable harm.

eBay first learned of BE in late 1997 or early 1998 when BE sought to retain the same public relations firm used by eBay. (See Plen Decl. Ex. 1.) This motion was filed on January 18, 2000. An unexplained delay of two years would certainly raise serious doubts as to the irreparability of any alleged harm. See Playboy Enters., Inc. v. Netscape Communications Corp., 55 F. Supp. 2d 1070, 1090 (C.D. Cal. 1999) (noting that delay of as little as 60 days to three months has been held sufficient to rebut the presumption of irreparable harm). Here, the circumstances establish that any delay resulted from eBay's good faith efforts to resolve this dispute without judicial intervention and do not rebut a finding of the possibility of irreparable harm.
In April 1999, eBay agreed to allow BE to crawl the eBay site for 90 days while the parties negotiated a license. In late August or early September 1999, after the parties had failed to negotiate a license, eBay requested that BE stop crawling the eBay site, and BE complied. It was not until November 2, 1999, that BE issued a press release indicating that it had resumed including eBay auction listings on its site. In response, on November 9, 1999, eBay sent BE a letter again informing BE that its activities were unauthorized and again offering to license BE's activities. After eBay and BE were again unable to agree on licensing terms, eBay attempted to block BE from accessing the eBay site. By the end of November 1999, despite blocking more than 150 IP addresses, it became apparent that eBay was unable to prevent BE's crawling of the eBay system via rotating proxy servers. Having failed in its attempt at self-help, eBay filed this suit on December 10, 1999, and filed this motion five weeks later. The fact that eBay's primary concern is the threat from the likely increase in crawling activity that would result if eBay is allowed to continue its unauthorized conduct, combined with eBay's repeated attempts to resolve this dispute without judicial intervention, and BE's continuing attempts to thwart eBay's protection of its property, convinces the court that eBay's delay in seeking preliminary relief was justified.

BE argues that even if eBay will be irreparably harmed if a preliminary injunction is not granted, BE will suffer greater irreparable harm if an injunction is granted. According to BE, lack of access to eBay's database will result in a two-thirds decrease in the items listed on BE, and a one-eighth reduction in the value of BE, from $80 million to $70 million. (Sweeney Decl. ¶¶ 42, 43.) Although the potential harm to BE does not appear insignificant, BE does not appear to have suffered any irreparable harm during the period it voluntarily ceased crawling the eBay site. Barring BE from automatically querying eBay's site does not prevent BE from maintaining an aggregation site including information from eBay's site. Any potential economic harm is appropriately addressed through the posting of an adequate bond.

Moreover, it appears that any harm alleged to result from being forced to cease an ongoing trespass may not be legally cognizable. In the copyright infringement context, once a plaintiff has established a strong likelihood of success on the merits, any harm to the defendant that results from the defendant being preliminarily enjoined from continuing to infringe is legally irrelevant. See Triad Sys. Corp. v. Southeastern Exp. Co., 64 F.3d 1330, 1338 (9th Cir. 1995) (defendant "cannot complain of the harm that will befall it when properly forced to desist from its infringing activities."). The Ninth Circuit has held it to be reversible error for a district court to even consider "the fact that an injunction would be devastating to [defendant's] business" once the plaintiff has made a strong showing of likely success on the merits of a copyright infringement claim. Cadence Design Sys., Inc. v. Avant! Corp., 125 F.3d 824, 830 (9th Cir. 1997). The reasoning in these cases appears to be that a defendant who builds a business model based upon a clear violation of the property rights of the plaintiff cannot defeat a preliminary injunction by claiming the business will be harmed if the defendant is forced to respect those property rights. See Concrete Mach. Co., Inc. v. Classic Lawn Ornaments, Inc., 843 F.2d 600, 613 (1st Cir. 1988) ("If a strong likelihood of success is demonstrated, then the court should issue the injunction even if the defendant will incur the relatively greater burden; a probable infringer simply should not be allowed to continue to profit from its continuing illegality at the copyright owner's expense."). The Federal Circuit has crafted a similar rule with respect to patent infringement. See Windsurfing Int'l Inc. v. AMP, Inc., 782 F.2d 995, 1003 n.12 (Fed. Cir. 1986) ("One who elects to build a business on a product found to infringe cannot be heard to complain if an injunction against continuing infringement destroys the business so elected."). Accordingly, the court concludes that eBay has demonstrated at least a possibility of suffering irreparable system harm and that BE has not established a balance of hardships weighing in its favor.
B. Likelihood of Success

As noted above, eBay moves for a preliminary injunction on all nine of its causes of action. These nine causes of action correspond to eight legal theories: (1) trespass to chattels, (2) false advertising under the Lanham Act, 15 U.S.C. § 1125(a), (3) federal and state trademark dilution, (4) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (5) unfair competition, (6) misappropriation, (7) interference with prospective economic advantage and (8) unjust enrichment. The court finds that eBay has established a sufficient likelihood of prevailing on the trespass claim to support the requested injunctive relief. Since the court finds eBay is entitled to the relief requested based on its trespass claim, the court does not address the merits of the remaining claims or BE's arguments that many of these other state law causes of action are preempted by federal copyright law. The court first addresses the merits of the trespass claim, then BE's arguments regarding copyright preemption of the trespass claim, and finally the public interest.

1. Trespass

Trespass to chattels "lies where an intentional interference with the possession of personal property has proximately cause injury." Thrifty-Tel v. Beznik, 46 Cal. App. 4th 1559, 1566 (1996). Trespass to chattels "although seldom employed as a tort theory in California" was recently applied to cover the unauthorized use of long distance telephone lines. Id. Specifically, the court noted "the electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action." Id. at n.6. Thus, it appears likely that the electronic signals sent by BE to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action.

In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff. See Thrifty-Tel, 46 Cal. App. 4th at 1566; see also Itano v. Colonial Yacht Anchorage, 267 Cal. App. 2d 84, 90 (1968) ("When conduct complained of consists of intermeddling with personal property 'the owner has a cause of action for trespass or case, and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.'") (quoting Zaslow v. Kroenert, 29 Cal. 2d 541, 550 (1946)). Here, eBay has presented evidence sufficient to establish a strong likelihood of proving both prongs and ultimately prevailing on the merits of its trespass claim.

a. BE's Unauthorized Interference

EBay argues that BE's use was unauthorized and intentional. EBay is correct. BE does not dispute that it employed an automated computer program to connect with and search eBay's electronic database. BE admits that, because other auction aggregators were including eBay's auctions in their listing, it continued to "crawl" eBay's web site even after eBay demanded BE terminate such activity.

BE argues that it cannot trespass eBay's web site because the site is publicly accessible. BE's argument is unconvincing. eBay's servers are private property, conditional access to which eBay grants the public. EBay does not generally permit the type of automated access made by BE. In fact, eBay explicitly notifies automated visitors that their access is not permitted. "In general, California does recognize a trespass claim where the defendant exceeds the scope of the consent." Baugh v.

Even if BE's web crawlers were authorized to make individual queries of eBay's system, BE's web crawlers exceeded the scope of any such consent when they began acting like robots by making repeated queries. See City of Amsterdam v. Daniel Goldreyer, Ltd., 882 F. Supp. 1273, 1281 (E.D.N.Y. 1995) ("One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion."). Moreover, eBay repeatedly and explicitly notified BE that its use of eBay's computer system was unauthorized. The entire reason BE directed its queries through proxy servers was to evade eBay's attempts to stop this unauthorized access. The court concludes that BE's activity is sufficiently outside of the scope of the use permitted by eBay that it is unauthorized for the purposes of establishing a trespass. See Civic Western Corp. v. Zila Industries, Inc., 66 Cal. App. 3d 1, 17 (1977) ("It seems clear, however, that a trespass may occur if the party, entering pursuant to a limited consent, . . . proceeds to exceed those limits . . .") (discussing trespass to real property).

eBay argues that BE interfered with eBay's possessory interest in its computer system. Although eBay appears unlikely to be able to show a substantial interference at this time, such a showing is not required. Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel. See Thrifty-Tel, 46 Cal. App. 4th at 1567 (distinguishing the tort from conversion). Although the court admits some uncertainty as to the precise level of possessory interference required to constitute an intermeddling, there does not appear to be any dispute that eBay can show that BE's conduct amounts to use of eBay's computer systems. Accordingly, eBay has made a strong showing that it is likely to prevail on the merits of its assertion that BE's use of eBay's computer system was an unauthorized and intentional interference with eBay's possessory interest.

b. Damage to eBay's Computer System

A trespasser is liable when the trespass diminishes the condition, quality or value of personal property. See Compuserve, Inc. v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997). The quality or value of personal property may be "diminished even though it is not physically damaged by defendant's conduct." Id. at 1022. The Restatement offers the following explanation for the harm requirement:

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 . . . 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 cmt. e (1977).

http://pub.bna.com/lw/21200.htm 11/26/00
eBay is likely to be able to demonstrate that BE's activities have diminished the quality or value of eBay's computer systems. BE's activities consume at least a portion of plaintiff's bandwidth and server capacity. Although there is some dispute as to the percentage of queries on eBay's site for which BE is responsible, BE admits that it sends some 80,000 to 100,000 requests to plaintiff's computer systems per day. (Ritchey Decl. Ex. 3 at 391:11-12.) Although eBay does not claim that this consumption has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use, eBay's claim is that BE's use is appropriating eBay's personal property by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes. See CompuServe, 962 F.Supp. at 1022 ("any value [plaintiff] realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base.").

BE argues that its searches represent a negligible load on plaintiff's computer systems, and do not rise to the level of impairment to the condition or value of eBay's computer system required to constitute a trespass. However, it is undisputed that eBay's server and its capacity are personal property, and that BE's searches use a portion of this property. Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property. Accordingly, BE's actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay. If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value. California law does not require eBay to wait for such a disaster before applying to this court for relief. The court concludes that eBay has made a strong showing that it is likely to prevail on the merits of its trespass claim, and that there is at least a possibility that it will suffer irreparable harm if preliminary injunctive relief is not granted. eBay is therefore entitled to preliminary injunctive relief.

2. Copyright Preemption

BE argues that the trespass claim, along with eBay's other state law causes of action, "is similar to eBay's originally filed but now dismissed copyright infringement claim, and each is based on eBay's assertion that Bidder's Edge copies eBay's auction listings, a right within federal copyright law." Opp'n at 8:10-12. BE is factually incorrect to the extent it argues that the trespass claim arises out of what BE does with the information it gathers by accessing eBay's computer system, rather than the mere fact that BE accesses and uses that system without authorization.

A state law cause of action is preempted by the Copyright Act if, (1) the rights asserted under state law are "equivalent" to those protected by the Copyright Act, and (2) the work involved falls within the "subject matter" of the Copyright Act as set forth in 17 U.S.C. §§ 102 and 103. Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998). "In order not to be equivalent, the right under state law must have an extra element that changes the nature of the action so that it is qualitatively different from a copyright infringement claim." Xerox Corp. v. Apple Computer, Inc., 734 F. Supp. 1542, 1550 (N.D. Cal. 1990). Here, eBay asserts a right not to have BE use its computer systems without authorization. The right to exclude others from using physical personal property is not equivalent to any rights protected by copyright and therefore constitutes an extra element that makes trespass qualitatively different from a copyright infringement claim. But see, Ticketmaster Corp. v.
Tickets.com, Inc., No. CV-99-7654 (C.D. Cal. minute order filed Mar. 27, 2000) (dismissing trespass claim based on unauthorized Internet information aggregation as preempted by copyright law).

3. Public Interest

The traditional equitable criteria for determining whether an injunction should issue include whether the public interest favors granting the injunction. American Motorcyclist Ass'n v. Watt, 714 F.2d 962, 965 (9th Cir. 1983). The parties submit a variety of declarations asserting that the Internet will cease to function if, according to eBay, personal and intellectual property rights are not respected, or, according to BE, if information published on the Internet cannot be universally accessed and used. Although the court suspects that the Internet will not only survive, but continue to grow and develop regardless of the outcome of this litigation, the court also recognizes that it is poorly suited to determine what balance between encouraging the exchange of information, and preserving economic incentives to create, will maximize the public good. Particularly on the limited record available at the preliminary injunction stage, the court is unable to determine whether the general public interest factors in favor of or against a preliminary injunction.

BE makes the more specific allegation that granting a preliminary injunction in favor of eBay will harm the public interest because eBay is alleged to have engaged in anticompetitive behavior in violation of federal antitrust law. The Ninth Circuit has noted that in evaluating whether to issue a preliminary injunction, the district court is under no obligation to consider the merits of any antitrust counterclaims once the plaintiff has demonstrated a likelihood of success on the merits. See Triad Sys. Corp. v. Southeastern Exp. Co., 64 F.3d 1330, 1336 n.13 (9th Cir. 1995) (discussing claim of copyright infringement). Although anticompetitive behavior may be appropriately considered in the context of a preliminary injunction based on trademark infringement, where misuse is an affirmative defense, see Helene Curtis Indus. v. Church & Dwight Co., 560 F.2d 1325 (7th Cir. 1977), it does not appear to be appropriately considered here, because there is no equivalent affirmative defense to trespass to chattels. Accordingly, the court concludes the public interest does not weigh against granting a preliminary injunction.

IV. ORDER

Bidder's Edge, its officers, agents, servants, employees, attorneys and those in active concert or participation with them who receive actual notice of this order by personal service or otherwise, are hereby enjoined pending the trial of this matter, from using any automated query program, robot, web crawler or other similar device, without written authorization, to access eBay's computer systems or networks, for the purpose of copying any part of eBay's auction database. As a condition of the preliminary injunction, eBay is ordered to post a bond in the amount of $2,000,000 to secure payment of any damages sustained by defendant if it is later found to have been wrongfully enjoined. This order shall take effect 10 days from the date on which it is filed.

Nothing in this order precludes BE from utilizing information obtained from eBay's site other than by automated query program, robot, web crawler or similar device. The court denies eBay's request for a preliminary injunction barring access to its site based upon BE's alleged trademark infringement, trademark dilution and other claims. This denial is without prejudice to an application for an injunction limiting or conditioning the use of any information obtained on the theory that BE's use violates some protected right of eBay.
FOOTNOTES

1 On April 21, 2000, defendant Bidder's Edge, Inc. filed an ex parte motion for leave to file a supplemental declaration in order to respond to factual assertions in the reply. Although the court suspects that with reasonable diligence BE could have prepared the declaration at least by the hearing date, the declaration consists merely of the results of four searches performed on major Internet search engines. eBay's opposition did not cite any prejudice that would result from its filing. Accordingly, BE's motion is granted.

2 Programs that recursively query other computers over the Internet in order to obtain a significant amount of information are referred to in the pleadings by various names, including software robots, robots, spiders and web crawlers.

3 It is unclear who Peter Leeds is, except that his email address at the time was <peter@biddersedge.com>.

4 Q: Are you aware of any complaints from eBay users about slowdowns that were caused by aggregators?

A: No.

5 BE appears to argue that this cannot be the case because searches performed on each of these search engines will return results that include eBay web pages. (Supp. Ploen Decl. ¶¶ 1-9.) However, this does not establish that these sites do not respect robot exclusion headers. There are numerous ways in which search engines can obtain information in compliance with exclusion headers, including: obtaining consent, abiding by the robot.txt file guidelines, or manually searching the sites. BE did not present any evidence of any site ever complaining about the activities of any of these search engines.

6 The bulk of eBay's moving papers and declarations address the alleged misuse of the eBay mark and the information BE obtains from the eBay computers. The court does not address the facts specific to these claims, nor the merits of these claims. Even if eBay were able to establish a likelihood of success on the merits as to these causes of action, such a showing would only support injunctive relief addressing BE's use of the eBay mark and BE's use of the eBay auction listings (the appropriate relief for which would appear to be a disclaimer regarding the lack of affiliation between eBay and BE and explicitly alerting customers to the limited scope of BE's information). Such a showing would not be sufficient to enjoin BE from accessing eBay's computer systems, which is the only relief eBay appears to request.

7 eBay does not appear to offer any support for the proposition that unjust enrichment is an independent cause of action, let alone an independently adequate basis for preliminary injunctive relief.

8 Although, as a practical matter, enjoining BE from accessing eBay's computers or searching eBay's auction database may result in BE's inability to make effective use of information from eBay's auction site.
9. Thus, eBay's motion appears to be, in part, a tactical effort to increase the strength of its license negotiating position and not just a genuine effort to prevent irreparable harm.

10. This case was filed on December 10, 1999. BE decommissioned a number of its servers in mid-December 1999. (See Mundy Depo. at 75:12-14.) Reformatting the hard drives resulted in the destruction of the server logs that may have indicated the actual duration of access to eBay's system. (See id. at 74:17-24.) eBay argues this should support an adverse inference against BE because eBay is unable to correlate BE's access to eBay's system with service disruptions. BE responds that these actions were a result of hardware failures unrelated to the litigation. The court agrees that these actions may support an inference that the information BE destroyed was prejudicial. However, final resolution of the fact-dependent questions regarding the circumstances under which this information was destroyed requires a more complete record. Accordingly, eBay is not entitled to a conclusive presumption of harm at this juncture in the proceedings, and eBay's motion to strike all evidence submitted by BE relating to a lack of harm is denied.

11. The phrase "brick and mortar" is often used to designate a traditional business when contrasting it with a predominantly, or entirely, on-line business. The phrase appears to refer to the historical reliance on conducting commerce within the context of a physical space made from materials such as brick and mortar, as opposed to the modern trend toward conducting commerce in a cyberspace made from computers programs.

12. "If 30 or 40 companies spring into existence using similar business models, what will be the total load and impact on eBay's servers?"

13. "One crawler may currently use 1% of eBay's resources. What if hundred of users used similar crawlers?"

14. "Given that Bidder's Edge can be seen to have imposed a load of 1.53% on eBay's listing servers, simple arithmetic and economics reveal how only a few more such companies deploying rude robots [that do not respect the Robot Exclusion Standard] would be required before eBay would be brought to its knees by what would be then a debilitating load."

15. As discussed below, eBay has established a strong likelihood of success on the merits of the trespass claim, and is therefore entitled to preliminary injunctive relief because it has established the possibility of irreparable harm. Accordingly, the court does not reach the issue of whether the threat of increased activity would be sufficient to support preliminary injunctive relief where the plaintiff has not made as strong of a showing of likelihood of success on the merits.

16. As other courts have noted, applying traditional legal principles to the Internet can be troublesome. See ImOn, Inc. v. ImaginOn, Inc., — F. Supp. 2d —, —, 2000 WL 310373, at *1 (S.D.N.Y. Mar. 27, 2000) ("Both parties are suppliers of 'services or products' on the Internet which, as I recognize and grapple with hereafter, is one of the most fluid, rapidly developing, and virtually daily changing areas of commerce that the law has had to focus upon and endeavor to apply established principles to.")

17. Because BE was expressly notified that its conduct was unauthorized, it does not matter whether BE ever agreed to a version of the eBay User Agreement that prohibited robotic activity.
Plaintiff believes that it may have experienced system failures and a decrease in system performance during the times that defendant was searching its system, however, it is unable to produce any correlation between its outages and defendant's activities. Plaintiff contends that it would likely be able to produce such a correlation but for defendant's alleged destruction of logs that recorded the details of its robotic search activities.
The motions to dismiss the First Amended Complaint (FAC) made by defendant Tickets.com, Inc. (hereafter Tickets) is granted with 10 days leave to amend as to claims 2 (breach of contract), 6 (misappropriation), 8 (trespass), and 9 (unjust enrichment). The motion is denied as to claims 1 (copyright infringement), 2 (federal unfair competition and reverse passing off), 4 (false advertising), 5 (state unfair business practices) and 10 (interference with business advantage). Defendant need not answer the claims not dismissed until either 10 days after a Second Amended complaint has been filed or notice is given that such will not be filed.

Both parties have made reference to declarations filed in connection with the forthcoming motion for preliminary injunction. Such matters may not be properly considered on an FRCP 12(b)(6) motion to dismiss the complaint, which limits consideration to matters in the complaint and items of which the court may take judicial notice (none here). However, where an amended complaint has been filed, items pleaded or attached as exhibits to the original complaint may be considered to the extent they contradict assertions in the amended complaint.

The web site of plaintiffs Ticketmaster Corporation and Ticketmaster Online-CitySearch, Inc. (hereafter collectively, in the singular Ticketmaster) operates to allow customers to purchase tickets to various events (concerts, ball games, etc.) through an internet connection with its customers. On the Ticketmaster home page, there are instructions and a directory to subsequent pages (one per event). The event pages provide basic information (short description of the event, date, time, place, and price) and a description of how to order tickets by either internet response, telephone, mail, or in person. Each of these subsequent pages is identifiable with an electronic address. The home page further contains (if a customer scrolls to the bottom) "terms and conditions" which prescribe, among other things, copying for commercial use. However, the customer need not view the terms and conditions to proceed straight to the event page which interests him. Ticketmaster has exclusive agreements with the events it carries on its web pages so that tickets are not generally available to those events except through Ticketmaster (or reserved for sale by the event itself, or available from premium ticket brokers who generally charge higher than face value).

Tickets also operates a web site (Tickets.Com) which performs a somewhat different ticketing service. While Tickets does sell some tickets to certain events on its own, it also provides information as to where and how tickets which it does not sell may be purchased. A short factual description as to event, time, date, place and price is listed. Where Tickets does not itself sell the tickets, a place is given the customers can click for a reference to another ticket broker, or to another on-line ticket seller. Here is where the unique feature of this case -- hyperlinks or deep linking -- comes in. Where the exclusive ticket broker is Ticketmaster, and the customer clicks on "Buy this ticket from another on-line ticketing company", the customer is instantly transferred to the interior web page of Ticketmaster (by passing the home page) for the particular event in question, where the customer may buy the tickets (from Ticketmaster, not Tickets) on-line. An explanation is generally given by Tickets as follows: "These tickets are sold by another ticketing company. Although we can't sell them to you, the link above will take you directly to the other company's web site where you can purchase them." The interior web page contains the Ticketmaster logo and the customer must know he is dealing with Ticketmaster, not Tickets.

In order to obtain the basic information on Ticketmaster events, Tickets is alleged to copy the interior web pages and extract the basic information (event, place, time, date and price) from them. That information is then
placed in Tickets format on its own interior web pages. Tickets no longer (if it once did, as alleged) merely copies the Ticketmaster event page on its own event page. However, by the use of hyper-linking (i.e. electronic transfer to the particularly numbered interior web page of Ticketmaster), the customer is transferred directly to the Ticketmaster interior event page.

The motion to dismiss the first claim (copyright infringement) is denied because the complaint alleges actual copying. Plaintiff claims that the copying includes printing the factual information derived from the Ticketmaster interior web pages. The court does not accept this argument. A copyright may not be claimed to protect factual data (Feist Publications '91 499 US 340, 113 LED2d 358). While the expression, organization, placement, etc., of the factual data may be protected, Tickets is not alleged to have copied the method of presentation, but rather to have extracted the factual data and presented it in its own format. Where Tickets is alleged to have copied (¶ 35 of FAC) is in the making of thousands of copies taken from Ticketmaster's interior web pages for the purpose of extracting the factual data carried thereon and using it to publish its own version containing the factual data. Thus, copying is alleged (albeit not republication of protected material). Thus, the court rejects Ticketmaster's basic contention that it is copyright infringement to take basic facts from its publicly available web pages and use those facts (if the expression and method of presentation is not copied). Copying is alleged by transferring the event pages to Ticket's own computer to facilitate extraction of the facts. This is a very different case from merely copying for its customers the Ticketmaster event pages. This falls in the same category of taking historical facts from a work of reference and printing them in different expression. By a similar analogy, the hyperlink to the interior web page (whatever it may do for the unfair competition or interference claims) does not allege copying.

Further, hyperlinking does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved. The customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently.

There is an ambiguity in the FAC which yet needs to be cleared up, although not involving a failure to state a claim. A federal court does not have jurisdiction of a copyright infringement claim until the copyright is registered (or refused registration). (In at least one circuit, application for registration is sufficient to confer jurisdiction.) In ¶ 26 of the FAC, it is alleged that the "Ticketmaster Web Site, including the Ticketmaster Event Pages, is subject to copyright owned by Ticketmaster Corp. The copyright of the Ticketmaster Web Site has been registered with the United States Copyright Office..." Exhibit F to the FAC shows that the title of the work copyrighted is "Ticketmaster.com Web Site II" and (later) "Ticketmaster.com Web site III" and that the nature of the authorship is "underlying source code." The event pages change from day to day as old events are dropped out and new ones are added. There is a possible ambiguity as to whether the copyright as registered covers not only the home page but also each of the event pages. Since the alleged copying is only of the event pages, there is still the question for further proceedings as to the court's jurisdiction over the claim of copyright infringement of the event pages.

The motion to dismiss the second claim (breach of contract) is founded on the "terms and conditions" set forth on the home page of the Ticketmaster site. This provides that anyone going beyond the home page agrees to the terms and conditions set forth, which include that the information is for personal use only, may not be used for commercial purposes, and no deep linking to the site is permitted. In defending this claim, Ticketmaster makes reference to the "shrink-wrap license" cases, where the packing on the outside of the CD stated that opening the package constitutes adherence to the license agreement (restricting republication) contained therein. This has been held to be enforceable. That is not the same as this case because the "shrink-wrap license agreement" is open and obvious and in fact hard to miss. Many web sites make you click on "agree" to the terms and conditions before going on, but Ticketmaster does not. Further, the terms and conditions are set forth so that the user needs to scroll down the home page to find and read them. Many customers instead are likely to proceed to the event page of interest rather than reading the "small print." It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with anyone using the web site. The motion is granted with leave to amend in case there are facts showing Tickets' knowledge of them plus facts showing implied agreement to them.

The motion is denied as to the 3d, 4th, and 5th claims (passing off, reverse passing off, and false advertising). These claims state federal (Lanham Act) claims. As defendants point out, the exhibits attached to the original complaint and the FAC do not appear to support the claims, but they are not necessarily intended to. The body of the FAC alleges that Tickets falsely suggested or implied an association with Ticketmaster, the giving of misleading information about phone numbers, and the unauthorized control over event pages of Ticketmaster.
The complaint also alleges deep linking as an example of unfair competition, but the court concludes that deep linking by itself (i.e., without confusion of source) does not necessarily involve unfair competition. The false advertising claim is supported by allegations that Tickets has falsified information about the availability of tickets through Ticketmaster and that tickets are available only through premium ticket brokers. Tickets acknowledge that there may have been some accidental errors, which were corrected, but this issue is for later proceedings. Commercial advertising (i.e., publication by a business competitor) is sufficiently alleged to state a claim.

The next topic is Copyright Act preemption of state law claims. State law claims which come "within the general scope of copyright" are preempted (17 USC § 301(a); see Dielsi CDCA'96 916 FSupp 985, 991). This means that matters within the scope of copyright law are preempted when the state law rights are equivalent to rights under the general scope of copyright. To survive, the state law claims must have an "extra element" which changes the nature of the claim (Del Madera Properties 9Cir'87 820 F2d 973, 976). Further, where copying is permitted by the Copyright Act, a contrary state law could not be enforced. Applying these principles to this case:

1. The contract claim is not preempted Aside from copying (which is preempted), the contract claim, alleges adherence by Tickets to a contract not to use for commercial purposes (possibly not preempted) and not to deep link (not preempted). (See, e.g., Trenton Infinity CDCA'94 865 FSupp 1416, 1429.)

2. The 6th and 8th claims (misappropriation and trespass) are preempted and the motion is granted as to these claims. The essence of each claim is the invasion and taking of factual information compiled by Ticketmaster. To the extent that state law would allow protection of factual data (not clear at all), this cannot be squared with the Copyright Act (see Feist, supra). In addition, it is hard to see how entering a publicly available web site could be called a trespass, since all are invited to enter.

3. The 7th claim (state unfair business practices) is preempted insofar as it alleges the taking and publication of factual data. However, the claim also alleges the use of false advertising, supplying the "extra element" over and above copyright law. Accordingly, the motion is denied as to this claim.

4. The 9th claim (unjust enrichment) is preempted and the motion to dismiss is granted since the allegation is that defendant enriched themselves by taking the factual material from Ticketmaster's web site. It is hard to see how this could be since Tickets is not selling the tickets or participating in the proceeds. Whether that is correct or not, copyright preemption covers the subject of taking factual data without taking the mode of expression of same.

5. The 10th claim (tortious interference with prospective business advantage) is not preempted. This claim is that advertisers who pay on the basis of the number of "hits" on the home page will not pay for deep linked reference to the interior event pages. This is alleged to be purposely done to disrupt Ticketmaster's income from those advertisers. Further, the allegation is made that bypassing the home page enables the customer to avoid the terms and conditions, which are not available to him on the event page. There are virtually no cases on deep linking, particularly none on linking to particular interior pages of a website. The allegations of deliberately disrupting business by hyper-linking do alleged the "extra element" necessary to escape preemption. Accordingly, the court is not ready to definitively rule on this in the context of an interference claim and the motion to dismiss is denied as to this claim.
United States District Court
Central District of California
Southern Division

Plaintiff,

vs.

Arriba Soft Corp., et al.
Defendants.

On apparent first impression, the Court holds the use by an
Internet “visual search engine” of others’ copyrighted images is a
prima facie copyright violation, but it may be justified under the
“fair use” doctrine. The Court finds that, under the particular
circumstances of this case, the “fair use” doctrine applies, and the
Digital Millennium Copyright Act is not violated.

Defendant’s Motion for Partial Summary Judgment on Plaintiff’s
First and Second Claims for Relief is GRANTED. Plaintiff’s Motion for
Partial Summary Judgment is DENIED.

I. BACKGROUND

Defendant Ditto (formerly known as Arriba) operates a “visual
search engine” on the Internet. Like other Internet search engines,
it allows a user to obtain a list of related Web content in response
to a search query entered by the user. Unlike other Internet search
eengines, Defendant's retrieves images instead of descriptive text. It
produces a list of reduced, "thumbnail" pictures related to the user's
query.

During the period when most of the relevant events in this case
occurred, Defendant's visual search engine was known as the Arriba
Vista Image Searcher. By "clicking" on the desired thumbnail, an
Arriba Vista user could view the "image attributes" window displaying
the full-size version of the image, a description of its dimensions,
and an address for the Web site where it originated. ¹ By clicking on
the address, the user could link to the originating Web site for the
image. ²

Ditto's search engine (in both of its versions) works by
maintaining an indexed database of approximately two million thumbnail
images. These thumbnails are obtained through the operation of
Ditto's "crawler," a computer program that travels the Web in search
of images to be converted into thumbnails and added to the index. ³

¹/ This full-size image was not technically located on
Defendant's Web site. It was displayed by opening a link to its
originating Web page. But only the image itself, and not any
other part of the originating Web page, was displayed on the
image attributes page. From the user's perspective, the source
of the image matters less than the context in which it is
displayed.

²/ Defendant's current search engine, ditto.com, operates in
a slightly different manner. When a ditto.com user clicks on a
thumbnail, two windows open simultaneously. One window contains
the full-size image; the other contains the originating Web page
in full.

³/ Images are briefly stored in full on Defendant's server
until the thumbnail is made; they are then deleted. Joint Stip.
¶ 32. There is no claim that Defendant provides any access to
(continued...)
Ditto's employees conduct a final screening to rank the most relevant thumbnails and eliminate inappropriate images.

Plaintiff Kelly is a photographer specializing in photographs of California gold rush country and related to the works of Laura Ingalls Wilder. He does not sell the photographs independently, but his photographs have appeared in several books. Plaintiff also maintains two Web sites, one of which (www.goldrush1849.com) provides a "virtual tour" of California's gold rush country and promotes Plaintiff's book on the subject, and the other (www.showmethegold.com) markets corporate retreats in California's gold rush country.

In January 1999, around thirty five of Plaintiff's images were indexed by the Ditto crawler and put in Defendant's image database. As a result, these images were made available in thumbnail form to users of Defendant's visual search engine.

After being notified of Plaintiff's objections, Ditto removed the images from its database, though due to various technical problems some of the images reappeared a few times. Meanwhile Plaintiff, having sent Defendant a notice of copyright infringement in January, filed this action in April. Plaintiff argues its copyrights in the images were infringed by Defendant's actions and also alleges Defendant violated the Digital Millennium Copyright Act (DMCA) by removing or altering the copyright management information associated with Plaintiff's images.4/

3/ (...continued) the full-sized images during this period.

4/ Defendant's request for judicial notice of a Nature article, and Plaintiff's objection to the request, are both inappropriate. The parties have already included this article as (continued...)
II. DISCUSSION

These cross motions for summary adjudication present two questions of first impression. The first is whether the display of copyrighted images by a "visual search engine" on the Internet constitutes fair use under the Copyright Act. The second is whether the display of such images without their copyright management information is a violation of the Digital Millennium Copyright Act.

Summary judgment is proper if there is no genuine issue of fact and the moving party is entitled to a judgment as a matter of law. Fed. R. Civ. Proc. 56(c). If no material historical facts are disputed, the ultimate conclusion to be drawn on the issue of "fair use" is for the Court and not a jury. Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985); Fisher v. Decca, 794 F.2d 432, 436 (9th Cir. 1986).

A. Fair Use

In order to show copyright infringement, Plaintiff must show ownership of a valid copyright and invasion of one of the exclusive rights of copyright holders. 17 U.S.C. § 106. Defendant does not dispute the validity of Plaintiff's copyrights or his ownership of them. Defendant also does not dispute it reproduced and displayed Plaintiff's images in thumbnail form without authorization. Plaintiff thus has shown a prima facie case of copyright infringement unless the fair use doctrine applies.

"Fair use" is a limitation on copyright owners' exclusive right "to reproduce the copyrighted work in copies." 17 U.S.C. § 106(1).

\[^{4/}(\ldots\text{continued})\]

Exhibit 5 to their Joint Stipulation of Facts.
It is codified at 17 U.S.C. § 107, which provides:

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include--

(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.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

Fair use is an affirmative defense, and defendants carry the burden of proof on the issue. American Geophysical Union v. Texaco Inc., 60 F.3d 913, 918 (2d Cir. 1995); Columbia Pictures Ind. v. Miramax Films Corp., 11 F.Supp.2d 1179, 1187 (C.D. Cal. 1998) ("[b]ecause fair use is an affirmative defense, Defendants bear the burden of proof on all of its factors"). Based on an analysis of the factors, the Court finds there is fair use here.
1. Purpose and Character Of The Use

The first factor considers the nature of the use, including whether the use is commercial or educational. This, however, does not end the inquiry. "Purpose and character" also involve an assessment of whether "the new work merely supersedes the objects of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message; it asks, in other words, whether and to what extent the new work is transformative." *Campbell v. Acuff-Rose Music*, 510 U.S. 569, 579 (1994) (citation omitted). "[T]he more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use." *Id.* at 579.

There is no dispute Defendant operates its Web site for commercial purposes. Plaintiff's images, however, did not represent a significant element of that commerce, nor were they exploited in any special way.\(^5\) They were reproduced as a result of Defendant's generally indiscriminate method of gathering images. Defendant has a commercial interest in developing a comprehensive thumbnail index so it can provide more complete results to users of its search engine. The Ditto crawler is designed to obtain large numbers of images from numerous sources without seeking authorization.\(^6\) Plaintiff's images

\(^5\) The use in this case is commercial, but it is unusual and less serious than many other commercial uses. If, for example, Plaintiff's images were used without authorization in advertising for Defendant's Web site, a finding of fair use would be much less likely.

\(^6\) The parties argue at length about the possibility of blocking the Ditto crawler from a Web site by use of a (continued...
were indexed as a result of these methods. While the use here was
commercial, it was also of a somewhat more incidental and less
exploitative nature than more traditional types of "commercial use."\(^7\)
The most significant factor favoring Defendant is the
transformative nature of its use of Plaintiff's images. Defendant's
use is very different from the use for which the images were
originally created. Plaintiff's photographs are artistic works used
for illustrative purposes. Defendant's visual search engine is
designed to catalog and improve access to images on the Internet.
Joint Stip. ¶¶ 27-29, 32. The character of the thumbnail index is not
esthetic, but functional; its purpose is not to be artistic, but to be
comprehensive.

To a lesser extent, the Arriba Vista image attributes page also
served this purpose by allowing users to obtain more details about an
image. The image attributes page, however, raises other concerns. It

\(^6\)(...continued)
"robots.txt" file or other methods. Defendant posted
instructions on its Web site for blocking the Ditto crawler in
March, after Plaintiff's images had already been indexed.
Plaintiff's Web sites have never used any of these blocking
methods. Joint Stip. ¶ 34.
The Ditto crawler has, in the past, apparently visited sites
that were supposed to be blocked. Plaintiff argues this is
evidence of bad faith by Defendant and suggests the fair use
defense should as a result be precluded. The record shows
Defendant made efforts to correct problems of this sort when it
became aware of them, and did not act in bad faith.

\(^7\) Defendant also sought to promote a now-discontinued
software product called Arriba Express. Arriba Express allowed
users to "vacuum" an entire originating Web site and store it on
their computers simply by pointing at a thumbnail. Joint Stip.
¶ 45-50, Exh. 18. The images would be stored along with all
content from the originating Web site. Arriba Express served a
function related to that of the search engine, and Defendant's
promotion of it represents a related type of "commercial use."
allowed users to view (and potentially download) full-size images without necessarily viewing the rest of the originating Web page. At the same time, it was less clearly connected to the search engine's purpose of finding and organizing Internet content for users. The presence of the image attributes page in the old version of the search engine somewhat detracts from the transformative effect of the search engine. But, when considering purpose and character of use in a new enterprise of this sort, it is more appropriate to consider the transformative purpose rather than the early imperfect means of achieving that purpose. The Court finds the purpose and character of Defendant's use was on the whole significantly transformative.

The Court finds the first factor weighs in favor of fair use.

2. Nature of the Copyrighted Work

The second factor in § 107 is an acknowledgment "that some works are closer to the core of intended copyright protection than others, with the consequence that fair use is more difficult to establish when the former works are copied." Campbell, supra 510 U.S. at 586. Artistic works like Plaintiff's photographs are part of that core. The Court finds the second factor weighs against fair use.

3. Amount And Substantiality of the Portion Used

The third fair use factor assesses whether the amount copied was "reasonable in relation to the purpose of the copying." Id. The analysis focuses on "the persuasiveness of a [copier's] justification for the particular copying done, and the enquiry will harken back to the first of the statutory factors, for . . . the extent of permissible copying varies with the purpose and character of the use." Id. at 586-87.
In the thumbnail index, Defendant used Plaintiff's images in their entirety, but reduced them in size. Defendant argues it is necessary for a visual search engine to copy images in their entirety so users can be sure of recognizing them, and the reduction in size and resolution mitigates damage that might otherwise result from copying. As Defendant has illustrated in its brief, thumbnails cannot be enlarged into useful images. Defendant's Memo of P & A, at 3. Use of partial images or images further reduced in size would make images difficult for users to identify, and would eliminate the usefulness of Defendant's search engine as a means of categorizing and improving access to Internet resources.

As with the first factor, the Arriba Vista image attributes page presents a greater problem because it displayed a full-size image separated from the surrounding content on its originating Web page. Image attributes (e.g. dimensions and the address of the originating site) could have been displayed without reproducing the full-size image, and the display of the full image was not necessary to the main purposes of the search engine.8/

If only the thumbnail index were at issue, Defendant's copying would likely be reasonable in light of its purposes. The image attributes page, however, was more remotely related to the purposes of the search engine. The Court finds the third factor weighs slightly against fair use.

4. Effect of the Use On The Potential Market or Value

8/ The newer search engine, ditto.com, appears to lessen this problem by eliminating the image attributes page and simultaneously opening the originating Web page along with a full-size image.
The fourth factor inquiry examines the direct impact of the defendant's use and also considers "whether unrestricted and widespread conduct of the sort engaged in by the defendant . . . would result in a substantially adverse impact on the potential market for the original." Campbell, supra, 510 U.S. at 590 (citation omitted).

The relevant market is Plaintiff's Web sites as a whole. The photographs are used to promote the products sold by Plaintiff's Web sites (including Plaintiff's books and corporate tour packages) and draw users to view the additional advertisements posted on those Web sites. The fourth factor addresses not just the potential market for a particular photo, but also its "value." The value of Plaintiff's photographs to Plaintiff could potentially be adversely affected if their promotional purposes are undermined.

Defendant argues there is no likely negative impact because its search engine does not compete with Plaintiff's Web sites and actually increases the number of users finding their way to those sites.

Plaintiff argues the market for his various products has been harmed. Defendant's conduct created a possibility that some users might improperly copy and use Plaintiff's images from Defendant's site. Defendant's search engine also enabled users to "deep link" directly to the pages containing retrieved images, and thereby bypass the "front page" of the originating Web site. As a result, these users would be less likely to view all of the advertisements on the Web sites or view the Web site's entire promotional message. However, Plaintiff has shown no evidence of any harm or adverse impact.

In the absence of any evidence about traffic to Plaintiff's Web sites or effects on Plaintiff's businesses, the Court cannot find any
market harm to Plaintiff. The Defendant has met its burden of proof by offering evidence tending to show a lack of market harm, and Plaintiff has not refuted that evidence. The Court finds the fourth factor weighs in favor of fair use.

5. Conclusion--Fair Use

The Court finds two of the four factors weigh in favor of fair use, and two weigh against it. The first and fourth factors (character of use and lack of market harm) weigh in favor of a fair use finding because of the established importance of search engines and the "transformative" nature of using reduced versions of images to organize and provide access to them. The second and third factors (creative nature of the work and amount or substantiality of copying) weigh against fair use.

The first factor of the fair use test is the most important in this case. Defendant never held Plaintiff's work out as its own, or even engaged in conduct specifically directed at Plaintiff's work. Plaintiff's images were swept up along with two million others available on the Internet, as part of Defendant's efforts to provide its users with a better way to find images on the Internet. Defendant's purposes were and are inherently transformative, even if its realization of those purposes was at times imperfect. Where, as here, a new use and new technology are evolving, the broad transformative purpose of the use weighs more heavily than the inevitable flaws in its early stages of development.

The Court has weighed all of the § 107 factors together. The Court finds Defendant's conduct constituted fair use of Plaintiff's images. There is no triable issue of material fact remaining to be
resolved on the question of fair use, and summary adjudication is appropriate. Defendant's motion is GRANTED and Plaintiff's motion is DENIED as to the copyright infringement claims.

B. Digital Millennium Copyright Act

Enacted on October 28, 1998, the Digital Millennium Copyright Act (DMCA) implements two earlier World Intellectual Property Organization treaties. Section 1202 of the DMCA governs "integrity of copyright management information."\(^9\) Section 1202(a) prohibits falsification of copyright management information with the intent to aid copyright infringement. Section 1202(b) prohibits, unless authorized, several forms of knowing removal or alteration of copyright management information.\(^10\) Section 1203 creates a federal civil action for

9/ "Copyright management information" is defined, in relevant part, as:
[Al]ny of the following information conveyed in connection with copies . . . of a work . . . or displays of a work, including in digital form . . . :
(1) The title and other information identifying the work, including the information set forth on a notice of copyright.
(2) The name of, and other identifying information about, the author of a work.
(3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.
17 U.S.C. § 1202 (c).

10/ Section 1202(b) provides, in relevant part,
No person shall, without the authority of the copyright owner or the law--
(1) intentionally remove or alter any copyright management information,

(continued...)
violations of these provisions.

Plaintiff argues Defendant violated § 1202(b) by displaying thumbnails of Plaintiff's images without displaying the corresponding copyright management information consisting of standard copyright notices in the surrounding text. Joint Stip. of Facts, ¶¶ 64-69. Because these notices do not appear in the images themselves, the Ditto crawler did not include them when it indexed the images.\textsuperscript{11} Id. ¶ 70. As a result, the images appeared in Defendant's index without the copyright management information, and any users retrieving Plaintiff's images while using Defendant's Web site would not see the copyright management information.

Section 1202(b)(1) does not apply to this case. Based on the language and structure of the statute, the Court holds this provision applies only to the removal of copyright management information on a plaintiff's product or original work. Moreover, even if § 1202(b)(1) applied, Plaintiff has not offered any evidence showing Defendant's actions were intentional, rather than merely an unintended side effect of the Ditto crawler's operation. \textsuperscript{7} Is the crawler intentional? \(\text{If the code is programmed, isn't that}\) Here, where the issue is the absence of copyright management information from copies of Plaintiff's works, the applicable provision is § 1202(b)(3). To show a violation of that section, Plaintiff must show Defendant makes available to its users the thumbnails and full-

\textsuperscript{10}(...continued) any right under [federal copyright law].

\textsuperscript{11} There was one exception--a version of the "Shasta Rainbow" image obtained by the Ditto crawler from a third-party Web site. The copyright notice for that image was incorporated into the image itself (fine print along the edge of the picture). See Joint Stip., ¶¶ 72-73. Plaintiff's allegations of DMCA violations are inapplicable to this image.
size images, which were copies of Plaintiff's work separated from their copyright management information, even though it knows or should know this will lead to infringement of Plaintiff's copyrights. There is no dispute the Ditto crawler removed Plaintiff's images from the context of Plaintiff's Web sites where their copyright management information was located, and converted them to thumbnails in Defendant's index. There is also no dispute the Arriba Vista search engine allowed full-size images to be viewed without their copyright management information.

Defendant's users could obtain a full-sized version of a thumbnailed image by clicking on the thumbnail. A user who did this was given the name of the Web site from which Defendant obtained the image, where any associated copyright management information would be available, and an opportunity to link there.\textsuperscript{12/} Users were also informed on Defendant's Web site that use restrictions and copyright limitations may apply to images retrieved by Defendant's search engine.\textsuperscript{13/}

Based on all of this, the Court finds Defendant did not have "reasonable grounds to know" it would cause its users to infringe

\textsuperscript{12/} Through Defendant's current search engine, ditto.com, the user can no longer open a full-sized image without also opening the site where its copyright management information is located.

\textsuperscript{13/} Plaintiff argues Defendant's warnings are insufficient because they do not appear with the thumbnail images on the search result pages produced by the search engine. The Arriba Vista Web site only offered a warning if users clicked on a link to its "Copyright" page. This warning may arguably have been placed in the wrong place to deter some potential copyright infringers. But this does not necessarily mean Defendant "knew" or "should have known" for the purposes of a DMCA violation, especially since Plaintiff offers no evidence of any actual copyright infringement about which Defendant "should have known."
Plaintiff's copyrights. Defendant warns its users about the possibility of use restrictions on the images in its index, and instructs them to check with the originating Web sites before copying and using those images, even in reduced thumbnail form.

Plaintiff's images are vulnerable to copyright infringement because they are displayed on Web sites. Plaintiff has not shown users of Defendant's site were any more likely to infringe his copyrights, any of these users did infringe, or Defendant should reasonably have expected infringement.

There is no genuine issue of material fact requiring a trial on Plaintiff's DMCA claims, and summary adjudication is appropriate. The
Court finds there was no violation of DMCA § 1202. Defendant's motion is GRANTED and Plaintiff's motion is DENIED on the DMCA claim.

DATED: December ____, 1999.

__________________________
GARY L. TAYLOR
UNITED STATES DISTRICT JUDGE
GigaLaw.com: "Legal Information for Internet Professionals"

UMG Recordings, Inc., et al. v. MP3.com, Inc.
United States District Court, Southern District of New York
May 4, 2000

The complex marvels of cyberspatial communication may create difficult legal issues; but not in this case. Defendant's infringement of plaintiffs' copyrights is clear. Accordingly, on April 28, 2000, the Court granted defendant's motion for partial summary judgment holding defendant liable for copyright infringement. This opinion will state the reasons why.

The pertinent facts, either undisputed or, where disputed, taken most favorably to defendant, are as follows:

The technology known as "MP3" permits rapid and efficient conversion of compact disc recordings ("CDs") to computer files easily accessed over the Internet. See generally Recording Industry Ass'n of America v. Diamond Multimedia Systems Inc., 180 F.3d 1072, 1073-74 (9th Cir.1999). Utilizing this technology, defendant MP3.com, on or around January 12, 2000, launched its "My.MP3.com" service, which is advertised as permitting subscribers to store, customize and listen to the recordings contained on their CDs from any place where they have an Internet connection. To make good on this offer, defendant purchased tens of thousands of popular CDs in which plaintiffs held the copyrights, and, without authorization, copied their recordings onto its computer servers so as to be able to play the recordings for its subscribers.

Specifically, in order to first access such a recording, a subscriber to MP3.com must either "prove" that he already owns the CD version of the recording by inserting his copy of the commercial CD into his computer CD-ROM drive for a few seconds (the "Beam-it Service") or must purchase the CD from one of defendant's cooperating online retailers (the "Instant Listening Service"). Thereafter, however, the subscriber can access via the Internet from a computer anywhere in the world the copy of plaintiffs' recording made by defendant. Thus, although defendant seeks to portray its service as the "functional equivalent" of storing its subscribers' CDs, in actuality defendant is re-playing for the subscribers converted versions of the recordings it copied, which it then offers for public distribution. (It should be noted that the original CDs are not any longer available to consumers.)

SEE ALSO
- Behind the Music Files: The MP3 Legal Controversy
- Free E-Enter you
- Giga
- Sul
- Have you your con ever bee involved name dis
- Vote
- Fr
- Discu
- "Persona on the In
- Join ti
- adv
- 30: Cred
- 11/26/00
without authorization, from plaintiffs' copyrighted CDs. On its face, this makes out a presumptive case of infringement under the Copyright Act of 1976 ("Copyright Act"), 17 U.S.C. § 101 et seq. See, e.g., Castle Rock Entertainment, Inc. v. Carol Publishing Group, Inc., 150 F.3d 132, 137 (2d Cir. 1998); Hasbro Bradley, Inc. v. Sparkle Toys, Inc., 780 F.2d 189, 192 (2d Cir. 1985). 1

1 Defendant's only challenge to plaintiffs' prima facie case of infringement is the suggestion, buried in a footnote in its opposition papers, that its music computer files are not in fact "reproductions" of plaintiffs' copyrighted works within the meaning of the Copyright Act. See, e.g., 17 U.S.C. § 114(b). Specifically, defendant claims that the simulated sounds on MP3-based music files are not physically identical to the sounds on the original CD recordings. See Def.'s Consolidated Opp. to Pls.' Motions for Partial Summ. J. at 13-14 n.9. Defendant concedes, however, that the human ear cannot detect a difference between the two. Id. Moreover, defendant admits that a goal of its copying is to create a music file that is sonically as identical to the original CD as possible. See Goodman Reply Aff., Robertson Dep., Ex. A, at 85. In such circumstances, some slight, humanly undetectable difference between the original and the copy does not qualify for exclusion from the coverage of the Act.

Defendant argues, however, that such copying is protected by the affirmative defense of "fair use." See 17 U.S.C. § 107. In analyzing such a defense, the Copyright Act specifies four factors that must be considered: "(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." Id. Other relevant factors may also be considered, since fair use is an "equitable rule of reason" to be applied in light of the overall purposes of the Copyright Act. Sony Corporation of America v. Universal City Studios, Inc., 464 U.S. 417, 448, 454 (1984); see Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 549 (1985).

Regarding the first factor -- "the purpose and character of the use" -- defendant does not dispute that its purpose is commercial, for while subscribers to My.MP3.com are not currently charged a fee, defendant seeks to attract a sufficiently large subscription base to draw advertising and otherwise make a profit. Consideration of the first factor, however, also involves inquiring into whether the new use essentially repeats the old or whether, instead, it "transforms" it by infusing it with new meaning, new understandings, or the like. See, e.g., Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994); Castle Rock, 150 F.3d at 142; See also Pierre N. Leval, "Toward a Fair Use Standard," 103 Harv. L. Rev. 1105, 111 (1990). Here, although defendant recites that My.MP3.com provides a transformative "space shift" by which subscribers can enjoy the sound recordings contained on their CDs without juggling around the physical discs themselves, this is
CDs without logging around the physical cases themselves, this is simply another way of saying that the unauthorized copies are being retransmitted in another medium -- an insufficient basis for any legitimate claim of transformation. See, e.g., Infinity Broadcast Corp. v. Kirkwood, 150 F.3d 104, 108 (2d Cir.1998) (rejecting the fair use defense by operator of a service that retransmitted copyrighted radio broadcasts over telephone lines); Los Angeles News Serv. v. Reuters Television Int'l Ltd., 149 F.3d 987 (9th Cir.1998) (rejecting the fair use defense where television news agencies copied copyrighted news footage and retransmitted it to news organizations), cert. denied, 525 U.S. 1141 (1999); see also American Geophysical Union v. Texaco Inc., 60 F.3d 913, 923 (2d Cir.), cert dismissed, 516 U.S. 1005 (1995); Basic Books, Inc. v. Kinko's Graphics Corp., 758 F.Supp. 1522, 153031 (S.D.N.Y.1991); see generally Leval, supra, at 1111 (repetition of copyrighted material that "merely repackages or republishes the original" is unlikely to be deemed a fair use).

Here, defendant adds no new "new aesthetics, new insights and understandings" to the original music recordings it copies, see Castle Rock, 150 F.3d at 142 (internal quotation marks omitted), but simply repackages those recordings to facilitate their transmission through another medium. While such services may be innovative, they are not transformative. 2

2 Defendant's reliance on the Ninth Circuit's "reverse engineering" cases, see Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir.2000); Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527 (9th Cir.1993), is misplaced, because, among other relevant distinctions, those cases involved the copying of software in order to develop a new product, see Sony Computer Entertainment, 203 F.3d at 606; Sega Enterprises, 977 F.2d at 1522, whereas here defendant copied CDs onto its servers not to create any new form of expression but rather to retransmit the same expression in a different medium.

Regarding the second factor -- "the nature of the copyrighted work" -- the creative recordings here being copied are "close[] to the core of intended copyright protection," Campbell, 510 U.S. at 586, and, conversely, far removed from the more factual or descriptive work more amenable to "fair use," see Nihon Keizai Shimbun, Inc. v. Comline Business Data, Inc., 166 F.3d 65, 72-73 (2d Cir.1999); see also Castle Rock, 150 F.3d at 143-44.

Regarding the third factor -- "the amount and substantiality of the portion [of the copyrighted work] used [by the copier] in relation to the copyrighted work as a whole" -- it is undisputed that defendant copies, and replays, the entirety of the copyrighted works here in issue, thus again negating any claim of fair use. See Infinity Broadcast, 150 F.3d at 109 ("[T]he more of a copyrighted work that is taken, the less likely the use is to be fair...."); see generally Leval, supra, at 1122 ("[T]he larger the volume... of what is taken, the greater the affront to the interests of the copyright owner, and the less likely that a taking will qualify as a fair use.").
Regarding the fourth factor -- "the effect of the use upon the potential market for or value of the copyrighted work" -- defendant's activities on their face invade plaintiffs' statutory right to license their copyrighted sound recordings to others for reproduction. See 17 U.S.C. § 106. Defendant, however, argues that, so far as the derivative market here involves is concerned, plaintiffs have not shown that such licensing is "traditional, reasonable, or likely to be developed." American Geophysical, 60 F.3d at 930 & n.17. Moreover, defendant argues, its activities can only enhance plaintiffs' sales, since subscribers cannot gain access to particular recordings made available by MP3.com unless they have already "purchased" (actually or purportedly), or agreed to purchase, their own CD copies of those recordings.

Such arguments -- though dressed in the garb of an expert's "opinion" (that, on inspection, consists almost entirely of speculative and conclusory statements) -- are unpersuasive. Any allegedly positive impact of defendant's activities on plaintiffs' prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs' copyrighted works. See Infinity Broadcast, 150 F.3d at 111. This would be so even if the copyrightholder had not yet entered the new market in issue, for a copyrightholder's "exclusive" rights, derived from the Constitution and the Copyright Act, include the right, within broad limits, to curb the development of such a derivative market by refusing to license a copyrighted work or by doing so only on terms the copyright owner finds acceptable. See Castle Rock, 150 F.3d at 145-46; Salinger v. Random House, Inc., 811 F.2d 90, 99 (2d Cir.), cert. denied, 484 U.S. 890 (1987). Here, moreover, plaintiffs have adduced substantial evidence that they have in fact taken steps to enter that market by entering into various licensing agreements. See, e.g., Forrest R. Aff., Ex. F., Vidich Dep. at 61-63; id., Ex. N; Goodman R. Aff., Ex. B., Silver Dep. at 64-65; id., Ex. D, Eisenberg Dep. at 13032; id., Ex. E., Evans Dep. 145-48.

Finally, regarding defendant's purported reliance on other factors, see Campbell, 510 U.S. at 577, this essentially reduces to the claim that My.MP3.com provides a useful service to consumers that, in its absence, will be served by "pirates." Copyright, however, is not designed to afford consumer protection or convenience but, rather, to protect the copyrightholders' property interests. Moreover, as a practical matter, plaintiffs have indicated no objection in principle to licensing their recordings to companies like MP3.com; they simply want to make sure they get the remuneration the law reserves for them as holders of copyrights on creative works. Stripped to its essence, defendant's "consumer protection" argument amounts to nothing more than a bald claim that defendant should be able to misappropriate plaintiffs' property simply because there is a consumer demand for it. This hardly appeals to the conscience of equity.

In sum, on any view, defendant's "fair use" defense is indefensible and must be denied as a matter of law. Defendant's other affirmative defenses, such as copyright misuse, abandonment, unclean hands, and estoppel are essentially
frivolous and may be disposed of briefly. While defendant contends, under the rubric of copyright misuse, that plaintiffs are misusing their "dominant market position to selectively prosecute only certain online music technology companies," Def.'s Consolidated Opp. to Pls.' Motions for Summ.J. at 21, the admissible evidence of records shows only that plaintiffs have reasonably exercised their right to determine which infringers to pursue, and in which order to pursue them, cf. Broadcast Music, Inc. v. Peppermint Club, Inc., 1985 WL 6141, at *4 (N.D.Ohio Dec. 16, 1985). The abandonment defense must also fail since defendant has failed to adduce any competent evidence of an overt act indicating that plaintiffs, who filed suit against MP3.com shortly after MP3.com launched its infringing My.MP3.com service, intentionally abandoned their copyrights. See Richard Feiner & Co., Inc. v. H.R. Indus., Inc., 10 F.Supp.2d 310, 313 (S.D.N.Y.1998). Similarly, defendant's estoppel defense must be rejected because defendant has failed to provide any competent evidence that it relied on any action by plaintiffs with respect to defendant's My.MP3.com service. Finally, the Court must reject defendant's unclean hands defense given defendant's failure to come forth with any admissible evidence showing bad faith or misconduct on the part of plaintiffs. See generally Dunlop-McCullen v. Local 1-S, AFL-CIO-CLC, 149 F.3d 85, 90 (2d Cir.1998); A.H. Emery Co. v. Marcan Prods. Corp., 389 F.2d 11, 18 n.4 (2d Cir.), cert. denied, 393 U.S. 835 (1968). 3

3 The Court also finds no reason to alter or postpone its determination simply because of the recent filing of the complaint in Lester Chambers et al. v. Time Warner, Inc., et al., 00 Civ. 2839 (S.D.N.Y. filed Apr. 12, 2000) (JSR), the allegations of which, according to the defendant here, call into question the exclusivity of plaintiffs' copyrights. The allegations of a complaint, having no evidentiary value, cannot defeat a motion for summary judgment.

The Court has also considered defendant's other points and arguments and finds them sufficiently without merit as not to warrant any further comment.

Accordingly, the Court, for the foregoing reasons, has determined that plaintiffs are entitled to partial summary judgment holding defendant to have infringed plaintiffs' copyrights.
(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 regard 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 distinctive 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 domain name, is identical or confusingly similar to or dilutive of that mark; or

"(III) is a trademark, word, or name protected 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 (c)(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 (e); and

“(ii) the court finds that the owner—

“(I) is not able to obtain in personam jurisdiction 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 provided by the registrant to the registrar; and

“(bb) publishing notice of the action as the court may direct promptly after filing the action.

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

“(C) In an in rem action under this paragraph, a domain 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 substantially 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 prohibited by a contract between the registrant and the named person. The exception under this subparagraph 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-
ble 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-
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 regarding the disposition of the domain name, documents sufficient for the court to establish the court’s control and authority regarding the disposition of the registration and use of the domain 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 dilutive 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 by such registrant is not unlawful under this Act. The court may grant injunctive relief to the domain 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 electronic 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 REGISTRATION INVOLVING PERSONAL NAMES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Patent and Trademark Office and the Federal Election Commission, shall conduct a study and report to Congress with recommendations on guidelines and procedures for resolving disputes involving
cludes 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 Preser-
vation Act (16 U.S.C. 470a(a)(1)(A)) is amended by add-
ing at the end the following: "Notwithstanding section
43(c) of the Act entitled 'An Act to provide for the reg-
istration and protection of trademarks used in commerce,
to carry out the provisions of certain international conven-
tions, 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 (includ-
ing any defense under section 43(c)(4) of such Act or re-
lating to fair use) or a person's right of free speech or
expression under the first amendment of the United States
Constitution.
Notes:

1. This policy is now in effect. See www.icann.org/udrp/udrp-schedule.htm for the implementation schedule.

2. This policy has been adopted by all accredited domain-name registrars for domain names ending in .com, .net, and .org. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).

3. The policy is between the registrar (or other registration authority in the case of a country-code top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses "we" and "our" to refer to the registrar and it uses "you" and "your" to refer to the domain-name holder.

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 a 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.
Rules for Uniform Domain Name Dispute Resolution Policy

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

Note: These rules are now in effect. See 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 telexcopy 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."; and

(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.
U.S. 9th Circuit Court of Appeals

AYER Dennison v Sumpton
9855810

AYER 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.

OPINION
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.
OPINION

TROTT, 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. S 1125(c) (Supp. II 1996) (amending the Lanham Trademark Act of 1946, 15 U.S.C. SS 1051-1127 (1994)), and the California dilution statute, Cal. Bus. & Prof. Code S 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 <avery.net> and <dennison.net> 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. S 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 Leafer, 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"), maintains a database of registrations and translates entered domain-name combinations into Internet protocol addresses. When accessing a web site, a user enters the character string <http://www.>, 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 purposes. The combination also includes a second-level domain ("SLD"), which can be any word not already reserved in combination with the TLD. 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 format <alias@SLD.TLD>, with <alias> 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. Mailbank'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 combinations <avery.net> and <dennison.net>.

Avery Dennison sells office products and industrial fasteners 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 advertising its products, including those marketed under the separate "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 presence on the Internet, marketing its products at <avery.com>
and <averydennison.com>, 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

Trademark protection is "the law's recognition of the psychological function of symbols." Mishawaka Rubber & Woolen Mfg. Co. v. S.S. Kresge Co., 316 U.S. 203, 205 (1942). Two goals of trademark law are reflected in the federal scheme. On the one hand, the law seeks to protect consumers who have formed particular associations with a mark. On the other hand, trademark law seeks to protect the investment in a mark made by the owner. Qualitex Co. v. Jacobson Prod's Co., 514 U.S. 159, 163—64 (1995).

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 Krafte-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 "likelihood 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 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 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 830, 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. Schachter, The Rational 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 statutes, "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 24.01). 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 1378, 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, S 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 CodeS 14330. Accuride Int'l, Inc. v. Accuride Corp., 871 F.2d 1531, 1539 (9th Cir. 1989) (requiring more than mere distinctiveness).

Applying the fameousness 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.

1

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. 118, 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 meaning. 15 U.S.C. S 1052(e)(4), (f) (1994); Abraham Zohn Corp. v. Lebow, 751 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. Hirluck'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. § 1125(c)(1)(A) (referring to "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.

2

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. § 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, <teletech.com>. 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
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 of 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 trademark 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.

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. § 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 distinctiveness, 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 § 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 <avery.net> and <dennison.net> 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
tvalue of marks as marks." Panavision Int'l, I.P. v. Toeppe,
945 F. Supp. 1296, 1303 (C.D. Cal. 1996), aff'd , 141 F.3d
1316 (9th Cir. 1998). In our Panavision decision, we consid-
ered the defendant's "attempt to sell the trademarks
themseleves." 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 con-
sequent intent to capitalize on the surname status of "Avery"
and "Dennison." Appellants do not use trademarks qua trade-
marks 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 <avery.net> and <dennison.net> con-
stituted commercial use under the Federal Trademark Dilution
Act, and this essential element of the dilution causes of action
likewise mandates summary judgment for Appellants.

C

Dilution

The district court then considered the dilution requirement
under both statutes, holding that Appellants' use of
<avery.net> and <dennison.net> caused dilution, or a likely-
hood 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 judg-
ment for Avery Dennison.

Two theories of dilution are implicated in this case. First,
Avery Dennison argues that Appellants' conduct is the cyber-
squatting dilution that we recognized in Panavision. See 141
F.3d at 1326-27. Second, Avery Dennison argues that Appel-
lants' conduct in housing the <avery.net> and <dennison.net>
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
<trademark.com>. 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
1998)).

[18] In the instant case, Appellants registered the TLD
<.net>, rather than <.com>, with the SLDs <avery> and
<dennison>. 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 <trademark.com> 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 with a <trademark.net> 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) (<candyland.com> as a domain-name combination for a sexually explicit website diluted plaintiff’s trademark, “Candyland,” for a children’s game); 3 McCarthy, supra, S 24:104. The district court did not reach Avery Dennison’s claims regarding tarnishment.

[20] Avery Dennison offers, as an alternative ground for affirming the district court, the fact that Appellants house <avery.net> and <dennison.net> at the same website as lewd domain-name registrations. However, the evidence likewise indicates that to move from <avery.net> 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 Dennison's trademarks. 15 U.S.C. S 1125(c)(1); Cal. Bus. & 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 <avery.net> and <dennison.net> to be commercial use, and because genuine 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 attorney's fees. The Lanham Act permits an award of attorneys' fees to a prevailing party "in exceptional cases." 15 U.S.C. 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 <www.> 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 <http://wipo2.wipo.int>), we only consider <www.>, 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
The Children's Online Privacy Protection Act

H.R. 4328 - OMNIBUS APPROPRIATIONS BILL

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;

http://www.gseis.ucla.edu/iclp/coppa.htm 11/26/00
(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 worldwide 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--
(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—

(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;
(D) 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.

Return to Cyberspace Law & Policy Institute Home Page.

sb: 5Nov.1998
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 such information to a person who 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 homepage 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 homepage 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 homepage 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.

(e) 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
Internet Privacy Policies
By Eric Goldman, Esq.
Cooley Godward LLP, Palo Alto, CA

1. **What is a Privacy Policy?**
   - A privacy policy is a statement of a company’s practices with respect to the collection, use and disclosure of user information
   - User agreement vs. marketing representations

2. **Why Do a Privacy Policy?**
   - Best practices in the industry
   - Overcome an obvious privacy issue with your product/site
   - Comfort users with third party validation
   - Required by a potential advertiser (e.g., IBM, Microsoft, Intel) or site where you advertise (e.g., Disney)
   - You deal with kids under 13
   - You have European operations

3. **Why Are Privacy Policies Such a Pain to Do?**
   - The three-headed hydra of marketing, engineering and legal
   - There are no “off-the-shelf” forms
   - Policies are difficult to amend, so plan for the future
   - Multiple audiences: users, reporters, investors, judges, plaintiff lawyers, government enforcement agencies
   - FTC and TRUSTe rules are out of sync with state-of-the-art business practices
   - Companies actually get busted (GeoCities, Real Networks, Liberty Financial, ReverseAuction) and the remedies can REALLY hurt!!

4. **The FTC’s Latest: COPPA**
   - Takes effect April 21, 2000
   - Applies to sites (or portions thereof) that market to kids 12 and under or know that they are collecting information from kids 12 and under
   - The summary: don’t do it if you don’t have to!!
   - Requirements:
     (1) Post a privacy policy on the site
     (2) Obtain verifiable parental consent. If you are collecting personal information for internal marketing, you can use unauthenticated email. Otherwise, you need consent through mail, fax, toll-free phone number, credit card authentication, or authenticated email.
     (3) Allow parents to review the personal information collected
     (4) Give parents the opportunity to restrict collection/use of their kids’ information
     (5) Not condition participation in an activity on the kid disclosing more info than necessary
     (6) Have reasonable security procedures
   - Bottom line: compliance is likely to require significant changes to existing business practices.
5. **EUROPEAN UNION PRIVACY DIRECTIVE.**

- The directive took effect in October 1998, but not yet implemented in all member states.
- The general rule: obtain express consent for use and disclosure of personal information [not limited to Internet collection]
- Some states require registration, so you cannot comply merely through your privacy policy.
- If you have no *presence* in Europe, do you need to comply?
- Data sharing with EU-based companies is tricky.

6. **GRANDMA GOLDSSTEIN’S 15 STEP RECIPE FOR DEPLOYING PRIVACY POLICIES.**

**Step 1:** Determine why you are doing a policy and which audience is most important

**Step 2:** Determine if COPPA applies. If so, sell!!!

**Step 3:** Determine if the EU Directive applies. If so, call European counsel.

**Step 4:** Determine if you are going to use one or more third party validators
- Options include TRUSTe, BBBOnline and PWC’s BetterWeb
- These validators all have their own substantive rules

**Step 5:** Review your site
- Look for existing data collection points, and consider future ones
- Look for existing privacy policy-like language

**Step 6:** Review existing practices
- Look at existing obligations to turn data over to third parties
- Look for other places where personal data is turned over anyway (e.g., email delivery outsourcing)
- Look at ISP/hosting agreements
- Look for situations where you have voluntarily agreed to limit your use/disclosure of information (e.g., distribution agreements or sponsorships)

**Step 7:** Determine how the policy will become a binding user agreement

**Step 8:** Determine how the policy will be amended in the future

**Step 9:** Draft the policy and get internal/external blessing

**Step 10:** Train employees about the privacy policy

**Step 11:** Scrub the site to remove all contrary statements

**Step 12:** Upload the policy

**Step 13:** As applicable, follow the procedures to amend the existing policy

**Step 14:** Keep archives of prior policies and segregate databases as necessary

**Step 15:** Establish a procedure for handling site changes

---

About the Speaker: Eric Goldman (formerly Eric Schlachter) is an attorney practicing cyberspace law with Cooley Godward LLP, Palo Alto, CA. He also is an adjunct professor of Cyberspace Law at Santa Clara University School of Law. Cooley Godward’s web page is located at http://www.cooley.com, and Eric’s personal home page is located at http://members.theglobe.com/ericgoldman/. Eric can be reached at egoldman@cooley.com.
UNITED STATES BANKRUPTCY COURT  
DISTRICT OF MASSACHUSETTS  
eastern division  

In re:  

TOYSMART.COM, LLC, Debtor.  

Chapter 11  
Case No. 00-13995-CJK  

STIPULATION AND ORDER ESTABLISHING CONDITIONS ON SALE OF CUSTOMER INFORMATION  

This Stipulation is entered into this twentieth day of July, 2000, by and between,  
Toysmart.com, LLC, debtor and debtor-in-possession ("Debtor" or "Toysmart"), and the  
Federal Trade Commission ("FTC").\(^1\)  

WHEREAS, on June 9, 2000, an involuntary petition was commenced against the Debtor  
a consent to the order for relief under chapter 11 of the Code;  

WHEREAS, the Debtor is a Delaware limited liability corporation involved in the "e-tail"  
business. The Debtor has, among other things, advertised, promoted, and sold toys on the  
Internet including through its Web site www.toysmart.com;  

WHEREAS, the FTC is an independent agency of the United States government created  
pursuant to 15 U.S.C. § 41, et seq. ("FTC Act"). The FTC enforces § 5(a) of the FTC Act,  
which prohibits unfair or deceptive acts or practices in or affecting commerce;  

WHEREAS, the Debtor has collected personal customer information including, but not  
limited to, consumers' names, addresses, billing information, shopping preferences, and  
family profile information;  

WHEREAS, from at least September 1999 to July 2000, the Debtor's Web site included a  
privacy statement ("Privacy Statement") stating that (1) "Personal information voluntarily  
submitted by visitors to our site, such as name, address, billing information and shopping  
preferences, is never shared with a third party. All information obtained by toysmart.com  
is used only to personalize your experience online," and (2) "When you register with  
toysmart.com, you can rest assured that your information will never be shared with a third  
party;"  

WHEREAS, on or about May 22, 2000, the Debtor announced that it had ceased  
operations and began to offer for sale customer information through advertisements  
appearing in the Wall Street Journal and the Boston Globe and through its Web site;  

WHEREAS, on June 29, 2000, the Debtor filed the Debtor's Motion For Authority To Sell  
Assets (Excluding Inventory) By Public Sale Free And Clear Of Liens, Claims And
Encumbrances ("Sale Motion") and related pleadings. Pursuant to the Sale Motion, the Debtor, among other things, seeks to sell a group of assets set forth in Category C and entitled "Web Site Applications, Names, Customer List, and Product Databases" consisting of the Debtor's right, title and interest in customer information, including contents of its customer databases including detailed customer lists and related information, as well as names, trademarks, goodwill, URL names, Web site source code, and data base schemas without content and publishable content located on its Web site (each and together, the "Goodwill"); and

WHEREAS, the FTC has filed a complaint in the United States District Court for the District of Massachusetts, Federal Trade Commission v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS, which alleges that the proposed sale of the customer information would constitute a deceptive act or practice in or affecting commerce under § 5(a) of the FTC Act; and

WHEREAS, the Debtor disputes the FTC's allegations and further responds that it has never violated the Privacy Statement, but in any event, seeks to resolve this matter so as to preserve the value of the Debtor's assets for the benefit of its creditors.

NOW THEREFORE, in an effort to resolve this matter without further cost or delay, the parties hereby agree, subject only to the approval of this Court, as follows:

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

"Qualified Buyer" shall mean an entity that (1) concentrates its business in the family commerce market, involving the areas of education, toys, learning, home and/or instruction, including commerce, content, product and services, and (2) expressly agrees to be Toysmart's successor-in-interest as to the Customer Information, and expressly agrees to the obligations set forth in Paragraphs 2, 3 and 4, below. Nothing herein, however, shall create any liability for such Qualified Buyer as a result of any actions or omissions by the Debtor, as the Customer Information is to be sold free and clear of all liens, claims and encumbrances, except for the Qualified Buyer's obligations under the Privacy Statement.

"Customer Information" shall mean information of or relating to consumers collected by the Debtor, including, but not limited to, name, address, billing information, shopping preferences, order history, gift registry selection, family profile information about consumers' children, such as name, gender, birthday, and toy interests.

"Third Party" shall mean any individual, firm, or organization other than the Qualified Buyer and its successors, except to the extent that disclosure of Customer Information to such an individual, firm, or organization is necessary to maintain the technical functioning of the Toysmart Web site or customer databases, or to fulfill a consumer's request. "Third Party" includes any affiliates of the Qualified Buyer.

"Privacy Statement" shall mean the privacy statement posted on the Toysmart Web site from at least September 1999 to July 2000, the terms of which are included in full in Exhibit 1.
The Debtor shall only assign or sell its Customer Information as part of the sale of its Goodwill and only to a Qualified Buyer approved by the Bankruptcy Court. In the process of approving any sale of the Customer Information, the Bankruptcy Court shall require that the Qualified Buyer agree to and comply with the terms of this Stipulation.

The Qualified Buyer shall treat Customer Information in accordance with the terms of the Privacy Statement and shall be responsible for any violation by it following the date of purchase. Among other things, the Qualified Buyer shall use Customer Information only to fulfill customer orders and to personalize customers' experience on the Web site, and shall not disclose, sell or transfer Customer Information to any Third Party.

If the Qualified Buyer materially changes the Privacy Statement, prior notice will be posted on the Web site. Any such material change in policy shall apply only to information collected following the change in policy. The Customer Information shall be governed by the Privacy Statement, unless the consumer provides affirmative consent ("opt-in") to the previously collected information being governed by the new policy.

In the event that an order is not entered on or before July 31, 2001, approving the sale of the Customer Information to a Qualified Buyer or approving a plan of reorganization, the Debtor shall, on or before August 31, 2001, delete or destroy all Customer Information in its possession, custody or control, and provide written confirmation to the FTC, sworn to under penalty of perjury, that all such Customer Information has been deleted or destroyed. Pending approval of any sale of the Customer Information to a Qualified Buyer or of a plan of reorganization, the Debtor shall handle Customer Information in accordance with the Privacy Statement.

This Stipulation and Order, after approval by the Bankruptcy Court, shall be attached to and incorporated in full into the terms of any plan of liquidation or reorganization that is ultimately approved in this bankruptcy case.

FEDERAL TRADE COMMISSION
Debra A. Valentine,
General Counsel,
Federal Trade Commission

Of Counsel:
Jeanne M. Crouse
Counsel for Bankruptcy & Redress
Washington, DC 20580
(202) 326-3312

Laura Mazzarella
Ellen Finn
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
(202) 326-3424/(202) 326-3296

By its Attorneys,
Harold B. Murphy (BBO #567781)
Alex M. Rodolakis (BBO #567781)
Hanify & King
One Federal Street
Boston, MA 02110

David N. Lord
Chief Executive Officer

TOYSMART.COM, LLC

http://www.ftc.gov/os/2000/07/toysmartbankruptcy.1.htm 11/26/00
Boston, MA 02110
(617) 423-0400

IT IS SO ORDERED.

Entered at Boston, Massachusetts, this ___ day of July, 2000.

Honorable Carol J. Kenner
United States Bankruptcy Judge

EXHIBIT 1

PRIVACY STATEMENT

Our promise

At toysmart.com, we take great pride in our relationships with our customers and pledge to maintain your privacy while visiting our site. Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by toysmart.com is used only to personalize your experience online. This information is received via the following areas of our site: My toysmart and the Gift Center. When you place additional orders, our site will update your order history, which you can view in My toysmart. If you sign up for the gift registry, information you submit will be added to your personal profile. Other than these two instances, the information that you provide us is not supplemented in any way.

Your option

If you do not wish to receive emails containing promotional offers or contests from toysmart.com, please click the box located at the bottom of the "My toysmart" registration page. If you are already registered and would like to opt-out of such promotional offers, please go to "My toysmart," click on the "My Profile" icon, and unselect the email option located at the bottom of the page. When you register with toysmart.com, you can rest assured that your information will never be shared with a third party.

Editing your personal information

If you would like to edit your personal information, please click on the "My toysmart" button located on the top of our homepage. Then, simply click on the "My Profile" icon and update any of your information.

Contests

toysmart.com is committed to protecting the privacy of all children who enter contests on our site. We request only the child's first name and age be sent with the contest entry. We email every child’s parent with notification that his or her child has entered the contest. Only winners' parents will be sent a release form, which requests a shipping address as well a permission request to post the winning entry on our site. No entries will be posted without a parent or guardian's permission, and no prizes will be sent without written consent from the parent or guardian.

Your information is safe with us!

All personal information is encrypted on a separate server. Also, we give you the option of further securing your information with the use of a password. To create a personal password, simply go to "My toysmart." Shopping with toysmart.com is guaranteed to be 100% safe. That means we will guarantee your protection against any liability if unauthorized charges are made to your card as a result of shopping at toysmart.com. Simply stated, you are guaranteed a safe and secure transaction every time you shop with us. Visit our
Questions regarding this statement should be directed to support@toysmart.com.

1. The FTC assents to this Court's jurisdiction solely for purposes of approval of this Stipulation. Should this Stipulation not be approved by the Bankruptcy Court, the FTC reserves the right to take all actions as it deems necessary and appropriate to protect its exercise of police and regulatory powers.
the CDA's heavy burden on adult speech. Although such verification is actually being used by some
commercial providers of sexually explicit material, the District Court's findings indicate that it is not
economically feasible for most noncommercial speakers. Pp. 35-37.

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

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

929 F. Supp. 824, affirmed.

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

NOTICE: This opinion is subject to formal revision before publication in the preliminary print of the United States
Reports. Readers are requested to notify the Reporter of Decisions, Supreme Court of the United States, Washington, D. C.
20544, 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 addressees. 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."\textsuperscript{6} It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."\textsuperscript{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."\textsuperscript{8} Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text--sometimes images.

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

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals.\textsuperscript{9} Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web."\textsuperscript{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."\textsuperscript{11} These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community."\textsuperscript{12} Thus, for example,

"when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing--wherever Internet users live. Similarly, the safer
sex instructions that Critical Path posts to its Web site, written in street language so that the
teenage receiver can understand them, are available not just in Philadelphia, but also in Provo
and Prague." 13

Some of the communications over the Internet that originate in foreign countries are also sexually
explicit. 14

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

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

Age Verification

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

Technology exists by which an operator of a Web site may condition access on the verification of
requested information such as a credit card number or an adult password. Credit card verification is
only feasible, however, either in connection with a commercial transaction in which the card is used,
or by payment to a verification agency. Using credit card possession as a surrogate for proof of age
would impose costs on non commercial Web sites that would require many of them to shut down. For
that reason, at the time of the trial, credit card verification was "effectively unavailable to a substantial
number of Internet content providers." Id., at 846 (finding 102). Moreover, the imposition of such a
requirement "would completely bar adults who do not have a credit card and lack the resources to
obtain one from accessing any blocked material." 22
Commercial pornographic sites that charge their users for access have assigned them passwords as a method of age verification. The record does not contain any evidence concerning the reliability of these technologies. Even if passwords are effective for commercial purveyors of indecent material, the District Court found that an adult password requirement would impose significant burdens on noncommercial sites, both because they would discourage users from accessing their sites and because the cost of creating and maintaining such screening systems would be "beyond their reach." 23

In sum, the District Court found:

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

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). 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 Presidentsigned 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, the two cases were consolidated, and a three judge District Court was convened pursuant to §561 of the Act. 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 four 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 its definition of material that is harmful to minors with the requirement that it be "utterly without redeeming social importance for minors." Id., at 646. The CDA fails to provide us with any definition of the term "indecent" as used in §223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by §223(d) lack serious literary, artistic, political, or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, in applying to all those under 18 years, includes an additional year of those nearest majority.

In Pacifica, we upheld a declaratory order of the Federal Communications Commission, holding that the broadcast of a recording of a 12-minute monologue entitled "Filthy Words" that had previously been delivered to a live audience "could have been the subject of administrative sanctions." 438 U.S., at 730 (internal quotations omitted). The Commission had found that the repetitive use of certain words referring to excretory or sexual activities or organs "in an afternoon broadcast when children are in the audience was patently offensive" and concluded that the monologue was indecent "as broadcast." Id., at 735. The respondent did not quarrel with the finding that the afternoon broadcast was patently offensive, but contended that it was not "indecent" within the meaning of the relevant statutes because it contained no prurient appeal. After rejecting respondent's statutory arguments, we confronted its two constitutional arguments: (1) that the Commission's construction of its authority to ban indecent speech was so broad that its order had to be set aside even if the broadcast at issue was unprotected; and (2) that since the recording was not obscene, the First Amendment forbade any 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 case 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 "almost 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 "as many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." 34 This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought." 929 F. Supp., at 842 (finding 74). We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," 47 U. S. C. A. §223(a) (Supp. 1997), while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs," §223(d). Given the absence of a definition of either term, 35 this difference in language will provoke uncertainty among speakers about how the two standards relate to each other 36 and just what they mean. 37 Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our 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 the statute is no more vague than the obscenity standard this Court established in Miller v. California, 413 U.S. 15 (1973). But that is not so. In Miller, this Court reviewed a criminal conviction against a commercial vendor who mailed brochures containing pictures of sexually explicit activities to individuals who had not requested such materials. Id., at 18. Having struggled for some time to establish a definition of obscenity, we set forth in Miller the test for obscenity that controls to this day:

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

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

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

The Government's reasoning is also flawed. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague. 38 Each of Miller's additional two prongs--(1) that, 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 "red[c]e the adult population . . . to . . . only what is fit for children." Denver, 518 U. S., at ___ (slip op., at 29) (internal quotation marks omitted) (quoting Sable, 492 U.S., at 128). 40 "[R]egardless of the strength of the government's interest" in protecting children, "[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox." Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 74-75 (1983).

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

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult to adult communication. The findings of the District Court make clear that this premise is untenable.

Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100 person chat group will be minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults. 42
The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms. 929 F. Supp., at 845 (findings 90-94). As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial—as well as some commercial—speakers who have Web sites to verify that their users are adults. Id., at 845-848 (findings 95-116). 43 These limitations must inevitably curtail a significant amount of adult communication on the Internet. By contrast, the District Court found that "[d]espite its limitations, currently available user based software suggests that a reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children will soon be widely available." Id., at 842 (finding 73) (emphasis added).

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

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

The breadth of this content based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so. The arguments in this Court have referred to possible alternatives such as requiring that indecent material be "tagged" in a way that facilitates parental control of material coming into their homes, making exceptions for messages with artistic or educational value, providing some tolerance for parental choice, and regulating some portions of the Internet—such as commercial web sites—differently than others, such as chat rooms. Particularly in the light of the absence of any detailed findings by the Congress, or even hearings addressing the special problems of the CDA, we are persuaded that the CDA is not narrowly tailored if that requirement has any meaning at all.
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 fallback 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. 434, 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.

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 ("specificperson" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in a[n] manner available" to minors ("display" provision). §223(d)(1)(B). None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech. Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment"). Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. See S. Conf. Rep. No. 104-230, p. 189 (1996) (CDA imposes "access restrictions . . . to protect minors from exposure to indecent material").

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults. 1 States have also denied minors access to speech deemed to be "harmful to minors." 2 The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the Court, however, I would invalidate the provisions only in those circumstances.

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no
right to obtain—it interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population . . . to reading only what is fit for children." Butler v. Michigan, 352 U.S. 380, 383 (1957). The First Amendment does not tolerate such interference. See id., at 383 (striking down a Michigan criminal law banning sale of books—to minors or adults—that contained words or pictures that "tende[d] to . . . corrup[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 reasonably assure 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). Appellants urge 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 right 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]hsoever...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]hsoever...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 the rights of adults are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained. The Court reaches a contrary conclusion, and from that holding that I respectfully dissent.

Footnotes
[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; Bibliobbytes; 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) (Levanthal, J., dissenting), rev'd, FCC v. Pacifica Foundation, 438 U.S. 726 (1978). When Pacifica was decided, given that radio stations were allowed to operate only pursuant to federal license, and that Congress had enacted legislation prohibiting licensees from broadcasting indecent speech, there was a risk that members of the radio audience might infer some sort of official or societal approval of whatever was heard over the radio, see 556 F. 2d, at 37, n. 18. No such risk attends messages received through the Internet, which is not supervised by any federal agency.

[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 (Determinations of "what appeals to the `prurient interest' or is 'patently offensive'. . . . are essentially questions of fact, and our Nation is simply too big and too diverse for this Court to reasonably expect that such standards could be articulated for all 50 States in a single formulation, even assuming the prerequisite consensus exists"). The CDA, which implements the "contemporary community standards" language of Miller, thus conflicts with the Conferees' own assertion that the CDA was intended "to establish a uniform national standard of content regulation." S. Conf. Rep., at 191.


[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 themessage 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 be detained and who should be set at large. This would, to some extent, substitute the judicial for the legislative department of the government." United States v. Reese, 92 U.S. 214, 221 (1876). In part because of these separation of powers concerns, we have held that a severability clause is "an aid merely; not an inexorable command." Dorcy v. Kansas, 264 U.S. 286, 290 (1924).

[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").


Sec. 1030. Fraud and related activity in connection with computers

- (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; [1]

(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 [2]

(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;

(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

(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),

() The United States Secret Service shall, in addition to any 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

- (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 [7]

- (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;
  - (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 the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

Footnotes

[1] So in original. Probably should be followed by "or".
[2] So in original. The word "and" probably should not appear.
[3] So in original. Probably should be followed by "and".
[4] So in original. The "; and" probably should be a period.
[6] So in original. The period probably should be a semicolon.
[7] So in original. The word "and" probably should not appear.
UNIVERSAL STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

-------------------------------

AMERICA ONLINE, INC.,

Plaintiff,

-against-

THE CHRISTIAN BROTHERS and

JASON VALE,

Defendants.

-------------------------------

98 Civ. 8959 (DAB)(HBP)

REPORT AND

RECOMMENDATION

PITMAN, United States Magistrate Judge:

TO THE HONORABLE DEBORAH A. BATTs, United States District Judge,

I. Introduction

On June 8, 1999, the Honorable Deborah A. Batts, United States District Judge for the Southern District of New York, entered a default judgment against defendants The Christian Brothers and Jason Vale (collectively "The Defendants") and referred the matter to me to conduct an inquest and to report and recommend concerning the amount of damages to be awarded to plaintiff America Online, Inc. ("AOL") and AOL's application for a permanent injunction. The default judgment was entered as a result of The Defendants' failure to answer or move against the complaint.

Pursuant to the Order of Reference, I issued a Scheduling Order on July 6,
1999, directing AOL to serve and file proposed findings of fact and conclusions of law by July 23, 1999 and directing The Defendants to submit responsive materials by August 25, 1999. My July 6 Scheduling Order further provided:

IF DEFENDANTS (1) FAIL TO RESPOND TO PLAINTIFF'S SUBMISSIONS, OR (2) FAIL TO CONTACT MY CHAMBERS BY AUGUST 25, 1999 AND REQUEST AN IN-COURT HEARING, IT IS MY INTENTION TO ISSUE A REPORT AND RECOMMENDATION CONCERNING BOTH DAMAGES AND PLAINTIFF'S REQUEST FOR A PERMANENT INJUNCTION ON THE BASIS OF PLAINTIFF'S WRITTEN SUBMISSIONS ALONE WITHOUT AN IN-COURT HEARING. See Transatlantic Marine Claims Agency, Inc. v. Ace Shipping Corp., 109 F.3d 105, 111 (2d Cir. 1997); Fustok v. ContiCommodity Services Inc., 873 F.2d 38, 40 (2d Cir. 1989) ("[t]he [i]ssue [n]ot necessary for the District Court to hold a hearing, as long as it ensured that there was a basis for the damages specified in the default judgment.")

(Emphasis in original).

Copies of my July 6 Scheduling Order were sent to counsel for AOL and to The Defendants directly since The Defendants are not represented by counsel. No copies of my July 6 Scheduling Order were returned as undeliverable.

In response to a request from AOL, by Order dated July 16, 1999, I extended AOL's time for making its submission to August 23, 1999 and extended The Defendants' time for making their responsive submission to September 23, 1999. My July 16 Order contained the same notice set forth above and was mailed to The Defendants directly. No copies of my July 16 Order have been returned as undeliverable.

AOL timely submitted proposed findings of fact and conclusions of law, supported by affidavits and declarations from individuals with knowledge of the underlying facts and numerous documentary exhibits. The Defendants have not appeared and have not responded to either of my Scheduling Orders in any way.

Since The Defendants have not responded to plaintiff's submissions in any way, I respectfully recommend, on the basis of AOL's written submissions, that the Court make the following findings of fact and conclusions of law.

II. Findings of Fact

A. The Parties

1. AOL, a Delaware corporation with its principal place of business in Dulles, Virginia, owns and operates a proprietary, content-based online service which affords its members access to the Internet and the capability to send and receive e-mail with other AOL members and with non-AOL members over the Internet. AOL's computer systems, which include specialized
computers ("servers") to process electronic messages, are located in the Commonwealth of Virginia (Complaint 5 (Footnote 1)).

2. Defendant The Christian Brothers is an unincorporated entity or association located and operating out of 151-47 18th Avenue, Whitestone, New York 11357 (Complaint 8).

3. Defendant Jason Vale is the principal of The Christian Brothers, and is a citizen of New York, residing at 151-47 18th Avenue, Whitestone, New York 11357 (Complaint 9).

4. Defendants operate and transact business, or have operated and transacted business, from numerous InterNIC-registered Internet domains, including the following: "laetrile.net"; "amygdalin.net"; "heavenlyhealing.com"; "christianbrothers.com"; "apricotsfromgod.com"; "canceranswer.com"; "naturalhealings.com"; "juicenoni.net"; "amygdalin.com"; "eatseeds.com" (Complaint 10; Declaration of Ivan Histand, dated August 19, 1999, ("Histand Dec."), 10).

5. The Defendants jointly operate and transact business within the aforementioned domains, acting in concert with one another and with third-party contractors and/or agents unknown to plaintiff AOL (Complaint 11).

B. AOL's E-Mail System

6. The Defendants committed the acts complained of herein through their use of the electronic messaging capabilities of the Internet. The Internet is a complex "network of networks" that interconnects innumerable smaller groups of linked computers. All of the networks comprising the Internet are connected in a manner that permits any computer on the Internet to communicate with any other computer on the Internet (Complaint 16).

7. E-mail consists of text messages sent electronically from one computer user to another over the Internet. The Internet makes it possible for a user rapidly to exchange e-mail messages with other Internet users in the United States and abroad. E-mail can be sent virtually instantaneously from one individual to another, or from an individual user to a large group of addresses. The Internet's e-mail functionality makes it possible for a sender to transmit simultaneously tens and even hundreds of thousands of copies of a single message (Complaint 18).

8. AOL allows its Members to exchange e-mail messages over the Internet with any other e-mail user in the world who has an Internet e-mail address. Members can exchange e-mail messages at no additional charge. AOL has offered this service under its well-known service mark, trade name and trademark, "AOL." To become an AOL member, one installs a copy of AOL's proprietary software on one's personal computer and opens an account with AOL. Thereafter, members are allowed to use the AOL service according to the service agreement ("Membership Agreement," annexed as Exhibit 1 to the Declaration of Carrie F. Davis, dated August 20, 1999 ("Davis Dec.") to which all new members must agree at the time they open a new account. AOL members either pay a flat monthly fee or a per-usage fee for AOL services (Complaint 27).

9. Under the Membership Agreement, AOL members are specifically prohibited from sending unsolicited commercial bulk e-mail, also known as "spam," and from using their membership to harvest or collect any information, including the user names or the e-mail addresses, of other AOL members. AOL will terminate the account of any AOL member who violates
the Membership Agreement. The Membership Agreement expressly reserves AOL’s right to block unsolicited e-mail sent to its members from the Internet, even if the mail is sent by non-members (Complaint 28).

10. AOL’s e-mail system was created solely for the benefit of AOL members, who pay the prescribed fees and who agree to adhere to AOL’s Membership Agreement. The e-mail system is operated through dedicated servers located at AOL’s headquarters in Dulles, Virginia, that store and route e-mail messages between AOL’s members. AOL permits its members to use the "aol.com" domain name which, when combined with a unique user name, gives each member a distinctive e-mail address from which to exchange e-mail with Internet users (e.g., "member38@aol.com") (Complaint 29).

11. AOL has registered the domain name "aol.com" with the InterNIC, a consortium run by the National Science Foundation responsible for assigning the unique addresses used by computers to communicate through the Internet. Domain names function as convenient shorthand for users of the Internet, giving Internet users the option of using readily understandable proper names to identify themselves and their communications. Businesses, for example, typically are assigned by the InterNIC domain names with the ".com" designation (e.g., "Brandy.com"), while educational and governmental organizations usually are assigned ".edu" and ".gov" domain names (e.g., "topuniversity.edu" and "federalagency.gov"). AOL’s domain name is used extensively in commerce and is recognized worldwide as a source identifier of AOL’s online services (Complaint 6, 20).

12. An e-mail address, for example, "johnsmith@aol.com", consists of two components: the user name, and the domain name. The component before the symbol "@" is the account name and specifies the individual sending or receiving the message. The component after the "@" symbol is the Internet domain name, which indicates the e-mail provider used by the individual to transmit and receive messages (e.g., "jdoe@company.com") (Complaint 21).

13. E-mail messages also contain "headers" generated by the sender’s Internet Service Provider ("ISP"), which identifies the sender’s return e-mail address, the message’s "subject," and other information related to the transmission of the e-mail message (such as the date, time and routing information). AOL’s system is configured such that these "headers" are excerpts at the beginning of each message and appear in full text at the conclusion of the message (Complaint 22).

14. It is possible for an e-mail sender to override his or her computer’s automatic system and deliberately change the information contained in the message’s header. E-mail senders may also purchase various software programs whose function is to alter e-mail header information. Changing information in the header of an e-mail message can disguise the true identity and location of the sender so that the recipient would believe that a different party and/or e-mail provider actually sent the message, and to otherwise circumvent filtering systems designed to block unwanted e-mail. Various "stealth" software programs, designed for and marketed to the senders of junk e-mail, facilitate the falsification of e-mail header information in mass mailings (Complaint 26).

C. The Strength of AOL’s Mark

15. AOL has used the initials "AOL" as a trademark and a service mark in various forms and styles, continuously in commerce to identify its products and services since October 1989. This mark was registered on July 2, 1996 as a trademark upon the Principal Register of the United States Patent and
Trademark Office as United States Registration No. 1,984,337. The mark was also registered on June 4, 1996 as a service mark upon the Principal Register of the PTO as United States Registration No. 1,977,731 (Complaint 6-7).

16. AOL has spent hundreds of millions of dollars on advertising, direct marketing, and public relations that incorporate and promote brand identification, including identification with AOL's Registered Marks, "AOL" and "America Online." By virtue of AOL's use and promotion of the Registered Marks, they have become valuable business assets. The Registered Marks are used and recognized throughout the United States and worldwide in association with AOL's online products and services. Approximately 89% of adults in this country are familiar with one or more the Registered Marks (Declaration of Rande Price, dated August 23, 1999 ("Price Decl."), 3).

17. AOL licenses the use of the Registered Marks in connection with services such as the AOL Long Distance Savings Plan and the America Online VISA Card (Price Decl. 4).

D. The Defendants' Bulk E-Mailing Practices

18. Since 1997, The Defendants have unlawfully obtained mailing lists of AOL members' e-mail addresses and repeatedly transmitted, at virtually no cost to The Defendants, over twenty million messages -- and up to hundreds of thousands of messages per hour -- across the Internet through AOL's computers and computer networks to AOL's members (Complaint 30).

19. The Defendants' promotional e-mails tout medical literature concerning a laetrile "cure" for cancer, and offer to sell laetrile itself. The e-mails often state, "If you would like to be brought to the most informative Web site on the Internet concerning cancer and the simple known answer, click on the following blue link." The e-mail then states "Click here and you'll automatically be brought to the Web site www.amygdaлин.net" (Complaint 31).

20. Another version of The Defendants' unsolicited bulk e-mail states:

   The answer to cancer has been known [sic] for years. This website proves that eating inexpensive apple seeds and/or apricot seeds completely cure [sic] most cancers. The theory also states that by eating just a few seeds per day will 99.95% guarantee that you will never develop cancer.

   Click on the link below to be brought to the site.

   www.vitaminb17.com

   Sincerely, Jason

   (Complaint 32).

21. A third variety of The Defendants' bulk e-mail states:

   The answer to cancer has been known for years.
   . . click below for more info.
(Complaint 33).

22. The header of these three variations of The Defendants' e-mail state that the e-mail was sent by someone at "aol.com." These headers are completely fraudulent, as these e-mails were never generated by AOL or an AOL customer. Thus, these headers falsely attribute the transmission of these e-mails to AOL (Complaint 34).

23. The Defendants' promotional messages regarding their "cancer cures" typically direct recipients to a Web site where additional information regarding the product is located. Through that Web site the user is able to purchase, among other things, laetrile, a videotape and a book promoting The Defendants' advice regarding cancer treatment (Complaint 35). 100 tablets of laetrile costs $34.00, the videotape and book together are sold for $40.00, and various other products sell for between $139.00 to $450.00 (Declaration of Jeffrey Ellender, dated August 23, 1999 ("Ellender Dec."), Ex. 2).

24. AOL has undertaken various technical efforts to permit its members to opt out of receiving messages from domains and IP addresses that are or have been the subject of member complaints regarding unsolicited bulk e-mail. These methods, however, rely on truthful e-mailing practices to be successful. When senders such as The Defendants mail from multiple and varying domains, employ random and varying user names, relay their messages through the servers of innocent third parties, or falsify the headers on their e-mails to indicate that their messages are from domains that AOL does not filter (e.g., "msn.com" or "aol.com"), AOL's computers and computer system cannot detect and filter the unsolicited bulk e-mail (Complaint 49).

25. The Defendants have engaged in deceptive practices to frustrate AOL's and its members' ability to filter The Defendants' junk mailings. The Defendants have increased the number of their registered domains and employed a shifting combination of random user names, domains, and IP addresses from which to transmit their promotional messages for the purpose and with the effect of evading AOL's efforts to identify incoming junk mail and block the messages before they are delivered (Complaint 37).

26. The Defendants also intentionally forge the headers in the electronic return addresses of their e-mail messages to conceal the domains from which they operate and transmit their e-mail. Often The Defendants use the domain name "aol.com." The purpose and effect of these practices is to prevent AOL from using technical means to block the unsolicited e-mail messages before they are delivered (Complaint 38).

27. The Defendants' incorporation of AOL's registered mark and domain name in the return addresses of their messages also creates the false and damaging misconception among the AOL members who receive these messages that AOL endorses or condones The Defendants' unsolicited bulk e-mail practices and the dubious cancer cure that they promote. Indeed, one of the member complaints received by AOL states "I can't do anything about these spams coming from AOL" (Complaint 39, Exhibit F). Moreover, The Defendants' use of forged "aol.com" header information is a misappropriation of AOL's domain name and registered mark (Complaint 39).

28. In addition, The Defendants have opened several AOL accounts, from which they transmit spam and harvest user names and addresses of AOL members in violation of the Membership Agreement (Complaint 60).
activity has the same effect as falsely generating the "aol.com" designation - it makes AOL members think that AOL either generates or approves of the spam.

E. Defendants Have Continued Their Unlawful Activity

Even After Receiving Notice From Both AOL

And The Court That Their Activity Was Unlawful

29. The Defendants have continued to transmit unsolicited bulk e-mail, either fraudulently using the "aol.com" designation, or from AOL accounts controlled by The Defendants, even after being sued and held in default. Examples of recent unsolicited e-mail from The Defendants to AOL Members since the commencement of this lawsuit are annexed to theHistand Dec. as Exhibit 1 and examples of The Defendants' e-mail containing a false "aol.com" designation that were transmitted after service of the default judgment are annexed to the Ellender Dec. as Exhibit 8.

30. The Defendants were on notice for months before AOL sued them that their transmission of unsolicited bulk e-mail was unlawful. After receiving thousands of complaints from its members, AOL sent The Defendants a letter by Federal Express and e-mail on February 10, 1998, demanding that they cease and desist their unauthorized transmissions to and through AOL's proprietary computers and computer networks (Complaint 41; Ellender Dec. 6 & Ex. 3).

31. Despite receiving this cease and desist letter, The Defendants have continued their unlawful conduct (Complaint 41; Ellender Dec. 7, 11, 18). AOL filed suit and personally served The Defendants with the summons and complaint on December 18, 1998 (Ellender Dec. 2, 8). The Defendants were also interviewed by a reporter about the lawsuit (Ellender Dec. 10). Nevertheless, The defendants did not stop their transmission of unsolicited bulk e-mail (Ellender Dec. 11).

32. When AOL's counsel did not hear from The Defendants, or any lawyer purporting to represent them, Jeffrey M. Ellender, AOL's counsel, telephoned defendant Jason Vale on January 25, 1999 (Ellender Dec. 9). During that conversation, Vale told Ellender that The Defendants were inclined to default. Ellender responded that such a move would be unwise, explained to Vale the consequences of defaulting, and urged Vale to either hire a lawyer or contact the Court's Pro Se Office to obtain instructions as to how to file an answer (Ellender Dec. 9).

33. Ellender gave Vale the telephone number and address for the Pro Se Office and extended both The Defendants' time to answer to February 25, 1999 (Ellender Dec. 9). In addition, Ellender instructed Vale to cease and desist transmitting unsolicited bulk e-mail over AOL's computer network (Ellender Dec. 9). Despite Ellender's urging that The Defendants respond to the complaint and that they cease and desist from transmitting unsolicited bulk e-mail, The Defendants ignored the complaint and continued to transmit unsolicited bulk e-mail to AOL members (Ellender Dec. 11, 12).

34. Indeed, in March 1999, over three months after being served with the Complaint, thousands of pieces of unsolicited bulk e-mail touting The Defendants' promotional literature and products were transmitted not only from The Defendants directly, but also from at least thirty-three AOL accounts listed under the name of "Johanna Vale," who, according to AOL's
account records, is listed as residing at 151-47 18th Avenue, Whitestone, New York, the same address as both The Defendants (Davis Dec. 4).

35. The Defendants further demonstrated their intent to ignore this lawsuit when they refused to accept service of AOL’s motion for a default judgment from AOL’s process server (Declaration of Michael P. Fanning, dated July 7, 1999 (“Fanning Dec.”), 3). AOL’s process server -- Michael Fanning -- had previously hand-delivered AOL’s complaint and other papers to The Defendants, and, thus, The Defendants knew him to be AOL’s process server (Fanning Dec. 2). When Fanning attempted to hand-deliver the motion for a default judgment to The Defendants, the papers were thrown out of the door (Fanning Dec. 3). As a result, AOL delivered the motion papers to The Defendants by Federal Express (Ellender Dec. 13).


37. On June 8, 1999, this Court entered a default judgment against The Defendants, and Ellender served them with that Order by Federal Express on June 9, 1999. Ellender also served The Defendants with Judge Batts’ Order referring AOL’s application for an injunction and monetary damages to me (Ellender Dec. 15-16).

38. Even after receiving notice that a default judgment had been entered against them and receiving notice of AOL’s application for an injunction and damages, The Defendants continued their illegal activity. For example, on August 17, 1999, The Defendants transmitted unsolicited bulk e-mail touting their purported cancer cures to members of an Internet service called Hotmail. Because these e-mails falsely stated that they were generated by "John@aol.com," they misappropriated AOL’s Registered Marks and gave the false impression that AOL approves of the dissemination of these e-mails or the products advertised in them (Ellender Dec. 18, Ex. 8).

39. These facts establish that this lawsuit has not deterred The Defendants. Given The Defendants conduct in (a) ignoring AOL’s cease and desist requests, (b) attempting hide the source of their bulk e-mail to evade AOL’s filters, (c) receiving notice of every pleading and motion filed by AOL and ignoring each of these documents and every aspect of the judicial process in this case, and (d) continuing to transmit unsolicited bulk e-mail to AOL members even after being sued and held in default, only an injunction, with its potential sanction of contempt, and punitive damages, will deter The Defendants from their unlawful conduct.

40. The above facts also show that The Defendants’ deliberately and willfully infringed AOL’s trademark and demonstrated a conscious disregard for the rights of AOL and its members.

F. The Irreparable Harm The Defendants Have Caused To AOL And Its Members

41. AOL’s Internet e-mail system consists of several hundred servers, all of which are integrated with AOL’s central computer facilities (Declaration of A. Douglas Steinberg, dated August 19, 1999 (“Steinberg Dec.”), 4). These mail servers have a finite processing speed and memory capacity that limit their ability to receive, sort, deliver and store e-mail. AOL incurs considerable costs to receive, sort, deliver and store e-mail messages sent to AOL members from the Internet (Steinberg Dec. 7).

http://www.nyuj.com/links/aol.html 11/26/00
42. As the volume of Internet e-mail transmitted through AOL's computers has increased, AOL has been obliged to purchase millions of dollars worth of additional equipment to increase the capacity of its computer systems (Steinberg Dec. 9). During 1997-1998, AOL was required to constantly purchase new equipment for both systems in order to prevent the volume of Internet e-mail from undermining the functioning and integrity of AOL's entire e-mail system (Steinberg Dec. 9).

43. During early 1998, AOL's e-mail system was comprised of computer equipment valued at approximately $85,000,000. Based on the standard four-year lease term applicable to AOL's computer equipment, the monthly expense for AOL's computer e-mail system was $2,340,000. AOL estimates that it processes e-mail on behalf of between 2.4 and 3 billion recipients each month. Dividing the higher -- and thus more conservative -- figure of 3 billion monthly recipients into the monthly equipment charge of $2,340,000 yields a per recipient cost of $.00078. This figure includes only AOL's equipment costs, and does not include overhead such as office space, software licenses, bandwidth, or even electricity. The per-recipient charge for 1997 would have been higher than this charge because latter expansions in AOL's e-mail system resulted in significant economies of scale that lowered the per recipient charge. Therefore, the per-recipient charge of $.00078 is a conservative estimate of the per-recipient charge that existed during 1997 (Steinberg Dec. 10).

44. AOL's Internet e-mail delivery system has, at times, been disrupted by the transmission of unsolicited bulk e-mail through AOL's e-mail servers to AOL Members (Steinberg Dec. 11). Unsolicited bulk e-mail diverts computer processing resources away from the handling of authorized e-mail for AOL Members (Steinberg Dec. 11). Unsolicited bulk e-mail depletes the processing and storage capacity of AOL's mail servers (Steinberg Dec. 11). Unsolicited bulk e-mail has caused measurable delays in the delivery of Internet e-mail to AOL's Members (Steinberg Dec. 11). Because of the effect of unsolicited bulk e-mail on AOL's e-mail system, AOL has been forced to invest resources in new hardware, software and personnel in an effort to maintain the performance capacity of AOL's e-mail system (Steinberg Dec. 11).

45. The massive lists used by bulk e-mailers are often outdated and contain a large percentage of invalid or nonexistent e-mail addresses. Each message sent to an invalid e-mail address increases the processing load on AOL's computers. AOL's computers first attempt to deliver the message. Next, AOL's computers attempt to return it to the e-mail address in the "from line" of the message. If the sender falsified the return address, as many junk e-mailers do, AOL's computers are unable to return the message to the sender and continue to attempt to return it for hours and even days. Processing these "bounce messages" consumes considerable processing resources within AOL's computer networks (Steinberg Dec. 12).

46. Unsolicited bulk e-mail is transmitted in large quantities to lists of e-mail addressees that contain a significant number of invalid and undeliverable addresses. Because of these characteristics of unsolicited bulk e-mail, AOL must expend additional processing power and memory capacity in order to receive, sort, deliver and store unsolicited bulk e-mail. The transmission of unsolicited bulk e-mail containing false source and transmission path information and invalid recipient addresses causes similar, ripple effect problems across the Internet, as AOL attempts to return such messages to their source (Steinberg Dec. 13).

47. The transmission of unsolicited bulk e-mail is widely condemned in the Internet community (Complaint 36). Most AOL members do not like to receive junk e-mail and complain vociferously about receiving it very often.
48. During 1997 and 1998, the day-to-day functioning of the AOL service was impaired by unsolicited bulk e-mail. During that time, the increased demand on AOL’s Internet e-mail systems caused by unsolicited bulk e-mail was a substantial cause of delays of twenty-four hours or longer in the delivery of Internet mail to AOL members. These delays upset AOL members who expect to send and receive e-mail virtually instantaneously. Moreover, in instances in which the volume of Internet e-mail -- composed in significant part of unsolicited bulk e-mail -- threatened to disrupt AOL’s entire e-mail service, AOL was forced temporarily to stop accepting any Internet e-mail for delivery (Steinberg Dec. 17).

49. The Defendants’ transmission of unsolicited bulk e-mail to AOL has damaged, and, if unabated, will continue to damage, AOL’s business, its goodwill, and its relationship with its members (Price Dec. 8). AOL’s valuable trademark and service mark and associated goodwill are diluted and damaged by their wrongful association with junk e-mail and junk e-mailers like The Defendants (Complaint 40; Price Dec. 8).

50. Finally, The Defendants’ dissemination of bulk e-mail advertising is particularly pernicious in this case because it wrongly implies that AOL endorses The Defendants’ supposed cancer cures (Complaint 48).

G. Market Value of Advertising

Services Misappropriated

Through Unsolicited Bulk E-mail

51. AOL makes space available on its service for use by advertisers on a paying basis, including on the E-Mail In-Box Screen (Declaration of Todd C. Discenza, dated August 19, 1999, ("Discenza Dec.") 3). The E-Mail In-Box Screen lists all e-mail messages that an AOL member has in his or her In-Box at that moment (Discenza Dec. 3). AOL’s E-mail In-Box Screen also contains an advertisement area consisting of a rectangular banner which appears (in AOL’s Version 4.0) in the upper right-hand corner of the screen (the “Banner Advertisement”) (Discenza Dec. 3).

52. The Banner Advertisement that appears on that screen is typically used by an advertiser to present a short phrase or descriptive text to an AOL Member that encourages the member to click on the advertisement for more details (Discenza Dec. 4). The text in the Banner Advertisement is comparable to the subject line of an e-mail message (Discenza Dec. 4 & Ex. 1). The amount of information that can be presented in the Banner Advertisement is comparable to the amount of information that is presented in the subject line of the e-mail messages that also appear on the E-Mail In-Box Screen (Discenza Dec. 4). An AOL member who wants to learn more about the item being advertised can click on the Banner Advertisement (Discenza Dec. 4). By doing so, the member would be taken to an Internet site or a dedicated area on AOL’s service (Discenza Dec. 4). When the member has finished looking through that web site, he/she can return to his/her E-Mail In-Box Screen by closing their web browser or clicking a form that appears on the AOL service (Discenza Dec. 4).

53. AOL charges advertisers for the right to advertise on its service,
including placing Banner Advertisements on its E-Mail In-Box Screen (Discenza Dec. 5). All prices charged are quoted in terms of cost per thousand impressions (abbreviated "CPM") (Discenza Dec. 5). An "impression" is a presentation of the Banner Advertisement on the screen to a consumer and is counted each time a Member's E-Mail In box is opened (Discenza Dec. 5).

54. From the middle of 1997 to the present, AOL has charged advertisers wishing to purchase Banner Advertisements on AOL's E-Mail In-Box Screen a rate varying from between $4 CPM to $7 CPM ($0.004 to $0.007 per impression) (Discenza Dec. 6). Over this time period, the average CPM charged for such advertisements is approximately $5 (Discenza Dec. 6). The Defendants have paid no amount to AOL in exchange for marketing their products to AOL Members on AOL's proprietary network through the transmission of unsolicited bulk e-mail (Discenza Dec. 7).

H. The Amount of Unsolicited
Bulk E-Mail Transmitted by

The Defendant to AOL Members

55. AOL maintains an electronic database and mailbox entitled TOSSPam@aol.com (Histand Dec. 2). The TOSSPam database is a searchable database of e-mail complaints sent by AOL members to the electronic e-mail address "TOSSPam." This electronic mailing address is maintained by AOL as a forwarding address for electronic mail complaints regarding unsolicited bulk e-mail received by AOL members from the Internet. All complaints and e-mails forwarded to the TOSSPam e-mail address are placed in the TOSSPam database. During the period relevant to this litigation, AOL has received an average of over 100,000 such e-mail complaints forwarded by its members to TOSSPam each day. As a result, the TOSSPam database presently contains tens of millions of member complaints concerning unsolicited bulk e-mail (Histand Dec. 3).

56. If an AOL member wishes to complain about a particular piece of unsolicited bulk e-mail, he/she must affirmatively forward the e-mail to TOSSPam. The AOL member must: (1) technically know how to forward the message; (2) know the e-mail address to which to forward the complaint (TOSSPam); and (3) take the time necessary to forward the message (Histand Dec. 5). The TOSSPam database does not contain all complaints regarding unsolicited bulk e-mail that may have been sent by a particular "junk mailer" to AOL members. The TOSSPam database also does not include any comments regarding unsolicited bulk e-mail messages that could not be delivered to an AOL member because of invalid addresses. Instead, the TOSSPam database contains only those e-mails that AOL Members have chosen to complain about. Consequently, the number of complaints in the TOSSPam database relating to a particular piece of unsolicited bulk e-mail, or a particular junk e-mailer, may be only a small fraction of the total number of unsolicited e-mail messages sent to AOL Members (Histand Dec. 5).

57. Additionally, complaints contained in the TOSSPam database prior to January 1998 probably reflect an even lower proportion of the actual number of e-mail messages transmitted by a particular junk e-mailer, because it was only after January of 1998 that AOL prominently displayed in its "Junk Mail" information area the availability of TOSSPam as a resource to which Members could send their complaints about unsolicited bulk e-mail (Histand Dec. 6).
58. The actual number of unsolicited bulk e-mail messages advertising a particular product or service that are transmitted to AOL members may be tens, or even hundreds, of times higher than the number of complaints forwarded by AOL members to the TOSSpam database. Many AOL members simply choose to delete unsolicited bulk e-mail immediately rather than forward it to TOSSpam, because forwarding such e-mails requires additional time and effort on the part of the AOL Member (Histand Dec. 7).

59. A reasonable calculation of the ratio between the number of complaints received by TOSSpam and the total number of unsolicited e-mail messages transmitted to an AOL Member is 1:500. In America Online v. CN Productions, Inc., Docket No. 98-0552-A (E.D. Va. Feb. 10, 1999) (annexed to Plaintiff's Memorandum of Law as Exhibit D), the Court concluded that a reasonable TOSSpam complaint to total e-mail ratio was 1:500 (Histand Dec. 9). (Footnote 2)

60. In connection with this lawsuit, AOL has conducted a search for the member complaints within the TOSSpam database concerning unsolicited bulk e-mail transmitted by The Defendants (Histand Dec. 10).

61. In searching the TOSSpam database for complaints regarding unsolicited bulk e-mail messages containing advertisements for The Defendants' websites since December, 1997, AOL has located 47,154 complaints from AOL members regarding e-mail advertisements sent by The Defendants (Histand Dec. 10-11). Of these complaints, at least 10,168 were made after the filing of this lawsuit in December, 1998 (Histand Dec. 11). Multiplying this number of complaints by 500 yields a total of 23,577,000 unsolicited bulk e-mails of which 5,084,000 were sent after The Defendants were served with the Complaint (Histand Dec. 12).

III. CONCLUSIONS OF LAW

A. Jurisdiction, Venue and Choice of Law

62. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, as this action arises under the laws of the United States including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Lanham Act, 15 U.S.C. § 1051 et seq. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332, as there is complete diversity of citizenship between the parties, and the amount in controversy exceeds $75,000.00, exclusive of interest and costs (Complaint 12, 13).

63. This Court has subject matter jurisdiction over AOL's state law claims pursuant to 28 U.S.C. § 1367 (Complaint 14).

64. This Court has personal jurisdiction over Defendants Vale and The Christian Brothers because they are residents of New York, have engaged in business activities in New York and have caused tortious injury in New York (Complaint 8, 11).

65. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial portion of the events or omissions giving rise to AOL's claims occurred in this District (Complaint 15).

66. The law applicable to AOL's state claims is determined by resort to New York's choice of law rules. See Klexon Co. v. Stentor Elec. Mfg. Co., 313
I shall address the damages to be awarded under each claim in the order in which the claims have been asserted.

B. Impairing Computer Facilities

In Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)

73. The Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(8)(A) defines the term "damage" to mean "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 . . . ." Subdivision (g) of the same statute provides that:

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.


75. Based on the facts set forth in paragraphs 55-61, above, it is reasonable to infer that for every complaint received by AOL concerning The Defendants, there were 499 transmissions for which there was no complaint. Thus, the actual complaints received by AOL must be multiplied by 500 to estimate the actual number of unsolicited e-mails transmitted by The Defendants. Since AOL received 47,154 complaints concerning The Defendants, it appears that The Defendants actually transmitted at least 23,577,000 unsolicited e-mails. Any uncertainty resulting from this methodology is appropriately borne by The Defendants. See generally Contemporary Mission, Inc. v. Famous Music Corp., 557 F.2d 918, 926-27 (2d Cir. 1977).

76. AOL analogizes The Defendants' unsolicited e-mail to advertising. I find this analogy to be appropriate.

77. If The Defendants had sent their e-mails as paid advertising, they would have paid between $0.004 and $0.007 per transmission (Discenza Dec. 6). Using an average price of $0.0055 and multiplying that price by The Defendants' 23,577,000 transmissions yields a product of $129,673.50, which represents the revenue AOL lost as result of The Defendants transmitting their promotional material as unsolicited bulk e-mail instead of advertising material.

78. The Defendants' conduct also damaged AOL by causing it to incur $17,940 in hardware processing costs alone (23 million messages x $0.00078) (Steinberg Dec. 10-16; Histand Dec. 10-12). In effect, by burdening AOL's e-mail system with millions of unsolicited advertisements, The Defendants not only gained advertising services, as described above, but e-mail processing services which lawful banner advertisers on AOL's network do not require.

79. Accordingly, on its first claim, AOL is entitled to recover $129,673.50 in lost advertising revenue and $17,940 in hardware processing costs, for a total of $147,613.50.

C. Exceeding Authorized Access In

Violation of the Computer Fraud and

Abuse Act, 18 U.S.C. § 1030(a)(5)(c)

80. AOL also claims it is entitled to recover under the Computer Fraud and Abuse Act on the theory that The Defendants exceeded the scope of their authorized access to AOL's computer network.

81. As a result of The Defendants' default, there can be no doubt that AOL is entitled to recover on this theory. However, the Federal Computer Fraud and Abuse Act provides for one measure of damages, see 18 U.S.C. § 1030(g), regardless of the nature of the violation. Thus, AOL's damages on its second claim would be identical to the damages awarded on its first claim.
82. Accordingly, for the reasons stated above, AOL is also entitled to recover $147,613.50 on the alternative theory alleged in its second claim. This amount is recommended in the alternative to the amount recommended on AOL's first claim; it should not be awarded in addition to the amount awarded on the first claim.

D. Violation of Section 43(a)


1125(a) - False Designation of Origin

83. On its third claim, AOL seeks restitution for the benefits misappropriated by The Defendants, "reasonable royalties," disgorgement of profits, trebling of all damages awarded and attorney's fees.

84. To the extent AOL seeks royalties, there is a failure of proof. AOL has not offered evidence of the rates at which it licenses its marks, nor has it offered any evidence as to what a reasonable royalty would be for licensing its marks. Although AOL argues that a reasonable royalty rate is the rate paid by advertisers who advertise on AOL's network, this theory cannot be correct. Although legitimate advertisers use AOL's mark, the fees that such advertisers pay also includes compensation for AOL's transmission of the advertising copy. Thus, the fee paid by advertisers includes elements beyond royalty payments, and is not probative of the value of a reasonable royalty.

85. To the extent AOL seeks The Defendants' profits, there is also a failure of proof. There is no evidence that The Defendants ever sold anything or that they ever derived any revenue from their actions. AOL claims that, based on the volume of the e-mails sent by The Defendants, there must have been some sales. AOL may be correct in this regard, but in the absence of some evidence as to the level of Defendants' sales, any attempt to quantify those sales would be pure guess-work. I realize that AOL is entitled to a relaxed standard of proof in this regard. Louis Vuitton, S.A. v. Spencer Handbags Corp., 765 F.2d 966, 973 (2d Cir. 1985); Gucci America Inc. v. Rebecca Gold Enterprises, Inc., 786 F. Supp. 177, 182 (S.D.N.Y. 1992). Nevertheless, I believe that any attempt to quantify The Defendants' sales here would be pure speculation.

86. AOL's claim for restitution under the Lanham Act stands on a better footing. Although restitution is not one of the remedies expressly made available in Section 35 of the Lanham Act, 15 U.S.C. § 1117, a wrongdoer's profits are recoverable "as restitution for unjust enrichment" resulting from the violation of the Lanham Act. The Daisy Group, Ltd. v. Newport News, Inc., 999 F. Supp. 548, 552 (S.D.N.Y. 1998). In addition, even in the absence of proof of sales by The Defendants, their unlawful use of AOL's mark allowed them to avoid costs improperly. From an accounting perspective, the economic impact of costs avoided is identical to the impact of sales made. Accordingly, I find that AOL is entitled to recover the defendants avoided as a result of the misappropriation of AOL's mark. (Footnote 3)

87. As explained in paragraph 77, above, The Defendants would have paid AOL $129,673.50 had they sent their bulk e-mails as advertising. AOL is entitled to recover this sum under its Lanham Act claim. Again, this award is in the alternative to the award I recommend on AOL's first two claims.

88. Since The Defendants' infringement was intentional and The Defendants
have offered no mitigating factors whatsoever, it is also appropriate that this figure be trebled for a total of $389,020.50. See generally Deering, Milliken & Co. v. Gilbert, 259 F.2d 191, 194-95 (2d Cir. 1959); Tanning Research Labs., Inc. v. Worldwide Import & Export Corp., 803 F. Supp. 506, 610 (E.D.N.Y. 1992).

89. The Lanham Act also permits an award of attorney's fees in exceptional cases. 15 U.S.C. § 1117(a). Willful infringement is an exceptional circumstance that will support an award of attorney's fees. Bambu Sales, Inc. v. Ozak Trading, Inc., supra, 58 F.3d at 854; Sara Lee Corp. v. Bags of New York, Inc., 36 F. Supp.2d 161, 170 (S.D.N.Y. 1999). Since I have previously found that The Defendants acted willfully, an award of attorney's fees is appropriate here.


91. AOL seeks $40,000 in fees and disbursements (Ellender Dec. 38). However, the contemporaneous billing records submitted by AOL's counsel show that this figure is inexplicably inflated by more than thirty percent. The billing records show that AOL was billed for legal services as follows:

Jeffrey Ellender, Esq.
97.4 hours @ $200/hour = 19,480.00

John McFerrin-Clancy, Esq.
5.75 hours @ $300/hour(Footnote 4) = 1,725.00

Richard H. Dolan, Esq.
2.5 hours @ $300/hour = 750.00

Goara Asarian
18.75 hours @ $100/hour = 1,875.00

Olton Prititi
13 hours @ $90/hour = 1,170.00

Alex Kwae
10.45 hours @ $90/hour = 940.50

TOTAL 25,940.50

Disbursements 4,625.21
GRAND TOTAL 30,565.21

Ellender Dec. Ex. 9).


93. However, the aggregate number of attorney hours for which compensation is sought -- 105.65 -- is excessive in view of the fact there was no appearance by The Defendants. Accordingly, I recommend that the fee award be reduced to an aggregate of $24,625.21, representing $20,000.00 in fees and $4,625.21 in disbursements. See generally Luciano v. Olsten Corp., 109 F.3d 111, 117 (2d Cir. 1997) (District Courts permitted to correct for excessive hours by "making an across-the-board reduction in the amount of hours").

94. Accordingly, on AOL's Lanham Act claim, I recommended that AOL be awarded $389,020.50, representing three times the value of the costs saved by The Defendants, and $24,625.21 in attorney's fees. One-third of the former figure -- $129,673.50 -- should be awarded in the alternative to the damages recommended with respect to AOL's first two claims; the balance of the $389,020.50, plus the $24,625.21 in attorney's fees, is in addition to the amounts recommended with respect to AOL's prior claims.

E. Violation of Federal Anti-Dilution


95. AOL makes no claim that it is entitled to damages under the Federal Anti-Dilution Statute, 15 U.S.C. § 1125(c). Accordingly, I decline to recommend an award of any damages on this claim.

F. Trespass to Chattels Under

Virginia Common Law

96. The only damages AOL seeks on its claim for trespass to chattels are punitive damages.

97. Punitive damages may be awarded under a Virginia law where a defendant's conduct is malicious, Peacock Buick, Inc. v. Durkin, 221 Va. 1133, 1136, 277 S.E.2d 225, 227 (1981) or is in "conscious disregard of the rights of others and is wanton and oppressive." National Carloading Corp. v. Astro Van Lines, Inc., 593 F.2d 559, 565 (4th Cir. 1979). The Defendants' conduct meets these standards, and I recommend that punitive damages be assessed against The Defendants in the amount of $200,000.00.
G. Violation of the Virginia Computer Crimes Act

98. In its sixth claim, AOL seeks an award of damages based on the Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.1 through 18.2-152.15.

99. Although Section 18.2-152.12(C) provides for liquidated damages and attorney's fees in favor of an electronic mail service provider against persons who transmit unsolicited bulk e-mail, that provision was not enacted until 1999, after this action was commenced. Since AOL does not contend Section 18.2-152.12(C) should be given retroactive application here, I do not apply it.

100. Virginia Code Section 18.2-152.12(A) provides that

Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefore and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

101. For the reasons stated in paragraphs 77-79, above, I conclude that AOL has been damaged by The Defendants Activities in the amount of $147,613.50. Accordingly, AOL is also entitled to recover the sum of $147,613.50 on its sixth claim. Again, this recommended award is in the alternative to the amount recommended on AOL's first, second, third and fifth claims.

H. Common Law Misappropriation of Name and Identity

102. AOL attempts to assert its seventh claim under New York substantive law (AOL's Proposed Findings of Fact and Conclusions of Law 71). Since I have concluded that Virginia's substantive law applies to AOL's claims, I recommend no monetary recovery with respect to AOL's seventh claim.

I. Violation of the New York General Business Law,

§§ 130, 349 and 350

103. Again, AOL attempts to assert its eighth claim under New York substantive law (AOL's Proposed Findings of Fact and Conclusions of Law 74). Since I have concluded that Virginia's substantive law applies to AOL's claims, I recommend no monetary recovery with respect to AOL's eighth claim.

J. Common Law Fraud

Under Virginia Law

104. AOL's common law fraud claim is far from clear. AOL does not allege that The Defendants made fraudulent misrepresentations to it upon which it
relied to its detriment. Rather AOL's fraud claim seems indistinguishable from its Lanham Act claim.

105. For example, AOL’s complaint alleges, in pertinent part:

106. As a result of Defendants' misrepresentation of AOL’s name, identity and domain name, AOL has suffered damages, and Defendants have earned profits in an amount to be proven at trial.

***

108. Defendants' acts of misrepresentation continue to damage AOL and Defendants continue to earn profits from this misrepresentation. As a result, the value of AOL’s business, reputation and substantial goodwill are being irreparably damaged. Because these damages cannot be readily ascertained, plaintiff lacks an adequate remedy at law.

109. Defendants' conduct was deliberate and intentional. Defendants' attempts to conceal the identity and e-mail address of the sender of the spam was intended to deceive AOL and the recipients of the spam of its true origin.

110. AOL has been damaged by Defendants' fraud through the loss of members and revenue and damage to its business name and reputation. Although these damages cannot be readily ascertained, they far exceed $75,000, exclusive of interest and costs.

(Complaint 106, 108-10).


Damages for fraud are measured by the extent of any detrimental reliance by the plaintiff on the representations of the defendant; where the plaintiffs do not actually lose anything there can be no recovery in fraud. See Murray v. Hadid, 238 Va. 722, 731, 385 S.E.2d 898 (1989); Community Bank v. Wright, 221 Va. 172, 175, 267 S.E.2d 158 (1980).


107. In Virginia, these damages are usually measured by the “benefit of the bargain” rule, i.e., the difference between the value of what the defrauded party received and the value that it would have received had the
108. Although The Defendants' default establishes that their misrepresentations operated as a fraud, AOL has not shown how it suffered any damages as a result of its reliance on the misrepresentations.

109. To the extent AOL seeks punitive damages on its fraud claim, the interests served by punitive damages are adequately met by my recommended award of punitive damages on AOL's claim for trespass to chattels. Accordingly, I recommend no additional award of punitive damages on AOL's fraud claim.

K. Unjust Enrichment under

Virginia Common Law

110. Under Virginia law, restitutionary recovery for unjust enrichment is appropriate when (1) a benefit has been conferred upon defendant by plaintiff; (2) defendant has appreciation or knowledge of the benefit, and (3) acceptance or retention of the benefit by defendant occurs under circumstances which would make it inequitable for defendant to retain the benefit without paying plaintiff. John C. Holland Enter., Inc. v. J.P. Mascaro & Sons, Inc., 653 F. Supp. 1242, 1246-47 (E.D. Va. 1987); City of Norfolk v. Norfolk County, 120 Va. 822, 91 S.E. 820, 822 (Va. 1917). Restitution is also authorized when the plaintiff demonstrates either that (1) it had a reasonable expectation of payment for a benefit appropriated by defendant; (2) defendant should reasonably have expected to pay for the benefit it appropriated, or (3) society's reasonable expectations of person and property would be defeated by nonpayment for the benefit. Provident Life & Accident Ins. Co. v. Waller, 906 F.2d 985, 993-94 (4th Cir. 1990).

111. As set forth in paragraph 77 above, The Defendants, through their unauthorized transmission of unsolicited bulk e-mail over AOL's network, avoided costs of $129,673.50 and have been unjustly enriched to that extent.

112. Accordingly, AOL is also entitled to recover the sum of $129,673.50 on its claim unjust enrichment claim. This sum should be awarded in the alternative to the sums recommended on AOL's first, second, third, fifth and sixth claims and not in addition to the sums awarded on those clams.

L. Nuisance under

Virginia Common Law

113. AOL's submissions do not address what damages, if any, are recoverable on its nuisance claim.

114. Although there is some general authority that nuisance is an elastic concept, Prosser & Keeton on the Law of Torts § 86 at 616 (W. Page Keeton ed., 5th ed. 1984) ("Nuisance has meant all things to all people . . . "). My own research has not disclosed any Virginia authorities recognizing a claim for nuisance that has not involved conduct affecting the use and enjoyment of real property. See generally National Energy Corp. v. Quinn, 223 Va. 83, 286 S.E.2d 181 (1982); City of Newport News v. Hertzler, 216 Va. 587, 221 S.E.2d 146 (1976); Barnes v. Graham Virginia Quarries, Inc., 204 Va. 414, 132 S.E.2d 395 (1963); Haywood v. Massie, 188 Va. 176, 49 S.E.2d 281 (1949); Brunn v. Lowe, 140 Va. 489, 120 S.E. 856 (1921).
115. Since Virginia appears to limit claims for nuisance to matters involving the use and enjoyment of real property and AOL has offered no explanation of how The Defendants' conduct constitutes a nuisance, I recommend that no damages be awarded on AOL's claim for nuisance.

M. AOL's Claim for Violation of the Washington State Unsolicited Commercial Electronic Mail Act

116. Since I previously determined that the internal law of the State of Virginia should be applied to AOL's claims, I recommend that no damages be awarded on AOL's claim under Washington State's Unsolicited Commercial Electronic Mail Act, Wash. Rev. Code §§ 19.190.010 - .050.

N. Prejudgment Interest

117. AOL seeks prejudgment interest on the damages recommended herein.

118. Although the Lanham Act does not expressly provide for awards of prejudgment interest, it is well settled that courts have the discretion to award prejudgment interest under the Lanham Act in "exceptional cases." American Honda Motor Co. v. Two Wheel Corp., 918 F.2d 1060, 1064 (2d Cir. 1990); Independent Living Aids, Inc. v. Maxi-Aids, Inc., 25 F. Supp. 2d 127, 135 (E.D.N.Y. 1998).

119. Virginia state law appears to permit an award of prejudgment interest on tort claims "so long as there is a rational basis in the evidence upon which to fix the date when interest should begin to run." McClung v. Smith, 870 F. Supp. 1384, 1409 (E.D. Va. 1994).

120. As a matter of discretion, I decline to recommend an award of prejudgment interest here. First, there is no evidence that The Defendants have done anything to prolong proceedings here and thereby delay the date of AOL's judgment. Second, AOL has not even identified a date from which interest should be awarded. Thus, I conclude that an award of prejudgment interest is inappropriate here.

O. Claim for Injunctive Relief

121. Permanent injunctive relief is appropriate when a defendant inflicts irreparable harm through tortious action. The Defendants' infringement of AOL's marks and trespass upon AOL's proprietary computer systems have caused irreparable harm to AOL by injuring AOL's goodwill. Accordingly, for the reasons set forth below, I further recommend that a permanent injunction be entered against The Defendants.

122. To obtain a permanent injunction, a party must show the absence of an adequate remedy at law and irreparable harm in the absence of injunctive relief. See New York State National Organization For Women v. Terry, 886 F.2d 1339, 1362 (2d Cir. 1989). The standard for a permanent injunction is essentially the same as for a preliminary injunction, except that the plaintiff must actually succeed on the merits. See Joined Production Corp. v. Village

123. AOL has adequately demonstrated irreparable harm in this case. Where, as here, trademark infringement has been shown, irreparable harm is presumed. "[I]rrerparable injury regularly follows from trademark infringement." Lone Star Steakhouse & Saloon v. Alpha, 43 F.3d 922, 939 (4th Cir. 1995). See also Genessee Brewing Co. v. Stroh Brewing Co., 124 F.3d 137, 142 (2d Cir. 1997); Hasbro, Inc. v. Lanard Toys, Ltd., 858 F.2d 70, 73 (2d Cir. 1988).


125. As discussed above, it is impossible to determine with certainty the number of unsolicited e-mails The Defendants have actually sent and it is impossible to quantify the damage those e-mails have caused to AOL's goodwill. Injunctive relief is appropriate to remedy such injury. Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027-28 (S.D. Ohio 1997). See Ecolab, Inc. v. K.P. Laundry Machinery, Inc., 656 F. Supp. 894, 899-900 (S.D.N.Y. 1987) (Leval, J.); New York State Motor Truck Ass'n v. City of New York, 654 F. Supp. 1521, 1540 (S.D.N.Y.), aff'd, 833 F.2d 430 (2d Cir. 1987).

126. Accordingly, I respectfully recommend that a permanent injunction be entered enjoining The Defendants, their officers, agents, conspirators, servants, affiliates, employees, parent and subsidiary corporations, attorneys and representatives, and all those in privity or acting in concert with Defendants, including but not limited to Johanna Vale, from directly or indirectly:

a. using or directing, aiding or conspiring with others to use the computers or computer networks of AOL, or any of its subsidiary or affiliate companies, in any manner, directly or indirectly, in connection with the transmission or transfer of any form of electronic information across the Internet;

b. opening, creating, obtaining access to and/or using in any way, or directing, aiding or conspiring with others to open, create, obtain access to and/or use in any way, any membership, subscription or service provided by AOL or any of its subsidiary or affiliate companies;

c. acquiring, compiling or transferring any names, e-mail addresses, or other identifying information for members or subscribers of any services offered by AOL or any of its subsidiary or affiliate companies, including particularly any e-mail addresses that contain the "aol.com" domain name;
d. sending or transmitting or directing, aiding, facilitating or conspiring with others to send or transmit, any electronic mail message, or any electronic communication of any kind, to or through the computers or computer networks of AOL, or any of its subsidiary or affiliate companies, or to members or subscribers to any service offered by AOL;

e. sending or transmitting to any destination, or directing, aiding, or conspiring with others to send or transmit to any destination, electronic mail or electronic communication bearing any false, fraudulent, anonymous, inactive, deceptive, or invalid return information, or containing the domain name "aol.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;

f. using any images, designs, logos or marks which copy, imitate or simulate any AOL trade or service mark for any purpose and/or using "AOL" in any Internet domain name or Internet Website for any purpose, including but not limited to, any advertisement, promotion, sale or use of any products or services;

g. performing any action or using any images, designs, logos or marks that are likely to cause confusion, mistakes, deceive or to otherwise mislead the trade or public into believing that AOL and The Defendants are in any way connected, or that AOL sponsors The Defendants, or that The Defendants are in any manner affiliated or associated with, or under the supervision or control of AOL, or that The Defendants and AOL or AOL's services are associated in any way;

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

IV. Conclusion

Accordingly, for all the foregoing reasons, I recommend that judgment be entered as follows:

1. That AOL be awarded damages on its twelve claims as follows:

   First Claim: $147,613.50

   Second Claim: $147,613.50. This recommended award is in the alternative to the amount recommended on AOL's first claim.

   Third Claim: $413,645.71. $129,673.50 of this sum is in the alternative to the amounts recommended on AOL's first and second claims; the balance ($283,972.21) is in addition to the amounts recommended on AOL's first and second claims.
Sec. 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 title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, 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.

Footnotes

[1] So in original. Probably should be "subparagraph
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 contributarily 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

http://members.theglobe.com/ericgoldman/alert.html?nfhp=975866825&rld=204526671

11/26/00
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.

http://members.theglobe.com/ericgoldman/alert.html?fhp=975866825&crld=204526671

11/26/00
UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

No. 97-1523

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.

COUNSEL


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 means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. Id. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgment on the pleadings, see Fed. R. Civ. P. 12 (c), so we accept the facts alleged in the complaint as true. Bruce v. Riddle, 631 F.2d 272, 273 (4th Cir. 1980). On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRXO 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, unfettered 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 online 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

http://www.techlawjournal.com/courts/zeran/71112opn.htm 11/26/00
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 publication. Restatement (Second) of Torts § 577; see also Tacket v. General Motors Corp., 836 F.2d 1042, 1046- 47 (7th Cir. 1987). In fact, every repetition of a defamatory statement is considered a publication. Keeton et al., supra, § 113, at 799.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication ... is charged with publication." Id. Even distributors are considered to be publishers for purposes of defamation law: Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents - - including the defamatory content - - and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published. Id. at 803. AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 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), recognize a legal distinction between publishers and distributors. He misapprehends, however, the significance of that distinction for the legal issue we consider here. It is undoubtedly true that mere conduits, or distributors, are subject to a different standard of liability. As explained above, distributors must at a minimum have knowledge of the existence of a defamatory statement as a prerequisite to liability. But this distinction signifies only that different standards of liability may be applied within the larger publisher category, depending on the specific type of publisher concerned. See Keeton et al., supra, § 113, at 799- 800 (explaining that every party involved is charged with publication, although degrees of legal responsibility differ). To the extent
that decisions like Stratton and Cubby utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. Stratton and Cubby do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

Zeron simply attaches too much importance to the presence of the distinct notice element in distributor liability. The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher. The computer service provider must decide whether to publish, edit, or withdraw the posting. In this respect, Zeron seeks to impose liability on AOL for assuming the role for which § 230 specifically proscribes liability -- the publisher role.

Our view that Zeron's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeron'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, Zeron certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeron next contends that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA.

Zeron 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 investigation 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. Auvil v. CBS 60 Minutes, 800 F. Supp. 928, 931 (E.D. Wash. 1992) (recognizing that it is unrealistic for network affiliates to "monitor incoming transmissions and exercise on-the-spot discretion 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. 767, 777 (1986) (recognizing that fears of unjustified liability produce a chilling effect antithetical to First Amendment's protection of speech). Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at 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. Solimino, 501 U.S. 104, 110-11 (1991) (statute need not expressly delimit manner in which common law principle is abrogated). Zeran's argument flies in the face of this warning. As explained above, interpreting § 230 to leave distributor liability in effect would defeat the two primary purposes of the statute and would certainly "lessen the scope plainly intended" by Congress' use of the term "publisher."

Section 230 represents the approach of Congress to a problem of national and international dimension. The Supreme Court underscored this point in ACLU v. Reno, finding that the Internet allows "tens of millions of people to communicate with one another and to access vast amounts of information from around the world. [I]t is a unique and wholly new medium of worldwide human communication." 117 S. Ct. at 2334 (citation omitted). Application of the canon invoked by Zeran here would significantly lessen Congress' power, derived from the Commerce Clause, to act in a field whose international character is apparent. While Congress allowed for the enforcement of "any State law that is consistent with [§ 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 inconsistent with this section." With respect to federal-state preemption, the Court has advised: "'When Congress has 'unmistakably . . . ordained,' that its enactments alone are to regulate a part of commerce, state laws regulating that aspect of commerce must fall. The result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose." Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977) (citations omitted). Here, Congress' command is explicitly stated. Its exercise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.
neither imposes any new liability on Zeran nor takes away any rights acquired under prior law. No person has a vested right in a nonfinal tort judgment, much less an unfiled tort claim. Hammond v. United States, 786 F.2d 8, 12 (1st Cir. 1986). Furthermore, 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

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."
California Superior Court
City and County of San Francisco
Department Number 304

RANDALL STONER
Plaintiff,

vs.

EBAY INC., a Delaware Corporation, et al.,
Defendants.

No. 305666

Order Granting Defendant's Motion for Summary Judgment

Defendants' Motion for Summary Judgment came on regularly for hearing on October 10, 2000. The question to be decided is whether eBay enjoys immunity under the Communications Decency Act ("CDA"), 47 U.S.C. §230, for the conduct underlying plaintiff's claims. Having reviewed the evidence, law and argument, the Court concludes that eBay is immune from any liability arising from plaintiff's claims, and therefore grants defendant's motion.

eBay is an online auction company. Plaintiff claims that eBay "has developed a method of operation that allows it to knowingly reap massive profits from the sale of bootleg and other unauthorized 'infringing' sound recordings in violation of Business and Professional Code §17200." (Plaintiff's memorandum of Points and Authorities (Plaintiff's P&A") p.I.) Specifically, plaintiff claims that eBay violates section 17200 in that "(1) eBay actually sells, or at minimum, advertises and offers for sale, and causes the sale of, various bootleg and other infringing sound recording, in direct violation of several applicable Penal Code Provisions (Pen. Code, §§653h, 653s, 655w); (2) eBay, independent of its users, engages in unfair business practices in that knowing full well that infringing sound recording auctions are prevalent of its site, eBay actively promotes and enables those auctions and takes a commission on each sale, even though it could eliminate said infringing auction if it wanted to; and (3) eBay itself engages in conduct likely to deceive the public in that it knows about and actively facilitates infringing sound recording auctions even though, as it also knows, many of the ultimate purchasers of the recordings truly do not realize they are buying illegal items with no resale value. (Plaintiff's P&A, p. 11-12, citing Second Amended Complaint ¶¶8-25.)

Defendant's immunity claims is based on 47 U.S.C. §230 (e)(1), which states that "[n]o provider or users of interactive computer service shall be treated as the publisher or speaker of any information content provider," and section 230(e)(3) which provides in part that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." Section 230 "creates a federal immunity to any state law cause of action that would hold computer service providers liable for information originating with a third party. 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 based. (Zeran v. America Online (4th Cir. 1997) 129 F.3d 327, 330.)
Immunity under the CDA requires proof of three elements. Defendant must establish (1) that eBay is an interactive computer services provider; (2) that eBay is not an information content provider with respect to the disputed activity; and (3) that plaintiff seeks to hold eBay liable for information originating with a third-party user of its service. (Ibid.) For purposes of this motion it is undisputed that eBay is an interactive computer service provider as defined in section 230(f)(2). (Plaintiff's Separate Statement of Undisputed Material Facts ("Plaintiff's Material Facts"), ¶10, pg. 6.) Additionally, eBay has satisfied its burden of establishing that it is not an information content provider as defined in section 230(f)(3). The undisputed facts establish that the descriptions of the goods and services auctioned over the eBay service are created entirely by the sellers. (Plaintiff's Material Facts, ¶2, pg.2.) eBay is not responsible for the creation or development of information relating to any of the products for which it provides auction services. While eBay may add additional information to its web pages, such as logos, category headings and seller rating, this information is not unlike the information added to many web pages, the purpose of which is to facilitate ease of use and access to the content provided by the third-party. eBay, therefore, is not an information content provider or joint information content provider with respect to the description of auctioned goods.

The more difficult question is whether plaintiff is seeking to hold eBay responsible for content provided by third parties. Plaintiff does not claim that there is anything improper about the manner in which eBay conducts its auction business, other than that it auctions sound recordings that may not lawfully be sold. However, plaintiff contends that eBay's services continue more than mere publication of product descriptions prepared by others, and are instead independent acts of eBay in furtherance of illegal sales. Therefore, plaintiff claims, this suit does not seek to hold eBay responsible for the publication of information provided by others, but for eBay's own participation in selling contraband musical recordings.

Despite plaintiff's attempt to characterize eBay as an active participant in the sale of products auctioned over its service, plaintiff is seeking to hold eBay responsible for informing prospective purchasers that illegal recordings may be purchased--information that originates with the third party sellers who use the computer service. The uncontested facts establish that eBay's role does not extend beyond the scope of the federal immunity. eBay provides an interactive computer service by which sellers of goods and services describe over the internet the products they wish to sell, and sell them to the person who agrees, by submitting a bid through eBay's web site in accordance with the rules of the service, to pay the highest price for the product. eBay provides interactive computer services for which it charges a fee, just as America Online provides interactive services for which it charges a fee. eBay does not select items to be auctioned, does not inspect or come into possession of those items at any time, does not describe the items to prospective bidders, and does not determine the minimum price which the seller will accept for the item. eBay does advertise and promote its auction service, and charges a fee for the use of its service. However, neither aggressive advertising nor the imposition of a fee--including a fee based in part on the price at which an item is sold--transforms an interactive service provider into a seller responsible for items sold. (Cf. Blumenthal v. Drudge (D.D.C. 1998) 992 F.Supp. 44, 51-52 (America Online immune from liability for libelous statements contained in the Drudge Report even though America Online paid Drudge to include the Report on its service and actively advertised the Report by, among other things, issuing a press release which made "clear the kind of material Drudge would provide to AOL subscribers--gossip and rumor--and urged potential subscribers to sign onto AOL in order to get the benefit of the Drudge Report.").)

Plaintiff points to several other features of eBay's service which he contends transform defendant
from a mere computer services provider to an active participant in the sale of the auctioned goods and services. eBay provides insurance for all auctioned items up to $200, less a $25 deductible. (Perkins' declaration, Ex. 1.) Coverage is available where a buyer pays for an item but does not receive it or where the buyer receives "an item that is less than that which is described" (Ibid.) Providing insurance, however, is not selling, or offering to sell, the insured merchandise. Providing limited insurance for all items auctioned over its service may encourage buyers to use the service, but does not make eBay the seller. If a seller misrepresents an auctioned item, giving rise to coverage, the insurer will have a subrogation claim against the seller, but not against eBay, (See, e.g., Fireman's Fund Ins. Co. v. Wilshire Film Ventures, Inc. (1997) 52 CalApp. 4th 553, 555-556.) eBay also provides escrow and payment services, for which additional fees are charged. eBay refers users to i-Escrow, which accepts payment from the buyer, and in turn pays the seller when the buyer has received and approved the auctioned merchandise. eBay's Billpoint service enables buyers to pay for auctioned items by credit card or electronic check. Neither the escrow service nor the Billpoint, however, renders eBay a seller. Both are merely additional services which promote the provident and efficient use of eBay's auction service, irrespective of the legality or illegality of the item being auctioned. These additional features are available with respect to all goods and services auctioned--they are not limited to recordings, much less to illegal recordings.

Plaintiff attempts to draw a distinction between eBay's interactive service, which he argues is based on a sales model, and other interactive services which are based on bulletin board models. While the majority of cases addressing CDA immunity may fit the bulletin board description, nothing in those cases or in the statutory language so limits the CDA's application. A principle objective of the immunity provision is to encourage commerce over the Internet by ensuring that interactive computer service providers are not held responsible for how third parties use their services. "It is the policy of the United States to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." (47 U.S.C.A. §230(b)(2).) This policy is based in part on Congress' finding that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services." (47 U.S.C.A. §230 (a)(5).) To accomplish this objective, the immunity extends beyond the publication of harmful material over the Internet, and encompasses the distribution of such material in transactions effected over the Internet. (See Doe v. America Online (Fla. Dist. Ct. App. 1998) 718 So.2d 385, (review granted, April 12, 1999, 729 So.2d 390) (immunity extends to action by a mother against America Online for selling and distributing pornographic material of her minor son in violation of Florida law.) Plaintiff's attempt to impose responsibility on eBay as the seller of items auctioned over its service is no different from the unsuccessful attempts that have been made to hold computer service providers liable as distributors rather than as publishers of defamatory or pornographic materials. (Doe v. America Online, supra, 718 So.2d. 385; Zeron, supra, 129 F.3d. 327, 332.)

At bottom, plaintiff's contention is that eBay should be held responsible for failing to monitor the products auctioned over its service. The very description of some recordings (e.g. "bootleg" tapes) identifies some as contraband so that plaintiff contends, eBay must be deemed to have notice that these may not lawfully be sold, and by failing to intervene must be deemed to have knowingly joined in the unlawful sale. However, cases decided under the CDA uniformly have held that notice of postings which indicate illegality does not defeat immunity. (See Zeron, supra, 129 F.3d at 331-334, Doe v. America Online, supra, 718 So.2d at 388-389.) The courts have recognized that imposing liability based on notice of content in the interactive computer service context would create an incentive for providers to restrict speech and abstain from self-regulation, thereby defeating the purposes of section 230. (Ibid.)
The record reflects that at any given time, eBay has over 4 million listings on its website, approximately 275,000 in the music category alone. (Plaintiff’s Material Facts, ¶12, pg. 7.) However, many of these products may be contraband, and however many it might be possible for defendant to identify as such, Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products. While such a service may be aware that a fraction of the large volume of data exchanged over its facilities involves unlawful activity, and might be able to detect a certain portion of these the threat of liability for failing to monitor effectively would, in the judgment of Congress, deter companies such as eBay from making their service available as widely and as freely as possible. Moreover, removing any legal obligation to monitor was thought to encourage voluntary efforts to screen out offensive or unlawful materials that might not be made by service providers if the failure to detect an inappropriate use of their system could be a predicate for liability. (Zeran, supra, 129 F.3d at 331.) The record reflects that eBay has adopted procedures to curtail the use of its service to sell inappropriate items. Plaintiff contends that these measures are inadequate, but imposing liability for defendant’s failure to do more would require precisely the monitoring of third party content that Congress determined should not be mandated.

While the description of a recording as "bootleg" certainly suggests that the recording is on that may not lawfully be sold, an inspection of the product nonetheless may be necessary to be sure.[FN1] Moreover, if eBay were responsible for permitting the sale of unauthorized recordings over its service, the company would be obliged to investigate in countless cases where the description of the item was more ambiguous, or where information from other sources provided a basis for suspicion. And if liability were imposed for the sale of unauthorized recordings in violation of the Penal Code provisions relied on here, there is no reason why liability would not extend to the auction of any other form of contraband, or of goods or services that violate some other legal duty that eBay was bound to know or that was brought to its attention. The burden that such an obligation would place on a service such as eBay likely would force it to cease, or at least significantly restrict, its operation. If such an obligation is to be imposed, it is Congress that must be asked to re-evaluate the immunity conferred by section 230.

There is, to be sure, some point at which the existing immunity would no longer apply. Although the limits of the immunity have not yet been clearly defined, any limitation placed on the immunity presumably would begin at the point at which providing otherwise lawful goods or services with knowledge that they are being put to an illegal use becomes the commission, or the aiding and abetting, of a crime. (See People v. Lauria (1967) 251 Cal.App.2d 471; People v. Beeman (1984) 35 Cal.3d 547; United States v. Blankenship (7th Cir. 1992) 970 F.2d 283.) Using the rather extreme hypothetical situation discussed at the hearing, if an interactive computer service were shown to be actively involved in the sale of drugs or other contraband, the fact that sales were consummated over the computer service would not necessarily provide a shield from liability. In order for liability to arise and the immunity to be lost, it would be necessary to show actual, rather than constructive, knowledge of illegal sales, and some affirmative action by the computer service, beyond making its facilities available in the normal manner, designed to accomplish the illegal sales. (See People v. Lauria, supra; People v. Beeman, supra, compare also Wilcox v. First Interstate Bank of Oregon (D. Ore. 1985) 605 F. Supp. 593, 594, affd. As mod. (9th Cir. 1987) 815 F.2d 522; C-O-Two Fire Equipment Co. v. United States (9th Cir. 1952) 197 F.2d 489, cert. den. (1952) 344 U.S. 892 (mere parallel activity by competitors does not constitute illegal agreement to restrain trade absent conduct inconsistent with best interests of competitors considered independently).) The uncontroverted circumstances in this case do not rise to such a level.
Accordingly, defendant's motion for summary judgment must be granted.

Dated: November 7, 2000
STUART R. POLLACK
Judge of the Superior Court

FOOTNOTES:

FN1. In some cases, falsely describing an article as illicit may add to its value. See, e.g., the lyrics to the Credence Clearwater hit song "Bootleg":

"Take you a glass of water,
make it against the law.
See how good the water tastes
when you can't have any at all."

See also the Eminem hit song, "My Name Is...(Bootleg Version)," which may be considerably more popular than the alternative version, "My Name Is"
194 F.3d 980

LOCKHEED MARTIN CORPORATION, Plaintiff-Counter-Defendant-Appellant,
v.
NETWORK SOLUTIONS, INC., Defendant-Counter-Claimant-Appellee.

No. 97-56734.

United States Court of Appeals,
Ninth Circuit.

Argued and Submitted June 8, 1999.

Filed Oct. 25, 1999

David W. Quinto, Quinn Emanuel Urquhart Oliver & Hedges, Los Angeles, California, for the plaintiff-counter-defendant-appellant.

Ronald L. Johnston, Suzanne V. Wilson, Blanc Williams Johnston & Kronstadt, Los Angeles, California, for the defendant-counter-claimant-appellee.

Appeal from the United States District Court for the Central District of California; Dean D. Pregerson, District Judge, Presiding.  D.C. No. CV-96- 07438-DDP (ANx).

Before: NELSON, REINHARDT, and TROTT, Circuit Judges.

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. §§ 1051- 1127 (1994 & Supp. I 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. § 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. § 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, 189 F.3d 868 (9th Cir.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 Clasing, 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: <skunkworks.com>, <skunkworks.net>, <skunkwrks.com>, <skunkwerx.com>, <theskunkworks.com>, <skunkworks1.com>, <skunkworks.org>, <skunkwear.com>, <theskunkworks.com>, <skunkwrks.com>, and <theencryptedskunkworks.com>. Lockheed alleges that many of these registrations infringe and dilute its "Skunk Works" service mark.

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>. Why didn't Lockheed grab this?

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

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, 102 S.Ct. 2182, 72 L.Ed.2d 606 (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, 102 S.Ct. 2182.

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 (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, 102 S.Ct. 2182. In Inwood Lab., the Supreme Court considered an action against a manufacturer of generic pharmaceuticals. Id. at 847, 102 S.Ct. 2182. Non-party pharmacists packaged the defendant's less-expensive generic pills, but labeled them with the plaintiff's brand name. Id. at 850, 102 S.Ct. 2182. 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, 102 S.Ct. 2182.

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 infringement if it "supplied [led] the necessary marketplace" for the sale of infringing products. Id. at 265 (citing Hard Rock, 955 F.2d at 1149).

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

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 website or other Internet form of communication in connection with goods or services... NSI's involvement with the use of domain names does not extend beyond registration.

985 F.Supp. at 958.

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, 76 F.3d at 265.

V

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:

[T]he 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, § 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

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, 83 S.Ct. 227, 9 L.Ed.2d 222 (1962). We consider four factors when reviewing a decision whether to permit an amendment: (1) bad faith on the part of the plaintiffs; (2) undue delay; (3) prejudice to the opposing party; and (4) futility of the proposed amendment. Griggs, 170 F.3d at 877.

Although delay is not a dispositive factor in the amendment analysis, 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.

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.

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.

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. Kegan 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, 102 S.Ct. 2182. 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.

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.