Cyber Law (Law 334)

Eric Goldman

Fall 2005
Cyberlaw (Law 434)
Eric Goldman
Fall 2005

1. **Sessions.** The course meets 10:30-11:45 am every Tuesday and Thursday from August 23 to December 1, except October 4 (Rosh Hashana), October 13 (Yom Kippur) and November 24 (Thanksgiving).

2. **Prerequisites.** The first year law school curriculum is a prerequisite. However, you do not need the IP survey course or a technical background.

3. **Grading.** The final exam will be 100% of the course grade. I strongly encourage you to review prior exams to understand my exam style. You can find prior exams and sample answers at my website (note that the law may have changed in the interim).

While the exam style should be similar to the past years’ styles, mechanically I may administer this exam in one of the following 3 ways: (1) as an in-class exam scheduled for December 6 at 8:30 am; (2) as a take-home exam with a few hours to complete your answer, which would be scheduled for December 6 at 8:30 am; or (3) as a take-home exam with several days to complete your answer. I will announce the format later in the semester.

4. **Reader.** The course reader is the only required reading (except for any materials I distribute during the semester).

5. **TWEN.** I have built a course page in TWEN which I use, among other things, to send you emails related to the course. YOU MUST REGISTER FOR THE TWEN COURSE NO LATER THAN AUGUST 26 AT 5:00 PM OR I MAY DROP YOU FROM THE COURSE.

6. **Office Hours.** I can schedule a time to speak with you at your convenience. Please email me to make an appointment. I’m also happy to talk by email.

7. **Schedule and Readings.**

   **Introduction: What is Cyberspace? Who Regulates It?**

   ACLU v. Reno (CDA I District Ct. Facts Only) ....................................................... Page 4
   Noah v. AOL (E.D. Va.) ......................................................................................... 21

   Optional: if you’re feeling uncomfortable with your technical knowledge, consider the Animated Internet website (an animated depiction of various Internet operations).
Foundation: Jurisdiction

Toys 'R' Us v. Step Two (3d Cir.) ......................................................... 33

Foundation: Contracts

Specht v. Netscape Communications (2d Cir.) ........................................ 47
Register.com v. Verio (2d Cir.) (except Trespass to Chattels Section) ........ 82

Foundation: Trespass/CFAA

18 USC §1030 ...................................................................................... 102
Intel v. Hamidi (Cal. Sup. Ct.) ............................................................. 108
Register.com v. Verio (Trespass to Chattels Section) ......................... 100

Foundation: Copyright

Copyright Office Circular 1 .................................................................. 153

Subtopic: File Sharing
17 USC §506(a) .................................................................................. 160
BMG v. Gonzalez ................................................................................. 161
MGM Studios v. Grokster (Sup. Ct.) .................................................. 164

Subtopic: Derivative Liability
17 USC §512 (Copyright Safe Harbors) ............................................... 214
Corbis v. Amazon .............................................................................. 225

Foundation: Trademarks and Domain Names

15 USC §§1125 & 1129 (Infringement, Dilution and ACPA) ................. 260
15 USC §1114 (Trademark Safe Harbors) ........................................... 267
Domain Name Dispute Resolution Policy and rules ............................ 270
Trademark FAQs .............................................................................. 289
Trademark Handout ......................................................................... 294
ACPA/UDRP Handout ..................................................................... 295
Bosley Medical Institute v. Kremer (9th Cir.) .................................... 296
Promatek v. Equitrac (7th Cir.) Original Order and Revision ............. 314
Lockheed Martin v. Network Solutions (9th Cir.) ............................... 324

Foundation: Pornography

Lamoreaux (9th Cir.) .......................................................................... 330
Pornography Handout ..................................................................... 330
Reno v. ACLU (Sup. Ct. 1997) ............................................................ 331
Ashcroft v. ACLU (Sup. Ct. 2004) ...................................................... 357
Foundation: Defamation and Information Torts

47 USC §230 (Safe Harbor for Interactive Computer Services) ........................................... 389
Zeran v. America Online (4th Cir.) ................................................................................ 392

Foundation: Privacy

16 CFR Part 312 (Regulations Implementing COPPA) ..................................................... 402
In re. Pharmatrak (1st Cir.) ............................................................................................... 410

Application: Spam

Where's the Beef? Dissecting Spam's Purported Harms ..................................................... 438
CAN-SPAM Act of 2003 ...................................................................................................... 453
16 CFR Part 316 (CAN-SPAM implementing regulations) .............................................. 474
Federal Trade Commission v. Phoenix Avatar (July 30, 2004 ruling) ............................. 481

Application: Search Engines

Ticketmaster v. Tickets.com (March 2003 Ruling) ............................................................... 506
Playboy v. Netscape (9th Cir. 2004) .................................................................................. 513

Application: Adware/Spyware

Spyware: Background and Policy Issues for Congress (May 16, 2005 version) .............. 536
1-800 Contacts v. WhenU (2d Cir. 2005) .......................................................................... 548
Utah Spyware Control Act (2005 amended version) ......................................................... 577
Will the Adware Industry Beat Spitzer? .......................................................................... 587

8. CONTACT INFORMATION.

Eric Goldman
Marquette University Law School, Room 109E
1103 W. Wisconsin Avenue
Milwaukee, WI 53233
Phone: 414-288-5232
Fax: 414-288-6403
Email: eric.goldman@marquette.edu

In all emails to me related to this course, please put the words “cyberlaw” in the subject line so that I can keep my courses straight (and avoid unintentional deletion as spam).

More course-related materials, including an electronic copy of this syllabus, are available at www.ericgoldman.org.
II. FINDINGS OF FACT

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

The Nature of Cyberspace

The Creation of the Internet and the Development of Cyberspace

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

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

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

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

4
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-sponsore[d 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:

http://www.pas.rochester.edu/~mbanks/CDA/decision/facts.html 8/5/2005
o THE NATURE OF CYBERSPACE
o CREATION OF THE INTERNET AND THE DEVELOPMENT OF CYBERSPACE
o HOW PEOPLE ACCESS THE INTERNET
o 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.

http://www.pas.rochester.edu/~mbanks/CDA/decision/facts.html 8/5/2005
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
CyberNOT list. The server provides software developers with access to a PICS rating service, and allows software developers to test their products' ability to interpret standard PICS labels. Microsystmets is also offering its PICS client test program for Windows free of charge. The client program can be used by developers of PICS rating services to test their services and products.

SurfWatch

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

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

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

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

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

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

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

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

Content on the Internet

74. The types of content now on the Internet defy easy classification. The entire card catalogue of the Carnegie Library is on-line, together with journals, journal abstracts, popular magazines, and titles of compact discs. The director of the Carnegie Library, Robert Croneberger, testified that on-line services are the emerging trend in libraries generally. Plaintiff Hotwired Ventures LLC organizes its Web site into information regarding travel, news and commentary, arts and entertainment, politics, and types of drinks. Plaintiff America Online, Inc., not only creates chat rooms for a broad variety of topics, but also allows members to create their own chat rooms to suit their own tastes. The ACLU uses an America Online chat room as an 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 non-profit entities or public interest groups to reach their desired audiences. There are examples in the parties' stipulation of some of the non-commercial uses that the Internet serves. Plaintiff Human Rights Watch, Inc., offers information on its Internet site regarding reported human rights abuses around the world. Plaintiff National Writers Union provides a forum for writers on issues of concern to them. Plaintiff Stop Prisoner Rape, Inc., posts text, graphics, and statistics regarding the incidence and prevention of rape in prisons. Plaintiff Critical Path AIDS Project, Inc., offers information on safer sex, the transmission of HIV, and the treatment of AIDS.

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

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

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

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

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

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

Sexually Explicit Material On the Internet

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

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

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

85. Once a provider posts content on the Internet, it is available to all other Internet users worldwide. Similarly, once a user posts a message to a newsgroup or bulletin board, that message becomes available to all subscribers to that newsgroup or bulletin board. For example, when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing -- wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague. A chat room organized by the ACLU to discuss the United States Supreme Court's decision in FCC v. Pacifica Foundation would transmit George Carlin's seven dirty words to anyone who enters. Messages posted to a newsgroup dedicated to the Oklahoma City bombing travel to all subscribers to that newsgroup.

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

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

88. Communications over the Internet do not "invasive" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content "by accident." A document's title or a
description of the document will usually appear before the document itself takes the step needed to view it, and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content. Even the Government's witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a sexually explicit site by accident.

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

**Obstacles to Age Verification on the Internet**

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

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

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

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

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

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

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

The Practicalities of the Proffered Defenses

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

Credit Card Verification

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

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

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

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

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

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

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

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

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

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

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

The Government's "Tagging" Proposal

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

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

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

111. The task of screening and tagging cannot be done simply by using software which screens for certain words, as Dr. Olsen acknowledged, and we find that determinations as to what is indecent require human judgment.
112. In lieu of reviewing each file individually, a content provider could tag its entire site but this would prevent minors from accessing much material that is not "indecent" under the CDA.

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

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

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

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

The Problems of Offshore Content and Caching

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

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

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

http://www.pas.rochester.edu/~mbanks/CDA/decision/facts.html 8/5/2005
America Online's caching service rather than from the New York Times's server.[21]

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

Anonymity

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

Plaintiffs' Choices Under the CDA

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

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

[on to CONCLUSIONS OF LAW]

Footnotes

1. [referenced in INTRODUCTION]
2. [referenced in INTRODUCTION]
3. [referenced in INTRODUCTION]
4. [referenced in INTRODUCTION]
5. [referenced in INTRODUCTION]
6. [referenced in INTRODUCTION]
7. [referenced in INTRODUCTION]
8. The court again expresses its appreciation to the parties for their cooperative attitude in evolving the stipulation.
9. The Government has not by motion challenged the standing of any plaintiff in either case, and we harbor no doubts of our own on that point, notwithstanding the Government's suggestion in a footnote of its post-hearing brief. See Defendants' Post-Hearing Memorandum at 37 n.46 ("Plaintiffs' assertions as to the speech at issue are so off-point as to raise standing concerns."). Descriptions of these plaintiffs, as well as of the nature and content of the speech they contend is or may be affected by the CDA, are set forth in paragraphs 70 through 356 at pages 30 through 103 of the parties' stipulation filed in these actions. These paragraphs will not be reproduced here, but will be deemed adopted as Findings of the court.
10. It became clear from the testimony that moderated newsgroups are the exception and unmoderated newsgroups are the rule.
11. The evidence adduced at the hearings provided detail to this paragraph of the parties' stipulation. See Findings 95 to 107.

12. Testimony adduced at the hearing suggests that market forces exist to limit the availability of material on-line that parents consider inappropriate for their children. Although the parties sharply dispute the efficacy of so-called "parental empowerment" software, there is a sufficiently wide zone of agreement on what is available to restrict access to unwanted sites that the parties were able to enter into twenty-one paragraphs of stipulated facts on the subject, which form the basis of paragraphs 49 through 69 of our Findings of fact. Because of the rapidity of developments in this field, some of the technological facts we have found may become partially obsolete by the time of publication of these Findings.

13. This membership is constantly growing, according to the testimony of Albert Vezza, Chairman of the World Wide Web Consortium. See also Defendants' Ex. D-167.

14. See also Defendants' Ex. D-174 and the testimony of Mr. Vezza.

15. From this point, our Findings are, unless noted, no longer based upon the parties' stipulation, but upon the record adduced at the hearings.

16. Mr. Bradner is a member of the Internet Engineering Task Force, the group primarily responsible for Internet technical standards, as well as other Internet-related associations responsible for, among other things, the prevailing Internet Protocols. He is also associated with Harvard University.

17. Dr. Olsen chairs the Computer Science Department at Brigham Young University in Provo, Utah, and is the recently-appointed Director of the Human Computer Interaction Institute at Carnegie- Mellon University in Pittsburgh, Pennsylvania.

18. The term "information content provider" is defined in 509 of the CDA, at the new 47 U.S.C. 230(e)(3), 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."

19. By "verification", we mean the method by which a user types in his or her credit card number, and the Web site ensures that the credit card is valid before it allows the user to enter the site.

20. InterNIC is a naming organization, not a regulator of content. InterNIC and two other European organizations maintain a master list of domain names to ensure that no duplication occurs. Creators of Web sites must register their domain name with InterNIC, and the agency will instruct the creator to choose another name if the new Web site has the name of an already-existing site. InterNIC has no control over content on a site after registration.

21. This paragraph and the preceding paragraph also illustrate that a content provider might store its own material or someone else's on a caching server. The goal -- saving money and time -- is the same in both cases.
261 F.Supp.2d 532

United States District Court,
E.D. Virginia,
Alexandria Division.

Saad NOAH, Plaintiff,
v.
AOL TIME WARNER INC. and America Online, Inc., Defendants.

No. CIV.A. 02-1316-A.

MEMORANDUM OPINION

ELLIS, District Judge.

Plaintiff, on behalf of himself and a class of those similarly situated, sues his Internet service provider (ISP) for damages and injunctive relief, claiming that the ISP wrongfully refused to prevent participants in an online chat room from posting or submitting harassing comments that blasphemed and defamed plaintiff's Islamic religion and his co-religionists. Specifically, plaintiff claims his ISP's failure to prevent chat room participants from using the ISP's chat room to publish the harassing and defamatory comments constitutes a breach of the ISP's customer agreement with plaintiff and a violation of Title II of the Civil Rights Act of 1964, 42 U.S.C. <section> 2000a et seq.

At issue on a threshold dismissal motion are
(i) the now familiar and well-litigated question whether a claim, like plaintiff's, which seeks to hold an ISP civilly liable as a publisher of third party statements is barred by the immunity granted ISP's by the Communications Decency Act of 1996, 47 U.S.C. <section> 230,
(ii) the less familiar, indeed novel question whether an online chat room is a "place of public accommodation" under Title II, and
(iii) the rather prosaic question whether plaintiff's breach of contract claim is barred by the very contract on which he relies, namely the Member Agreement contract.

For the reasons that follow, plaintiff's claims do not survive threshold inspection and must therefore be dismissed.

I. [FN1]

FN1. The facts recited here are derived from the complaint and taken as true for purposes of resolving the dismissal motion at bar. See Harrison v. Westinghouse Savannah River Co., 176 F.3d 776, 783 (4th Cir.1999).
Plaintiff Saad Noah, a Muslim, is a resident of Illinois and was a subscriber of defendant America Online, Inc. ("AOL")'s Internet service until he cancelled the service in July of 2000. AOL, which is located in the Eastern District of Virginia, is, according to the complaint, the world's largest Internet service provider, with more than 30 million subscribers, or "members," worldwide. Defendant AOL Time Warner Inc. is the parent company of AOL.

Among the many services AOL provides its members are what are popularly known as "chat rooms." These occur where, as AOL does here, an ISP allows its participants to use its facilities to engage in real-time electronic conversations. Chat room participants type in their comments or observations, which are then read by other chat room participants, who may then type in their responses. Conversations in a chat room unfold in real time; the submitted comments appear transiently on participants' screens and then scroll off the screen as the conversation progresses. AOL chat rooms are typically set up for the discussion of a particular topic or area of interest, and any AOL member who wishes to join a conversation in a public chat room may do so.

Two AOL chat rooms are the focus of plaintiff's claims: the "Beliefs Islam" chat room and the "Koran" chat room. It is in these chat rooms that plaintiff alleges that he and other Muslims have been harassed, insulted, threatened, ridiculed and slandered by other AOL members due to their religious beliefs. The complaint lists dozens of harassing statements made by other AOL members in these chat rooms on specified dates, all of which plaintiff alleges he brought to AOL's attention together with requests that AOL take action to enforce its member guidelines and halt promulgation of the harassing statements. The statements span a period of two and one-half years, from January 10, 1998 to July 1, 2000, and are attributable to various AOL chat room participants only by virtue of a screen name. A representative sample of the reported offensive comments follows:

(i) On January 10, 1998 the AOL Member with the screen name "Aristotlee" wrote "islam is meaniglessssss thought," "allahsick cut offfffffff," "dumballah bastard," "allah assssshole," "allahs dick is in holy dick place hey." "FUCK ALLAH," etc.
(iii) On November 4, 1998, "Hefedehefe" wrote "SMELLY TOWEL HEADS" and "MUSLIM TOWEL HEADS."
(iv) On July 11, 1999, "Jzingher" wrote "The Koran and Islam are creations of Satan to distract people from the true faith which is Judaism. Mohammed was merely a huckster who found a simple people he could manipulate."
(v) On July 18, 1999 "SARGON I" wrote "Qura'n lies about everything-a Satan made
verses of darkness and destruction!", "Mohammed was no shit, only a killer, thief, a liar and a adulterer!", and "BYE STUPID MUSLIMS....ALL GO TO HELL."

(vi) On July 1, 2000, "DXfina3000 wrote "muslims suck," "they suck ass," "korans is use to wipe ass," "fuckin muslins," and "well allah can suck my dick you peice of ass."

Plaintiff understandably complained about these offensive, obnoxious, and indecent statements, initially through the channels provided by AOL for such complaints and eventually through emails sent directly to AOL’s CEO Steve Case. Plaintiff alleges that although he reported every one of the alleged violations to AOL, AOL refused to exercise its power to eliminate the harassment in the "Beliefs Islam" and "Koran" chat rooms. Moreover, plaintiff contends that AOL gave a "green light" to the harassment of Muslims in these forums, claiming that such harassment was not tolerated in chat rooms dealing with other subjects and faiths. In protest, plaintiff cancelled his AOL account in July 2000. Plaintiff further alleges that other Muslim members of AOL have also complained to AOL about similar harassing statements.

The relationship between AOL and each of its subscribing members is governed by the Terms of Service ("TOS"), which include a Member Agreement and the Community Guidelines. The Member Agreement is a "legal document that details [a member's] rights and obligations as an AOL member," and it requires, inter alia, that AOL members adhere to AOL's standards for online speech, as set forth in the Community Guidelines. These Guidelines state, in pertinent part, that

... You will be considered in violation of the Terms of Service if you (or others using your account) do any of the following: ....
* Harass, threaten, embarrass, or do anything else to another member that is unwanted. This means: ... don't attack their race, heritage, etc....
* Transmit or facilitate distribution of content that is harmful, abusive, racially or ethnically offensive, vulgar, sexually explicit, or in a reasonable person's view, objectionable. Community standards may vary, but there is no place on the service where hate speech is tolerated.
* Disrupt the flow of chat in chat rooms with vulgar language, abusiveness, ...

The Member Agreement states that AOL has the right to enforce these Community Guidelines "in its sole discretion." In response to a violation, "AOL may take action against your account," ranging from "issuance of a warning about a violation to termination of your account." AOL's Community Action Team is responsible for enforcing the content and conduct standards and members are encouraged to notify AOL of violations they observe online. Importantly, however, the Member Agreement states that AOL members "... also understand and agree that the AOL Community Guidelines and the AOL Privacy Policy, including AOL's enforcement of those policies, are not intended to confer, and do not confer, any rights or remedies upon any person."

Plaintiff filed this pro se action on September 3, 2002, claiming that AOL's alleged refusal to intervene to stop the harassing statements and enforce the TOS
constitutes (i) discrimination in a place of public accommodation, in violation of Title II of the Civil Rights Act of 1964, 42 U.S.C. § 2000a, and (ii) a breach of AOL's TOS and the Member Agreement. The action purports to be a class action, brought on behalf of plaintiff and all others similarly situated.

In addition to these claims raised in the complaint, plaintiff seems to assert a third claim against defendants in his response to the motion to dismiss, where he alleges new facts concerning several incidents involving disciplinary actions taken by AOL against plaintiff and other, unnamed Muslim AOL members. Although the nature of the incidents is not entirely clear, plaintiff alleges that AOL discriminated against plaintiff and other Muslim AOL members by issuing false warnings against them and terminating their accounts in an effort to silence their pro-Islam speech. Plaintiff alleges his own AOL account was briefly terminated by AOL and subsequently reinstated, but his past messages were not restored. Relying on these incidents, plaintiff belatedly claims a violation of his First Amendment rights and of the First Amendment rights of similarly situated Muslims. Although not properly pled in the complaint, given plaintiff's pro se status this claim will nonetheless be considered on this motion to dismiss as if it had been raised in the original complaint. [FN2]

FN2. While it is true, as courts have uniformly noted, that pro se plaintiffs' pleadings should be charitably read, it is not and should not be the task of courts to sift through the facts alleged in a complaint to advise pro se plaintiffs of what claims they might have. See Weller v. Dep't of Soc. Serv. for the City of Baltimore, 901 F.2d 387, 391 (4th Cir. 1990) (noting that "the 'special judicial solicitude' with which a district court should view such pro se complaints does not transform the court into an advocate").

Defendants AOL and AOL Time Warner filed a motion to dismiss plaintiff's claims on January 22, 2003. Nearly a month later, two days before the motion was noticed for a hearing, plaintiff belatedly requested and ultimately received, as a matter of grace, an extension of time until March 7, 2003, in which to file his response. See Noah v. AOL Time Warner, Inc., Civil Action No. 02-1316-A (E.D. Va. February 20, 2003) (Order). Plaintiff missed this deadline as well, filing his response on March 10, 2003. Thereafter, defendants filed their reply on March 17, 2003. Because the issues and governing authorities are adequately set forth in the pleadings, oral argument is unnecessary and may be dispensed with, and this motion is appropriately disposed of on the papers.

II.

[1] As an initial matter, it must be noted that plaintiff, as a pro se litigant, may not pursue his claims as a class action for the obvious and sensible reason that a pro se plaintiff is simply not equipped by reason of training or experience to
provider ... of an interactive computer service shall be treated as the publisher" of third-party content. 47 U.S.C. § 230(e)(1); see Kathleen R. v. City of Livermore, 87 Cal.App.4th 684, 104 Cal.Rptr.2d 772 (2001) (distinguishing Loudoun on these grounds).

In sum, § 230 bars plaintiff's claim under Title II because it seeks to treat AOL as the publisher of the allegedly harassing statements of other AOL members. To be sure, the offensive statements plaintiff complains of are a far cry from the "diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity" that § 230 is intended to promote and protect. 47 U.S.C. § 230(a). Indeed, the statements reported by plaintiff suggest a darker side of what has been called the "robust nature of Internet communication." Zeran, 129 F.3d at 330. Nonetheless, § 230 reflects Congress's judgment that imposing liability on service providers for the harmful speech of others would likely do more harm than good, by exposing service providers to unmanageable liability and potentially leading to the closure or restriction of such open forums as AOL's chat rooms. Id. at 331. Accordingly, under § 230, plaintiff may not seek recourse against AOL as publisher of the offending statements; instead, plaintiff must pursue his rights, if any, against the offending AOL members themselves.

B.

[5] Even assuming, arguendo, that plaintiff's Title II claim is not barred by § 230, it must nonetheless be dismissed for failure to state a claim because AOL's chat rooms and other online services do not constitute a "place of public accommodation" under Title II.

Title II provides that "[a]ll persons shall be entitled to full and equal enjoyment of the goods, services, facilities, privileges, advantages, and accommodations of any place of public accommodation, as defined in this section, without discrimination or segregation on the ground of race, color, religion, or national origin." 42 U.S.C. § 2000a(a). Title II defines a "place of public accommodation" as follows:

Each of the following establishments which serves the public is a place of public accommodation within the meaning of this subchapter ...

(1) any inn, hotel, motel, or other establishment which provides lodging to transient guests, other than an establishment located within a building which contains not more than five rooms for rent or hire and which is actually occupied by the proprietor of such establishment as his residence;

(2) any restaurant, cafeteria, lunchroom, lunch counter, soda fountain, or other facility principally engaged in selling food for consumption on the premises, including, but not limited to, any such facility located on the premises of any retail establishment; or any gas station;

(3) any motion picture house, theater, concert hall, sports arena, stadium or other place of exhibition or entertainment; and
any establishment (A)(i) which is physically located within the premises of any establishment otherwise covered by this subsection, or (ii) within the premises of which is physically located any such covered establishment, and (B) which holds itself out as serving patrons of such covered establishment.

42 U.S.C. <section> 2000a(b).

The theory of plaintiff's Title II claim is that he was denied the right of equal enjoyment of AOL's chat rooms because of AOL's alleged failure to take steps to stop the harassing comments and because of AOL's warnings to plaintiff and brief termination of plaintiff's service. In this regard, plaintiff contends that the chat rooms are "place[s] of ... entertainment" and thus within the public accommodation definition. 42 U.S.C. <section> 2000a(b)(3). Yet, as the relevant case law and an examination the statute's exhaustive definition make clear, "places of public accommodation" are limited to actual, physical places and structures, and thus cannot include chat rooms, which are not actual physical facilities but instead are virtual forums for communication provided by AOL to its members.

Title II's definition of "places of public accommodation" provides a list of "establishments" that qualify as such places. This list, without exception, consists of actual physical structures; namely any "inn, hotel, motel, ... restaurant, cafeteria, lunchroom, lunch counter, soda fountain, ... gasoline station ... motion picture house, theater, concert hall, sports arena [or] stadium." 42 U.S.C. <section> 2000a(b)(1)-(3). In addition, <section> 2000a(b)(4) emphasizes the importance of physical presence by referring to any "establishment ... which is physically located within" an establishment otherwise covered, or "within ... which" an otherwise covered establishment "is physically located." 42 U.S.C. <section> 2000a(b)(4) (emphasis added). Thus, in interpreting the catchall phrase "other place of exhibition or entertainment" on which plaintiff relies, the statute's consistent reference to actual physical structures points convincingly to the conclusion that the phrase does not include forums for entertainment that are not physical structures or locations. 42 U.S.C. <section> 2000a(b)(3); see Welsh v. Boy Scouts of America, 993 F.2d 1267, 1269 (7th Cir.1993) (holding that the statute, "in listing several specific physical facilities, sheds light on the meaning of 'other place of ... entertainment' "); Clegg v. Cult Awareness Network, 18 F.3d 752, 755 (9th Cir.1994) (holding that, by its plain language, Title II covers only "places, lodgings, facilities and establishments open to the public").

As the Supreme Court has held, <section> 2000a(b)(3) should be read broadly to give effect to the statute's purpose, namely to eliminate the "daily affront and humiliation" caused by "discriminatory denials of access to facilities ostensibly open to the general public." Daniel v. Paul, 395 U.S. 298, 306, 307-08, 89 S.Ct. 1697, 23 L.Ed.2d 318 (1969) (holding that an amusement park with facilities for swimming, boating, miniature golf, and dancing is a "place of entertainment" under Title II) (emphasis added). This broad coverage stems from a "natural reading of [the statute's] language," which should be "given full effect according to its generally accepted meaning." Id. As such, it is clear that the reach of Title II,
however broad, cannot extend beyond actual physical facilities. Given Title II's sharp focus on actual physical facilities, such as inns, motels, restaurants, gas stations, theaters, and stadiums, it is clear that Congress intended the statute to reach only the listed facilities and other similar physical structures, not to "regulate a wide spectrum of consensual human relationships." Welsh, 993 F.2d at 1270.

This emphasis on actual physical facilities is reinforced by the cases rejecting Title II claims against membership organizations. In Welsh, the plaintiffs, who were atheists, claimed that the Boy Scouts of America violated Title II in denying them membership, arguing that the Boy Scouts were a "place of ... entertainment." The majority of the Seventh Circuit panel in Welsh concluded that the Boy Scouts of America is not a "place of public accommodation" under Title II because it is not "closely connected to a particular facility." Welsh, 993 F.2d at 1269. [FN7] In doing so, the Welsh majority distinguished the Boy Scouts from membership organizations in which membership "functions as a 'ticket' to admission to a facility or location," that have been consistently held to be places of public accommodation under Title II. Id. at 1272. [FN8] Similarly, the Ninth Circuit in Clegg held that the Cult Awareness Network, a nonprofit organization that provides information to the public concerning cults and supports former cult members, was not a "place of public accommodation" because it had "no affiliation with any public facility." Clegg, 18 F.3d at 755. In short, it is clear from the cases considering membership organizations that status as a place of public accommodation under Title II requires some connection to some specific physical facility or structure. As noted in Welsh and Clegg, to ignore this requirement is to ignore the plain language of the statute and to render the list of example facilities provided by the statute superfluous. See Welsh, 993 F.2d at 1269; Clegg, 18 F.3d at 755.

FN7. Notably, the Boy Scouts have been deemed a place of public accommodation under the broader New Jersey state public accommodation law. See Boy Scouts of America v. Dale, 530 U.S. 640, 656-57, 120 S.Ct. 2446, 147 L.Ed.2d 554 (2000). The Supreme Court in Dale noted that the New Jersey Supreme Court's failure to "even attempt[ ] to tie the term 'place' to a physical location" increased the potential for a conflict between the state public accommodations laws and the First Amendment. Id. at 657, 120 S.Ct. 2446. In doing so, the Supreme Court implicitly endorsed the rationale behind a "physical facility" requirement in federal Title II law. See id. at 657 n. 3, 120 S.Ct. 2446 (noting that the New Jersey Supreme Court stands alone in its treatment of the Boy Scouts as a place of public accommodation).

FN8. See, e.g., Smith v. YMCA of Montgomery, 462 F.2d 634, 636 (5th Cir.1972) (holding that Title II reaches YMCA that operates gymnasiums, a health club, and swimming pool); Nesmith v. YMCA of Raleigh, N.C., 397 F.2d 96, 99-100 (4th Cir.1968) (same); United States v. Lansdowne Swim Club, 713 F.Supp. 785, 790
In arguing that places of public accommodation are not limited to actual physical facilities under Title II, plaintiff turns to the case law interpreting the analogous "place of public accommodation" provision under Title III of the Americans With Disability Act (ADA). See 42 U.S.C. § 12182 (prohibiting discrimination in any place of public accommodation on the basis of disability); § 12181(7) (defining "place of public accommodation"). While the case law concerning places of public accommodation under the ADA is more abundant than that under Title II, it is not entirely uniform. Yet, a detour into the parallel ADA cases is instructive and ultimately supports the conclusion that "places of public accommodation" must consist of, or have a clear connection to, actual physical facilities or structures.

The circuits are split regarding the essential question whether a place of public accommodation under the ADA must be an actual concrete physical structure. On the one hand, as plaintiff notes, the First Circuit has held that "places of public accommodation" under Title III of the ADA are not limited to actual physical facilities. See Carpahets Distribution Center, Inc. v. Automotive Wholesalers Assoc. of New England, Inc., 37 F.3d 12, 18-20 (1st Cir.1994) (holding that a trade association which administers a health insurance program, without any connection to a physical facility, can be a "place of public accommodation"). [FN9] On the other hand, the Third, Sixth and Ninth Circuits, in similar cases involving health insurance programs, followed the logic of Welsh and Clegg in holding that places of public accommodation under Title III of the ADA must be physical places. See Parker v. Metropolitan Life Insurance Co., 121 F.3d 1006, 1014 (6th Cir.1997) (holding that "the clear connotation of the words in § 1218(7) is that a public accommodation is a physical place," because "[e]very term listed in § 1218(7) ... is a physical place open to public access"); Ford v. Schering-Plough Corp., 145 F.3d 601, 612-13 (3rd Cir.1998) (holding that "the plain meaning of Title III is that a public accommodation is a place," and that § 1218(7) does not "refer to non-physical access"); Weyer v. Twentieth Century Fox Film Corp., 198 F.3d 1104, 1114-16 (9th Cir.2000) (following Parker and Ford). Thus, it appears that the weight of authority endorses the "actual physical structure" requirement in the ADA context as well. [FN10]

FN9. In reaching this conclusion, the First Circuit in Carpahets relied on the ADA's more expansive definition of "place of public accommodation," in particular its inclusion of a "travel service," "insurance office," and "other service establishments" as places of public accommodation Id. at 19; 42 U.S.C. § 12181(7). Focusing on these terms, the First Circuit concluded that
"Congress clearly contemplated that 'service establishments' include providers of services which do not require a person to physically enter an actual physical structure," and thus that the Title III of the ADA is not limited to "physical structures which person must enter to obtain goods and services." Id. at 19-20. Simply put, the Carparts court found it irrational to conclude that Title III of the ADA reaches those who enter an office to purchase insurance services, but not those who purchase them over the mail or by telephone. Id. at 19. Notably, Title II of the Civil Rights Act does not include a "travel service," "insurance office," or "other service establishments" in its definition, making the relevance of Carparts and its progeny to Title II questionable, at best.

FN10. Yet, Carparts has not been completely abandoned. Indeed, some courts have continued to follow its holding and logic in cases involving health insurance programs, including a court in this district. See Lewis v. Aetna Life Ins. Co., 982 F.Supp. 1158, 1164 (E.D.Va.1997).

Most significantly, two more recent ADA cases involving fact situations much closer to those at bar reaffirm the principle that a "places of public accommodation," even under the ADA's broader definition, must be actual, physical facilities. In one case, the plaintiffs claimed that Southwest Airlines was in violation of the ADA because its "southwest.com" web site was incompatible with "screen reader" programs and thus inaccessible to blind persons. See Access Now, Inc. v. Southwest Airlines, Co., 227 F.Supp.2d 1312, 1316 (S.D.Fla.2002). Thus, the question presented was whether the airline's web site, which serves as an online ticket counter, constitutes a "place of public accommodation" under the ADA. The Access Now court held that places of public accommodation under the ADA are limited to "physical concrete structures," and that the web site was not an actual physical structure. Id. at 1319. Rejecting the invitation to endorse the Carparts approach and apply the ADA to Internet web sites despite their lack of physical presence, the Access Now court concluded that "[i]f the ADA to cover 'virtual' spaces would create new rights without well-defined standards." Id. at 1318. [FN11] Similarly, in another case, plaintiff contended that the defendant's digital cable system was in violation of the ADA because its on-screen channel guide was not accessible to the visually impaired. See Torres v. AT & T Broadband, LLC, 158 F.Supp.2d 1035, 1037-38 (N.D.Cal.2001). Here too, the district court rejected the notion that the digital cable system was a "place of public accommodation," because "in no way does viewing the system's images require the plaintiff to gain access to any actual physical public place," Id. at 1038 (citing Weyer, 198 F.3d at 1114-16). Furthermore, the Torres court sensibly concluded that the mere fact that the digital cable system relied on physical facilities to support and transmit its services did not convert the cable service into a "physical public place." Id. at 1038.

FN11. But see Doe v. Mutual of Omaha Ins. Co., 179 F.3d 557, 559 (7th Cir.1999)
(citing Carparts approvingly and stating, in dicta, that Title III of the ADA reaches "the owner or operator of a store, hotel, restaurant, dentist's office, travel agency, theater, Web site, or other facility (whether in physical space or in electronic space") (emphasis added) (citation omitted).

In sum, whether one relies on the Title II case law or looks to the broader ADA definition of public place of accommodation, it is clear that the logic of the statute and the weight of authority indicate that "places of entertainment" must be actual physical facilities. With this principle firmly established, it is clear that AOL's online chat rooms cannot be construed as "places of public accommodation" under Title II. An online chat room may arguably be a "place of entertainment," but it is not a physical structure to which a member of the public may be granted or denied access, and as such is fundamentally different from a "motion picture house, theater, concert hall, sports arena, [or] stadium." 42 U.S.C. § 2000a(b)(3) . Although a chat room may serve as a virtual forum through which AOL members can meet and converse in cyberspace, it is not an "establishment," under the plain meaning of that term as defined by the statute. Unlike a theater, concert hall, arena, or any of the other "places of entertainment" specifically listed in § 2000a(b), a chat room does not exist in a particular physical location, indeed it can be accessed almost anywhere, including from homes, schools, cybercafes and libraries. In sum, although a chat room or other online forum might be referred to metaphorically as a "location" or "place," it lacks the physical presence necessary to constitute a place of public accommodation under Title II. See Access Now, 227 F.Supp.2d at 1312 (holding that an airline's online ticket service, which is arguably a "virtual" version of its physical ticket counters, is not a "place of public accommodation" because it is not a "physical concrete structure"); Torres, 158 F.Supp.2d at 1038 (holding that a digital cable system is not an "actual physical public place"). Accordingly, even if plaintiff's Title II claim were not barred by § 230's grant of immunity to service providers, it would be fail on the independent ground that AOL's chat rooms are not places of public accommodation. [FN12]

FN12. Plaintiff's Title II claim suffers additional infirmities, as well. First, plaintiff requests compensatory and punitive damages for his Title II claim, but he is not entitled to recover damages under Title II. See Newman v. Piggie Park Enters., 390 U.S. 400, 401, 88 S.Ct. 964, 19 L.Ed.2d 1263 (holding that "[w]hen a plaintiff brings an action under [Title II], he cannot recover damages"). Second, because plaintiff cancelled his AOL membership well before this action was filed, he may not be able to show "continuing, present adverse effects" and therefore may lack standing to seek injunctive relief. See City of Los Angeles v. Lyons, 461 U.S. 95, 102, 103 S.Ct. 1660, 75 L.Ed.2d 675 (1983). Finally, construing Title II as plaintiff requests, to require that AOL censor or limit the speech of its members, may well cause the statute to run afoul of the First Amendment. See Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, 515 U.S. 557, 579, 115 S.Ct. 2338, 132 L.Ed.2d 487 (1995).
V.

[6] Plaintiff’s breach of contract claim must likewise be dismissed because the contractual rights plaintiff claims are simply not provided for in AOL’s Member Agreement. The plain language of the Member Agreement makes clear that AOL is not obligated to take any action against those who violate its Community Guidelines. Thus, the Member Agreement provides that AOL "has the right to enforce them in its sole discretion," and that "if you ... violate the AOL Community Guidelines, AOL may take action against your account." (emphasis added). The Member Agreement also states that "[y]ou also understand and agree that the AOL Community Guidelines and the AOL Privacy Policy, including AOL's enforcement of those policies, are not intended to confer, and do not confer, any rights or remedies upon any person." (emphasis added). The Member Agreement states that while AOL "reserve[s] the right to remove content that, in AOL's judgment, does not meet its standards or does not comply with AOL's current Community Guidelines ... AOL is not responsible for any failure or delay in removing such material."

In light of this plain contractual language, plaintiff cannot claim that AOL breached a duty to protect him from the harassing speech of others; the Member Agreement expressly disclaims any such duty. Furthermore, as the Third Circuit noted in Green, AOL’s disclaimer of any obligation to enforce its Community Guidelines is perfectly in line with the evident Congressional intent of <section>230, namely to ensure that service providers are not held responsible for content provided by third parties. See Green, 318 F.3d at 471 (noting that "the Member Agreement between the parties tracks the provisions of section 230"); see also Zerec, 129 F.3d at 331 (noting that Congress enacted <section>230 to ensure that service providers could self-regulate the dissemination of offensive material without exposing themselves to liability as publishers as a result of such self-regulation).

Furthermore, plaintiff’s attempt to cast this claim as a third-party beneficiary claim is unavailing. Under the Member Agreement, AOL no more owes a duty to other AOL members to enforce its Community Guidelines than it does with respect to plaintiff.

E.

[7] Finally, plaintiff’s belatedly-raised First Amendment claim is easily disposed of at this stage. In essence, plaintiff claims that AOL violated his First Amendment rights by issuing him warnings and briefly terminating his account, allegedly in response to his pro-Islamic statements. Yet, even assuming the truth of plaintiff’s allegations, the First Amendment is of no avail to him in these circumstances; it does not protect against actions taken by private entities, rather it is "a guarantee only against abridgment by government, federal or state." Hudgens v. NLRB, 424 U.S. 507, 513, 96 S.Ct. 1029, 47 L.Ed.2d 196 (1976). Plaintiff does not argue that AOL is a state actor, nor is there any evident basis for such an
argument. See Green, 318 F.3d at 472 (noting that AOL is a "private, for profit company" and rejecting the argument that AOL should be treated as a state actor); Cyber Promotions Inc. v. American Online, Inc., 948 F.Supp. 436, 441-44 (E.D.Pa.1996) (rejecting the argument that AOL is a state actor). Accordingly, because AOL is not a state actor, plaintiff's First Amendment claim must be dismissed.

An appropriate order will issue.
PRECEDENTIAL

Filed January 27, 2003

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 01-3390

TOYS "R" US, INC.;
GEOFFREY, INC.,

Appellants

v.

STEP TWO, S.A.;
IMAGINARIUM NET, S.L.

ON APPEAL FROM THE
UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF NEW JERSEY

District Court Judge: Honorable Katharine S. Hayden
(D.C. No. 01-00632)

Argued: September 12, 2002

Before: ALITO and FUENTES, Circuit Judges,
and OBERDORFER,* District Judge.

(Opinion Filed: January 27, 2003)

* The Honorable Louis F. Oberdorfer, Senior District Judge for the
District of Columbia, sitting by designation.

PAUL FIELDS (Argued)
ROBERT S. WEISBEN
HEATHER C. WILDE
Darby & Darby
805 Third Avenue
New York, NY 10022

Counsel for Appellants

SUSAN H. FARINA
MARK G. MATUSCHAK (Argued)
ELIZABETH M. REILLY
Hale & Dorr
60 State Street
Boston, MA 02109

Counsel for Appellees

OPINION OF THE COURT

OBERDORFER, District Judge:
Toys "R" Us, Inc. and Geoffrey, Inc. ("Toys") brought this action against Step Two, S.A. and Imaginarium Net, S.L. ("Step Two"), alleging that Step Two used its Internet websites to engage in trademark infringement, unfair competition, misuse of the trademark notice symbol, and unlawful "cybersquatting," in violation of the Lanham Act, 15 U.S.C. S 1501 et seq., and New Jersey state law. The District Court denied Toys' request for jurisdictional discovery and, simultaneously, granted Step Two's motion to dismiss for lack of personal jurisdiction. We hold that the District Court should not have denied Toys' request for jurisdictional discovery. We therefore reverse and remand for limited jurisdictional discovery, relating to Step Two's business activities in the United States, and for reconsideration of personal jurisdiction with the benefit of the product of that discovery, with a view to its renewing administration of the case, in the event the District Court finds that it does have jurisdiction.

I.

Toys, a Delaware corporation with its headquarters in New Jersey, owns retail stores worldwide where it sells toys, games, and numerous other products. In August 1999, Toys acquired Imaginarium Toy Centers, Inc., which owned and operated a network of "Imaginarium" stores for the sale of educational toys and games. As part of this acquisition, Toys acquired several Imaginarium trademarks, and subsequently filed applications for the registration of additional Imaginarium marks. Prior to Toys' acquisition, the owners of the Imaginarium mark had been marketing a line of educational toys and games since 1985 and had first registered the Imaginarium mark with the United States Patent and Trademark Office in 1989. Toys currently owns thirty-seven freestanding Imaginarium stores in the U.S., of which seven are located in New Jersey. In addition, there are Imaginarium shops within 175 of the Toys "R" Us stores in the U.S., including five New Jersey stores.

Step Two is a Spanish corporation that owns or has franchised toy stores operating under the name "Imaginarium" in Spain and nine other countries. It first registered the Imaginarium mark in Spain in 1991, and opened its first Imaginarium store in the Spanish city of Zaragoza in November 1992. Step Two began expanding its chain of Imaginarium stores by means of a franchise system in 1994. It has registered the Imaginarium mark in several other countries where its stores are located. There are now 165 Step Two Imaginarium stores. The stores have the same unique facade and logo as those owned by Toys, and sell the same types of merchandise as Toys sells in its Imaginarium stores. However, Step Two does not operate any stores, maintain any offices or bank accounts, or have any employees anywhere in the United States. Nor does it pay taxes to the U.S. or to any U.S. state. (JA 135-36.) Step Two maintains that it has not directed any advertising or
marketing efforts towards the United States. The record
does, however, indicate some contacts between Step Two
and the United States: for example, a portion of the
merchandise sold at Step Two’s Imaginarium stores is
purchased from vendors in the United States. Additionally,
Felix Tena, President of Step Two, attends the New York
Toy Fair once each year. (JA 314.)

In the mid-1990s, both parties turned to the Internet to
boost their sales. In 1995, Imaginarium Toy Centers, Inc.

(which Toys later acquired) registered the domain name
<imaginarium.com> and launched a website featuring
merchandise sold at Imaginarium stores. In 1996, Step Two
registered the domain name <imaginarium.es>, and began
advertising merchandise that was available at its
Imaginarium stores.1 In April 1999, Imaginarium Toy
Centers registered the domain name <imaginarium.net>,
and launched another website where it offered
Imaginarium merchandise for sale. In June 1999, Step Two
registered two additional "Imaginarium" domain names,
<imaginariumworld.com> and <imaginarium-world.com>. In
May 2000, Step Two registered three more domain names:
<imaginariumnet.com>, <imaginariumnet.net>, and
<imaginariumnet.org>.2 Step Two’s websites are
maintained by Imaginarium Net, S.L., a subsidiary of Step

At the time this lawsuit was filed, four of the
aforementioned sites operated by Step Two were interactive,
allowing users to purchase merchandise online.3 When
buying merchandise via Step Two’s websites, purchasers
are asked to input their name and email address, as well as
a credit card number, delivery address, and phone number.
At no point during the online purchase process are users
asked to input their billing or mailing address. The websites
provide a contact phone number within Spain that

1. Step Two maintains that goods have been available for purchase via
its website only since November 2000. Before that time, merchandise
was advertised, but not sold, online.

2. Step Two originally contracted with the European company
Intercomputer Soft, S.A. (now owned by PsiNet Europe) to register the
domain names <imaginariumworld.com> and <imaginarium-world.com>,
and with the European company Interdomain to register
<imaginariumnet.com>, <imaginariumnet.net>, and
<imaginariumnet.org>. These domain names were ultimately registered
with Network Solutions, Inc. ("NSI"), a U.S. company. Step Two pays
PsiNet Europe to maintain these domain names, and does not send any
payments to NSI. (JA 314.)

3. The websites at <imaginariumnet.com> and <imaginariumnet.net>
were not used to sell merchandise. Discovery may be necessary to
determine whether Step Two has changed its websites during the course
of this litigation.
lacks the country code that a user overseas would need to dial. Moreover, the prices are in Spanish pesetas and Euros, and goods ordered from those sites can be shipped only within Spain. Step Two’s Imaginarium web sites are entirely in Spanish.

Visitors to the four sales-oriented Step Two web sites may elect to receive an electronic newsletter, or sign up for membership in "Club Imaginarium," a promotional club with games and information for children. Each registrant for Club Imaginarium is required to provide a name and an email address. At the time this suit was filed, there was a section for "voluntary information," including the registrant’s home address, on the Club Imaginarium registration page. This optional portion of the page required users to choose from a pull-down list of Spanish provinces, and did not accommodate mailing addresses in the United States. After joining Club Imaginarium via the web site, registrants receive an automatic email response.

Mr. Tena submitted an affidavit stating that Step Two had not made any sales via its web sites to U.S. residents. (JA 136.) Toyo, however, adduced evidence of two sales to residents of New Jersey conducted via Step Two’s Imaginarium web sites. These purchases were initiated by Toyo. Lydia Leon, a legal assistant in the Legal Department of Geoffrey, Inc., made the first purchase. Ms. Leon, a resident of New Jersey, purchased a toy via <www.imaginariumworld.com> on January 23, 2001. (JA 167-69.) The second purchase was made in February 2001 by Luis M. Lopez, an employee of Darby & Darby P.C., attorneys for Toyo. Mr. Lopez is also a resident of New Jersey, and accessed <www.imaginarium.es> to make his purchase. (JA 207-14.)

For both of these sales, the items were shipped to Angeles Benavides Davila, a Toys employee in Madrid,

---

4. An earlier version of the Club Imaginarium registration form was included in the record as Exhibit N of the Affidavit of Luis M. Lopez. (JA 272.) This page asked users to input the "Province," and did not have a pull-down menu. There was no field for "Country." According to Step Two, this alternate version was available only at <www.imaginariumnet.org>.

Spain; Ms. Benavides Davila then forwarded the items to the offices of Geoffrey, Inc. in New Jersey. Both purchases were made with credit cards issued by U.S. banks. Additionally, both purchasers received in New Jersey an email confirming their purchases, and a subsequent email with a login and password to access Club Imaginarium. One of the two purchasers also separately registered for
Club Imaginarium, exchanged emails with a Step Two employee about his purchase, and received a copy of an email newsletter from Step Two. Aside from these two sales, there is no evidence in the record of a sale to anyone in the United States. After learning of these two sales, Mr. Tena submitted a second affidavit stating that his company does not know where its purchasers reside, as that information is not apparent from a purchaser's email address, and Step Two keeps records only of shipping addresses. (JA 310-11.)

On February 7, 2001, Toys filed the instant complaint against Step Two in federal district court. Step Two moved to dismiss for lack of personal jurisdiction on April 10, 2001. Toys opposed the motion, and requested discovery on the issue of jurisdiction. After hearing oral argument on July 30, 2001, the District Court denied the discovery request and granted the motion to dismiss. Toys appealed these decisions on August 28, 2001.

II.

In the following discussion, we first consider the standard for personal jurisdiction based upon a defendant's operation of a commercially interactive web site, as articulated by courts within this circuit and other Courts of Appeals. In light of that standard and the arguments presented in the proceeding below, we then assess the propriety of the District Court's denial of jurisdictional discovery.

A. Personal Jurisdiction Based on the Operation of a Web Site

The advent of the Internet has required courts to fashion guidelines for when personal jurisdiction can be based on a defendant's operation of a web site. Courts have sought to articulate a standard that both embodies traditional rules and accounts for new factual scenarios created by the Internet. Under traditional jurisdictional analysis, the exercise of specific personal jurisdiction requires that the "plaintiff's cause of action is related to or arises out of the defendant's contacts with the forum." Pinker v. Roche Holdings Ltd., 292 F.3d 361, 368 (3d Cir. 2002). Beyond this basic nexus, for a finding of specific personal jurisdiction, the Due Process Clause of the Fifth Amendment requires (1) that the "defendant ha[ve] constitutionally sufficient 'minimum contacts' with the forum," id. (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 474 (1985)), and (2) that "subjecting the defendant to the court's jurisdiction comports with 'traditional notions of fair play and substantial justice,'" id. (quoting Int'l Shoe Co. v. Washington, 326 U.S. 301, 316 (1945)). The first requirement, "minimum contacts," has been defined as "'some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits

The precise question raised by this case is whether the operation of a commercially interactive web site accessible in the forum state is sufficient to support specific personal jurisdiction, or whether there must be additional evidence that the defendant has "purposefully availed" itself of the privilege of engaging in activity in that state. Prior decisions indicate that such evidence is necessary, and that it should reflect intentional interaction with the forum state. If a defendant web site operator intentionally targets the site to the forum state, and/or knowingly conducts business with forum state residents via the site, then the "purposeful availment" requirement is satisfied. Below, we first review cases from this and other circuits that articulate this requirement. Next, we consider the role of related non-Internet contacts in demonstrating purposeful availment.

We then assess whether the "purposeful availment" requirement has been satisfied in the present case.

1. The "Purposeful Availment" Requirement in Internet Cases

a. Third Circuit Cases

The opinion in Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) has become a seminal authority regarding personal jurisdiction based upon the operation of an Internet web site. The court in Zippo stressed that the propriety of exercising jurisdiction depends on where on a sliding scale of commercial interactivity the web site falls. In cases where the defendant is clearly doing business through its web site in the forum state, and where the claim relates to or arises out of use of the web site, the Zippo court held that personal jurisdiction exists. Id. at 1124. In reaching this conclusion, the Zippo court relied on CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996), which found the exercise of personal jurisdiction to be proper where the commercial web site's interactivity reflected specifically intended interaction with residents of the forum state. Zippo, 952 F. Supp. at 1124 (citing CompuServe, 89 F.3d at 1264-66).

Analyzing the case before it, the Zippo court similarly underscored the intentional nature of the defendant's conduct vis-a-vis the forum state. In Zippo, the defendant had purposefully availed itself of doing business in Pennsylvania when it "repeatedly and consciously chose to process Pennsylvania residents' applications and to assign
them passwords," knowing that the contacts would result in business relationships with Pennsylvania customers. Id. at 1126. The court summarized the pivotal importance of intentionality as follows:

When a defendant makes a conscious choice to conduct business with the residents of a forum state, 'it has clear notice that it is subject to suit there.' . . . If [the defendant] had not wanted to be amenable to jurisdiction in Pennsylvania, . . . it could have chosen not to sell its services to Pennsylvania residents.

Id. at 1126-27 (citing World-Wide Volkswagen, 444 U.S. at 297).

Since Zippo, several district court decisions from this Circuit have made explicit the requirement that the defendant intentionally interact with the forum state via the web site in order to show purposeful availment and, in turn, justify the exercise of specific personal jurisdiction. See, e.g., S. Morantz, Inc. v. Hang & Shine Ultrasonics, Inc., 79 F. Supp. 2d 537, 540 (E.D. Pa. 1999) (observing that "a web site targeted at a particular jurisdiction is likely to give rise to personal jurisdiction."). As another district court in this Circuit put it, "[c]ourts have repeatedly recognized that there must be 'something more' . . . to demonstrate that the defendant directed its activity towards the forum state." Desktop Technologies, Inc. v. Colorworks Reprod. & Design, 1999 WL 98572, at *5 (E.D. Pa. Feb. 25, 1999) (citation omitted) (emphasis added).

b. Case Law from Other Circuits

Several Courts of Appeals decisions have adopted "purposeful availment" requirements that are consistent with the principles articulated in the Zippo line of cases. The Fourth Circuit, in ALS Scan v. Digital Service Consultants, Inc., 293 F.3d 707 (4th Cir. 2002), expressly incorporated an "intentionality" requirement when fashioning a test for personal jurisdiction in the context of the Internet:

a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State’s courts.

Id. at 714 (emphasis added).

In Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997), the Ninth Circuit considered an infringement action brought against a Florida web site operator whose allegedly infringing site was accessible in Arizona, the state where the plaintiff had its principal place of business. In declining
to exercise specific personal jurisdiction, the Cybersell court found there must be "something more"[beyond the mere posting of a passive web site] to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state." Id. at 418. Decisions from other circuits have articulated similar standards. See, e.g., Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002) (holding that the purposeful availment requirement is satisfied "if the web site is interactive to a degree that reveals specifically intended interaction with residents of the state") (citation omitted) (emphasis added).

2. Non-Internet Contacts

In deciding whether to exercise jurisdiction over a cause of action arising from a defendant's operation of a web site, a court may consider the defendant's related non-Internet activities as part of the "purposeful availment" calculus. One case that relies on non-Internet contacts for the exercise of jurisdiction -- a case Toys repeatedly cites -- is Euromarket Designs, Inc. v. Crate and Barrel Ltd.,, 96 F. Supp. 2d 824 (N.D. Ill. 2000). In Euromarket, the court exercised jurisdiction over an Irish manufacturer based on its commercially interactive web site, even though the products purchased through the web site could not be shipped to Illinois. The court identified a number of non-Internet contacts between the defendant and Illinois, including the fact that the defendant's vendors included Illinois suppliers, its attendance at trade shows in Illinois, and its advertisement in publications that circulate in the United States (albeit originating outside). Id. at 838. The Euromarket court also relied on the fact that the defendant billed Illinois customers, collected revenues from Illinois customers, and recorded sales from goods ordered from Illinois, id., and that the web site was designed to accommodate addresses in the United States. Id. at 836.

Thus far, Toys has not shown that Step Two maintained the type of contacts that supported jurisdiction in Euromarket -- i.e., that the defendant intentionally and knowingly transacted business with residents of the forum state, and had significant other contacts with the forum besides those generated by its web site. This limited record does not provide an occasion for us to spell out the exact mix of Internet and non-Internet contacts required to support an exercise of personal jurisdiction. That determination should be made on a case-by-case basis by assessing the "nature and quality" of the contacts. Zippo, 952 F. Supp. at 1127 (quoting Int'l Shoe, 320 U.S. at 320). However, non-internet contacts such as serial business trips to the forum state, telephone and fax communications directed to the forum state, purchase contracts with forum
state residents, contracts that apply the law of the forum state, and advertisements in local newspapers, may form part of the "something more" needed to establish personal jurisdiction. See Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 726 (E.D. Pa. 1999), and cases there collected. It is noteworthy that the Supreme Court in Burger King Corp., when expounding on the "minimum contacts" requirement, referred generally to a defendant's "activities" in the forum state -- a term that includes the aforementioned non-Internet contacts. Burger King Corp., 471 U.S. at 475.

3. Personal Jurisdiction over Step Two

As Zippo and the Courts of Appeals decisions indicate, the mere operation of a commercially interactive web site should not subject the operator to jurisdiction anywhere in the world. Rather, there must be evidence that the defendant "purposefully availed" itself of conducting activity in the forum state, by directly targeting its web site to the state, knowingly interacting with residents of the forum state via its web site, or through sufficient other related contacts.

Based on the facts established in this case thus far, Toys has failed to satisfy the purposeful availment requirement. Step Two's web sites, while commercial and interactive, do not appear to have been designed or intended to reach customers in New Jersey. Step Two's web sites are entirely in Spanish; prices for its merchandise are in pesetas or Euros, and merchandise can be shipped only to addresses within Spain. Most important, none of the portions of Step Two's web sites are designed to accommodate addresses within the United States. While it is possible to join Club Imaginarium and receive newsletters with only an email address, Step Two asks registrants to indicate their residence using fields that are not designed for addresses in the United States.

Moreover, the record may not now support a finding that

Step Two knowingly conducted business with residents of New Jersey. The only documented sales to persons in the United States are the two contacts orchestrated by Toys, and it appears that Step Two scarcely recognized that sales with U.S. residents had been consummated.

At best, Toys has presented only inconclusive circumstantial evidence to suggest that Step Two targeted its web site to New Jersey residents, or that it purposefully availed itself of any effort to conduct activity in New Jersey. Many of the grounds for jurisdiction that Toys advanced below have been deemed insufficient by the courts. First, the two documented sales appear to be the kind of "fortuitous," "random," and "attenuated" contacts that the Supreme Court has held insufficient to warrant the exercise of jurisdiction. See Burger King Corp., 471 U.S. at 475 (citations omitted). As for the electronic newsletters and
other email correspondence, "telephone communication or mail sent by a defendant [do] not trigger personal jurisdiction if they ‘do not show purposeful availment.’ " Barrett, 44 F. Supp. 2d at 729 (quoting Mellon Bank (East) PSFS, N.A. v. DiVeronica Bros., Inc., 983 F.2d 551, 556 (3d Cir. 1993)). The court in Barrett found that the exchange of three emails between the plaintiff and defendant regarding the contents of the defendant’s web site, without more, did not "amount to the level of purposeful targeting required under the minimum contacts analysis." Id. at 729; see also

5. Toys argues that Step Two was aware that it was conducting business with New Jersey residents. In particular, Toys points to the email correspondence between Mr. Luis M. Lopez and a representative of Step Two regarding Mr. Lopez’s overpayment. Mr. Lopez requested that the difference be mailed to his home address in "South Orange, NJ 07079," but did not spell out "New Jersey" or specify that he resided in the United States. (JA 254, 256.) The Step Two representative, apparently uncertain about the address, sent a reply stating "I have received your address and as far as I can see, it is pretty far from here (we are in Zaragoza). I would appreciate your giving me more information on the address so that I can be sure that it will arrive." (JA 256.) Mr. Lopez’s response to this message -- if he sent one -- is not included in the record. Although Step Two ultimately learned that Mr. Lopez is a United States resident, a trier of fact could reasonably find from the correspondence that the company did not contemplate that sales would occur with U.S.-based purchasers.

Machulsky v. Hall, 210 F. Supp. 2d 531, 542 (D.N.J. 2002) (minimal email correspondence, "by itself or even in conjunction with a single purchase, does not constitute sufficient minimum contacts."). Non-Internet contacts, such as Mr. Tena’s visits to New York and the relationships with U.S. vendors, have not been explored sufficiently to determine whether they are related to Toys’ cause of action, or whether they reflect "purposeful availment."

Absent further evidence showing purposeful availment, Toys cannot establish specific jurisdiction over Step Two.6 However, any information regarding Step Two’s intent vis-a-vis its Internet business and regarding other related contacts is known by Step Two, and can be learned by Toys only through discovery. The District Court’s denial of jurisdictional discovery is thus a critical issue, insofar as it may have prevented Toys from obtaining the information needed to establish personal jurisdiction. We next turn to whether the District Court properly denied Toys’ request for jurisdictional discovery.

B. Jurisdictional Discovery

The pivotal issue on appeal is whether the District Court erred in denying Toys’ request for jurisdictional discovery. A district court’s decision to deny jurisdictional discovery is reviewed for abuse of discretion. See Brumfield v. Sanders,
6. As an alternative to the "minimum contacts" analysis for specific jurisdiction, Toys argues that jurisdiction over Step Two may be based on the "effects" test. Following the lead of the Supreme Court in Calder v. Jones, 465 U.S. 783, 788-89 (1984), the Third Circuit has held that personal jurisdiction may, under certain circumstances, be based on the effects in the forum state of a defendant's tortious actions elsewhere. Remick v. Manfredy, 238 F.3d 248, 258 (3d Cir. 2001). One of the Third Circuit's requirements is that the "defendant expressly aimed his tortious conduct at the forum . . . ." Id. (internal quotations omitted).

Even assuming that Step Two's registration of the Imaginarium domain names and its operation of web sites under that name bring about an injury to Toys in New Jersey (its corporate headquarters), Toys has failed to establish that Step Two engaged in intentionally tortious conduct expressly aimed at New Jersey. In the present case, this intentionality requirement is the key missing component for jurisdiction under either the "minimum contacts" analysis or the "effects" test.

232 F.3d 376, 380 (3d Cir. 2000); Pacitti v. Macy's, 193 F.3d 766, 776 (3d Cir. 1999).

Toys requested jurisdictional discovery for the purpose of establishing either specific personal jurisdiction, or jurisdiction under the federal long-arm statute, Fed. R. Civ. P. 4(k)(2). The District Court denied Toys' request, explaining that "the clear focus of the Court is directed, as it should be, to the web site[,] [a]nd to the activity of the defendants related to that web site, which is making sales here, . . . ." The court added that "the apparent contradictions, if such there will be in the Tena affidavit, [and] what else Mr. Tena might have been doing here, just have no relationship to where the eye is directed and should stay and that is, the web site activities of this defendant." (JA 13-14.)

We are persuaded that the District Court erred when it denied Toys' request for jurisdictional discovery. The court's unwavering focus on the web site precluded consideration of other Internet and non-Internet contacts -- indicated in various parts of the record -- which, if explored, might provide the "something more" needed to bring Step Two within our jurisdiction. Cybersell, Inc., 130 F.3d at 418; Desktop Technologies, Inc., 1999 WL 98572, at *3. Although the plaintiff bears the burden of demonstrating facts that support personal jurisdiction, Pinker, 292 F.3d at 368, courts are to assist the plaintiff by allowing jurisdictional discovery unless the plaintiff's claim is "clearly frivolous." Massachusetts School of Law at Andover, Inc. v. American Bar Ass'n, 107 F.3d 1026, 1042 (3d Cir. 1997). If a plaintiff presents factual allegations that suggest "with reasonable particularity" the possible existence of the requisite "contacts between [the party] and the forum state," Mellon Bank (East) PSFS, Nat'l Ass'n v. Farino, 960 F.2d 1217, 1223 (3d Cir. 1992), the plaintiff's right to conduct jurisdictional discovery should be sustained.
7. The federal long-arm statute sanctions personal jurisdiction over foreign defendants for claims arising under federal law when the defendant has sufficient contacts with the nation as a whole to justify the imposition of U.S. law, but without sufficient contacts to satisfy the due process concerns of the long-arm statute of any particular state.

Where the plaintiff has made this required threshold showing, courts within this Circuit have sustained the right to conduct discovery before the district court dismisses for lack of personal jurisdiction. See, e.g., In re Automotive Refinishing Paint Antitrust Litigation, 2002 WL 31261330, at *9 (E.D. Pa. July 31, 2002) (denying motion to dismiss and permitting jurisdictional discovery where plaintiff made a "threshold prima facie showing of personal jurisdiction over Defendants"); W. Africa Trading & Shipping Co., et al. v. London Int'l Group, et al., 968 F. Supp. 996, 1001 (D.N.J. 1997) (denying defendant's motion to dismiss where the plaintiff's request for jurisdictional discovery is critical to the determination of whether [the court can] exercise personal jurisdiction over the defendant.""); Centralized Health Systems, Inc. v. Cambridge Medical Instruments, Inc., 1989 WL 136277, at *1 (E.D. Pa. Nov. 8, 1989) (holding motion to dismiss in abeyance to permit party to take discovery on jurisdiction where distribution arrangement might satisfy minimum contacts). Here, instead of adopting a deferential approach to Toys' request for discovery, the District Court appears to have focused entirely on the website, thereby preventing further inquiry into non-Internet contacts.

The record before the District Court contained sufficient non-frivolous allegations (and admissions) to support the request for jurisdictional discovery. First, Toys' complaint alleges that Step Two has "completely copied the IMAGINARIUM concept" from Toys. Compl. at P 24. For example, Toys alleges that "the mix of toys sold by Step Two is identical to the mix of toys sold by Toys under the IMAGINARIUM mark," and that "Step Two continues to copy Toys' marketing developments and Intellectual property." Id. at PP 24, 25. Underlying Toys' complaint is its concern that Step Two is "attempt[ing] to expand [its] business throughout the world including the United States by operating international web sites that offer goods similar to the goods offered in Toy's [sic] IMAGINARIUM stores." Id. at P 29. Step Two's intent, according to Toys, is to "capitalize for [its] own pecuniary gain on the goodwill and excellent reputation of Toys . . . ." Id. at P 50.

It is well established that in deciding a motion to dismiss for lack of jurisdiction, a court is required to accept the plaintiff's allegations as true, and is to construe disputed facts in favor of the plaintiff. Pinker, 292 F.3d at 368. Given
the allegations as to Step Two’s mimicry of Toys’ ventures on the Internet and its copy-cat marketing efforts, it would be reasonable to allow more detailed discovery into Step Two’s business plans for purchases, sales, and marketing. Limited discovery relating to these matters would shed light on the extent, if any, Step Two’s business activity— including, but not limited to, its web site — were aimed towards the United States. This information, known only to Step Two, would speak to an essential element of the personal jurisdiction calculus.

Other aspects of the record should have also alerted the District Court to the possible existence of the "something else" needed to exercise personal jurisdiction. For example, Step Two concedes that a portion of the merchandise sold through its Imaginarium stores and web sites are purchased from U.S. vendors, and that Mr. Tena attends the New York Toy Fair each year. Further discovery into the vendor relationships and Mr. Tena’s activities here, if any, may shed light on Step Two’s intentions with respect to the U.S. market, or the extent of its business contacts in the United States. Discovery might also reveal whether these non-Internet contacts directly facilitate Step Two’s alleged exploitation of Toys’ marketing techniques by providing it with a supply of items identical to Toys’ inventory to sell on its web sites.

The two documented sales to residents of New Jersey— and the subsequent emails sent from Step Two to the two purchasers — also speak “with reasonable particularity” to the possible existence of contacts needed to support jurisdiction. Mellon Bank (East) PSFS, 960 F.2d at 1223. Although affiliates of Toys orchestrated the two sales, Mr. Tena’s conflicting affidavits raise the possibility that additional sales to U.S. residents may have been conducted via the web sites. The need for additional discovery regarding sales is further underscored by the parties’ uncertainty as to whether the residence of purchasers can be determined from their credit card number or through some other electronic means.

Counsel for Toys mentioned some of these contacts when it explained to the District Court why it should be allowed jurisdictional discovery:

Mr. Tena states in his affidavit that he has substantial regular and systematic contacts with the United States, [and] he attends trade shows. He purchases from vendors in the United States. I think at the very least, Your Honor, we should be able to inquire into what these substantial and continuing contacts are. Because apparently he buys a lot of the toys that he resells from U.S. vendors, because the ones that we have got were in English that we would be permitted to take discovery on that aspect. To determine whether or not . . . he has made more sales within the State of New
Jersey and in the United States as a whole, as far as accepting orders from United States residents. And/or whether there's a basis for general jurisdiction under Rule 4(k)(2), because of his regular and systematic contacts with the United States. Apparently a lot of his toys are obtained through United States vendors.

(JA 389.)

Toys' request for jurisdictional discovery was specific, non-frivolous, and a logical follow-up based on the information known to Toys. The District Court erred by denying this reasonable request. Toys should be allowed jurisdictional discovery, on the limited issue of Step Two's business activities in the United States, including business plans, marketing strategies, sales, and other commercial interactions. Although Step Two does not appear to have widespread contacts with the United States, this limited discovery will also help determine whether jurisdiction exists under the federal long-arm statute. Accordingly, on remand, the District Court should consider whether any newly discovered facts will support jurisdiction under traditional jurisdictional analysis, or under Rule 4(k)(2).

CONCLUSION

For all of the reasons set forth above, we reverse the District Court's denial of Toys' request for jurisdictional discovery, vacate the District Court's dismissal of Toys' complaint, and remand the case for limited jurisdictional discovery guided by the foregoing analysis, and for reconsideration of jurisdiction with the benefit of the product of that discovery.

A True Copy:
Teste:

Clerk of the United States Court of Appeals for the Third Circuit
United States Court of Appeals
For the Second Circuit

August Term, 2001

Argued: March 14, 2002

Docket Nos. 01-7860(L), 01-7870(CON), 01-7872(CON)

Decided: October 1, 2002

Christopher Specht, John Gibson, Michael Fagan, Sean Kelly, Mark Gruber, and Sherry Weindorf, individually and on behalf of all others similarly situated,

Plaintiffs–Appellees,

v.

Netscape Communications Corporation and America Online, Inc.,

Defendants–Appellants.


Plaintiffs in this action brought suit, individually and on behalf of all others similarly situated, against a provider of computer software programs and its corporate parent, alleging that a “plug-in” software program, created by defendants to facilitate Internet use and made available on defendants’ website for free downloading, invaded plaintiffs’ privacy by clandestinely transmitting personal information to the software provider when plaintiffs employed the plug-in program to browse the Internet. Defendants moved to compel arbitration and to stay court proceedings, arguing that plaintiffs’ claims were subject to an arbitration provision contained in license terms that plaintiffs allegedly had accepted when they downloaded the plug-in program. The United States District Court for the Southern District of New York (Alvin K. Hellerstein, J.) denied the motion. We affirm, holding that (1) plaintiffs neither
received reasonable notice of the existence of the license terms nor manifested unambiguous
assent to those terms before acting on the webpage's invitation to download the plug-in program;
(2) plaintiffs' claims relating to the plug-in program are not subject to a separate arbitration
agreement contained in license terms governing use of defendants' Internet browser software;
and (3) the legal doctrine that requires nonsignatories to an arbitration agreement to arbitrate
when they have received a direct benefit under a contract containing the arbitration agreement
does not apply to a website owner who allegedly benefited when users employing the plug-in
program downloaded files from the website.

Affirmed.

Hostetler, Wilmer Cutler & Pickering, Washington, DC, on the brief; David C. Goldberg, America Online, Inc., Dulles,
VA, of counsel), for Defendants-Appellants.

JOSHUA N. RUBIN, Abbey Gardy, LLP, New York, NY (Jill S.
Abrams, Courtney E. Lynch, Richard B. Margolies, Abbey
Gardy, LLP, New York, NY, on the brief; James V.
Bashian, Law Offices of James V. Bashian, New York, NY;
George G. Mahfood, Leesfield, Leighton, Rubio &
Mahfood, Miami, FL, of counsel), for Plaintiffs-Appellees.

SOTOMAYOR, Circuit Judge:

This is an appeal from a judgment of the Southern District of New York denying a
motion by defendants-appellants Netscape Communications Corporation and its corporate parent,
America Online, Inc. (collectively, "defendants" or "Netscape"), to compel arbitration and to stay
court proceedings. In order to resolve the central question of arbitrability presented here, we
must address issues of contract formation in cyberspace. Principally, we are asked to determine
whether plaintiffs-appellees ("plaintiffs"), by acting upon defendants’ invitation to download free software made available on defendants’ webpage, agreed to be bound by the software’s license terms (which included the arbitration clause at issue), even though plaintiffs could not have learned of the existence of those terms unless, prior to executing the download, they had scrolled down the webpage to a screen located below the download button. We agree with the district court that a reasonably prudent Internet user in circumstances such as these would not have known or learned of the existence of the license terms before responding to defendants’ invitation to download the free software, and that defendants therefore did not provide reasonable notice of the license terms. In consequence, plaintiffs’ bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms.

We also agree with the district court that plaintiffs’ claims relating to the software at issue—a "plug-in" program entitled SmartDownload ("SmartDownload" or "the plug-in program"), offered by Netscape to enhance the functioning of the separate browser program called Netscape Communicator ("Communicator" or "the browser program")—are not subject to an arbitration agreement contained in the license terms governing the use of Communicator. Finally, we conclude that the district court properly rejected defendants’ argument that plaintiff website owner Christopher Specht, though not a party to any Netscape license agreement, is nevertheless required to arbitrate his claims concerning SmartDownload because he allegedly benefited directly under SmartDownload’s license agreement. Defendants’ theory that Specht benefited whenever visitors employing SmartDownload downloaded certain files made available on his website is simply too tenuous and speculative to justify application of the legal doctrine that requires a nonparty to an arbitration agreement to arbitrate if he or she has received a direct
benefit under a contract containing the arbitration agreement.

We therefore affirm the district court’s denial of defendants’ motion to compel arbitration and to stay court proceedings.

BACKGROUND

I. Facts

In three related putative class actions, plaintiffs alleged that, unknown to them, their use of SmartDownload transmitted to defendants private information about plaintiffs’ downloading of files from the Internet, thereby effecting an electronic surveillance of their online activities in violation of two federal statutes, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et seq., and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Specifically, plaintiffs alleged that when they first used Netscape’s Communicator—a software program that permits Internet browsing—the program created and stored on each of their computer hard drives a small text file known as a “cookie” that functioned “as a kind of electronic identification tag for future communications” between their computers and Netscape. Plaintiffs further alleged that when they installed SmartDownload—a separate software “plug-in” that served to enhance Communicator’s browsing

---

1 Although the district court did not consolidate these three cases, it noted that its opinion denying the motion to compel arbitration and to stay court proceedings “appl[ied] equally to all three cases.” Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585, 587 n.1 (S.D.N.Y. 2001). On August 10, 2001, this Court consolidated the appeals.

2 Netscape’s website defines “plug-ins” as “software programs that extend the capabilities of the Netscape Browser in a specific way—giving you, for example, the ability to play audio samples or view video movies from within your browser.” (http://wp.netscape.com/plugins/) SmartDownload purportedly made it easier for users of browser programs like Communicator to download files from the Internet without losing their progress when they paused to engage in some other task, or if their Internet connection was severed. See Specht, 150 F. Supp. 2d at 587.
capabilities—SmartDownload created and stored on their computer hard drives another string of characters, known as a “Key,” which similarly functioned as an identification tag in future communications with Netscape. According to the complaints in this case, each time a computer user employed Communicator to download a file from the Internet, SmartDownload “assume[d] from Communicator the task of downloading” the file and transmitted to Netscape the address of the file being downloaded together with the cookie created by Communicator and the Key created by SmartDownload. These processes, plaintiffs claim, constituted unlawful “eavesdropping” on users of Netscape’s software products as well as on Internet websites from which users employing SmartDownload downloaded files.

In the time period relevant to this litigation, Netscape offered on its website various software programs, including Communicator and SmartDownload, which visitors to the site were invited to obtain free of charge. It is undisputed that five of the six named plaintiffs—Michael Fagan, John Gibson, Mark Gruber, Sean Kelly, and Sherry Weindorf—downloaded Communicator from the Netscape website. These plaintiffs acknowledge that when they proceeded to initiate installation\(^3\) of Communicator, they were automatically shown a scrollable text of that program’s license agreement and were not permitted to complete the installation until they had clicked on a “Yes” button to indicate that they accepted all the license terms.\(^4\) If a user

\(^3\) There is a difference between downloading and installing a software program. When a user downloads a program from the Internet to his or her computer, the program file is stored on the user’s hard drive but typically is not operable until the user installs or executes it, usually by double-clicking on the file and causing the program to run.

\(^4\) This kind of online software license agreement has come to be known as “clickwrap” (by analogy to “shrinkwrap,” used in the licensing of tangible forms of software sold in packages) because it “presents the user with a message on his or her computer screen, requiring that the user manifest his or her assent to the terms of the license agreement by clicking on an
attempted to install Communicator without clicking “Yes,” the installation would be aborted. All
five named user plaintiffs\(^5\) expressly agreed to Communicator’s license terms by clicking “Yes.”
The Communicator license agreement that these plaintiffs saw made no mention of
SmartDownload or other plug-in programs, and stated that “[t]hese terms apply to Netscape
Communicator and Netscape Navigator\(^6\) and that “all disputes relating to this Agreement
(allowing any dispute relating to intellectual property rights)” are subject to “binding arbitration
in Santa Clara County, California.”

Although Communicator could be obtained independently of SmartDownload, all
the named user plaintiffs, except Fagan, downloaded and installed Communicator in connection

icon. The product cannot be obtained or used unless and until the icon is clicked.” *Specht*, 150
F. Supp. 2d at 593-94 (footnote omitted). Just as breaking the shrinkwrap seal and using the
enclosed computer program after encountering notice of the existence of governing license terms
has been deemed by some courts to constitute assent to those terms in the context of tangible
software, see, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1451 (7th Cir. 1996), so clicking on
a webpage’s shrinkwrap button after receiving notice of the existence of license terms has been
held by some courts to manifest an Internet user’s assent to terms governing the use of
downloadable intangible software, see, e.g., *Hotmail Corp. v. Van$ Money Pie Inc.*, 47

\(^5\) The term “user plaintiffs” here and elsewhere in this opinion denotes those plaintiffs
who are suing for harm they allegedly incurred as computer users, in contrast to plaintiff Specht,
who alleges that he was harmed in his capacity as a website owner.

\(^6\) While Navigator was Netscape’s “stand-alone” Internet browser program during the
period in question, Communicator was a “software suite” that comprised Navigator and other
software products. All five named user plaintiffs stated in affidavits that they had obtained
upgraded versions of Communicator. Fagan, who, as noted below, allegedly did not obtain the
browser program in connection with downloading SmartDownload, expressed some uncertainty
during his deposition as to whether he had acquired Communicator or Navigator. The identity of
Fagan’s browser program is immaterial to this appeal, however, as Communicator and Navigator
shared the same license agreement.
with downloading SmartDownload. Each of these plaintiffs allegedly arrived at a Netscape webpage captioned “SmartDownload Communicator” that urged them to “Download With Confidence Using SmartDownload!” At or near the bottom of the screen facing plaintiffs was the prompt “Start Download” and a tinted button labeled “Download.” By clicking on the button, plaintiffs initiated the download of SmartDownload. Once that process was complete, SmartDownload, as its first plug-in task, permitted plaintiffs to proceed with downloading and installing Communicator, an operation that was accompanied by the clickwrap display of Communicator’s license terms described above.

The signal difference between downloading Communicator and downloading SmartDownload was that no clickwrap presentation accompanied the latter operation. Instead, once plaintiffs Gibson, Gruber, Kelly, and Weindorf had clicked on the “Download” button located at or near the bottom of their screen, and the downloading of SmartDownload was complete, these plaintiffs encountered no further information about the plug-in program or the existence of license terms governing its use. The sole reference to SmartDownload’s license

7 Unlike the four other user plaintiffs, Fagan chose the option of obtaining Netscape’s browser program without first downloading SmartDownload. As discussed below, Fagan allegedly obtained SmartDownload from a separate “shareware” website unrelated to Netscape.

8 For purposes of this opinion, the term “webpage” or “page” is used to designate a document that resides, usually with other webpages, on a single Internet website and that contains information that is viewed on a computer monitor by scrolling through the document. To view a webpage in its entirety, a user typically must scroll through multiple screens.

9 Plaintiff Kelly, a relatively sophisticated Internet user, testified that when he clicked to download SmartDownload, he did not think that he was downloading a software program at all, but rather that SmartDownload “was merely a piece of download technology.” He later became aware that SmartDownload was residing as software on his hard drive when he attempted to download electronic files from the Internet.
terms on the “SmartDownload Communicator” webpage was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen.

Had plaintiffs scrolled down instead of acting on defendants’ invitation to click on the “Download” button, they would have encountered the following invitation: “Please review and agree to the terms of the Netscape SmartDownload software license agreement before downloading and using the software.” Plaintiffs Gibson, Gruber, Kelly, and Weindorf averred in their affidavits that they never saw this reference to the SmartDownload license agreement when they clicked on the “Download” button. They also testified during depositions that they saw no reference to license terms when they clicked to download SmartDownload, although under questioning by defendants’ counsel, some plaintiffs added that they could not “remember” or be “sure” whether the screen shots of the SmartDownload page attached to their affidavits reflected precisely what they had seen on their computer screens when they downloaded SmartDownload.10

In sum, plaintiffs Gibson, Gruber, Kelly, and Weindorf allege that the process of obtaining SmartDownload contrasted sharply with that of obtaining Communicator. Having selected SmartDownload, they were required neither to express unambiguous assent to that program’s license agreement nor even to view the license terms or become aware of their existence before proceeding with the invited download of the free plug-in program. Moreover, once these plaintiffs had initiated the download, the existence of SmartDownload’s license terms

10 In the screen shot of the SmartDownload webpage attached to Weindorf’s affidavit, the reference to license terms is partially visible, though almost illegible, at the bottom of the screen. In the screen shots attached to the affidavits of Gibson, Gruber, and Kelly, the reference to license terms is not visible.
was not mentioned while the software was running or at any later point in plaintiffs’ experience of the product.

Even for a user who, unlike plaintiffs, did happen to scroll down past the download button, SmartDownload’s license terms would not have been immediately displayed in the manner of Communicator’s clickwrapped terms. Instead, if such a user had seen the notice of SmartDownload’s terms and then clicked on the underlined invitation to review and agree to the terms, a hypertext link would have taken the user to a separate webpage entitled “License & Support Agreements.” The first paragraph on this page read, in pertinent part:

The use of each Netscape software product is governed by a license agreement. You must read and agree to the license agreement terms BEFORE acquiring a product. Please click on the appropriate link below to review the current license agreement for the product of interest to you before acquisition. For products available for download, you must read and agree to the license agreement terms BEFORE you install the software. If you do not agree to the license terms, do not download, install or use the software.

Below this paragraph appeared a list of license agreements, the first of which was “License Agreement for Netscape Navigator and Netscape Communicator Product Family (Netscape Navigator, Netscape Communicator and Netscape SmartDownload).” If the user clicked on that link, he or she would be taken to yet another webpage that contained the full text of a license agreement that was identical in every respect to the Communicator license agreement except that it stated that its “terms apply to Netscape Communicator, Netscape Navigator, and Netscape SmartDownload.” The license agreement granted the user a nonexclusive license to use and reproduce the software, subject to certain terms:

BY CLICKING THE ACCEPTANCE BUTTON OR
INSTALLING OR USING NETSCAPE COMMUNICATOR, NETSCAPE NAVIGATOR, OR NETSCAPE SMARTDOWNLOAD SOFTWARE (THE "PRODUCT"), THE INDIVIDUAL OR ENTITY LICENSING THE PRODUCT ("LICENSEE") IS CONSENTING TO BE BOUND BY AND IS BECOMING A PARTY TO THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THE BUTTON INDICATING NON-ACCEPTANCE MUST BE SELECTED, AND LICENSEE MUST NOT INSTALL OR USE THE SOFTWARE.

Among the license terms was a provision requiring virtually all disputes relating to the agreement to be submitted to arbitration:

Unless otherwise agreed in writing, all disputes relating to this Agreement (excepting any dispute relating to intellectual property rights) shall be subject to final and binding arbitration in Santa Clara County, California, under the auspices of JAMS/EndDispute, with the losing party paying all costs of arbitration.

Unlike the four named user plaintiffs who downloaded SmartDownload from the Netscape website, the fifth named plaintiff, Michael Fagan, claims to have downloaded the plug-in program from a "shareware" website operated by ZDNet, an entity unrelated to Netscape. Shareware sites are websites, maintained by companies or individuals, that contain libraries of free, publicly available software. The pages that a user would have seen while downloading SmartDownload from ZDNet differed from those that he or she would have encountered while downloading SmartDownload from the Netscape website. Notably, instead of any kind of notice of the SmartDownload license agreement, the ZDNet pages offered only a hypertext link to "more information" about SmartDownload, which, if clicked on, took the user to a Netscape webpage that, in turn, contained a link to the license agreement. Thus, a visitor to the ZDNet website could have obtained SmartDownload, as Fagan avers he did, without ever seeing a
reference to that program’s license terms, even if he or she had scrolled through all of ZDNet’s webpages.

The sixth named plaintiff, Christopher Specht, never obtained or used SmartDownload, but instead operated a website from which visitors could download certain electronic files that permitted them to create an account with an internet service provider called WhyWeb. Specht alleges that every time a user who had previously installed SmartDownload visited his website and downloaded WhyWeb-related files, defendants intercepted this information. Defendants allege that Specht would receive a representative’s commission from WhyWeb every time a user who obtained a WhyWeb file from his website subsequently subscribed to the WhyWeb service. Thus, argue defendants, because the “Netscape license agreement... conferred on each user the right to download and use both Communicator and SmartDownload software,” Specht received a benefit under that license agreement in that SmartDownload “assisted in obtaining the WhyWeb file and increased the likelihood of success in the download process.” This benefit, defendants claim, was direct enough to require Specht to arbitrate his claims pursuant to Netscape’s license terms. Specht, however, maintains that he never received any commissions based on the WhyWeb files available on his website.

II. Proceedings Below

In the district court, defendants moved to compel arbitration and to stay court proceedings pursuant to the Federal Arbitration Act (“FAA”), 9 U.S.C. § 4, arguing that the disputes reflected in the complaints, like any other dispute relating to the SmartDownload license agreement, are subject to the arbitration clause contained in that agreement. Finding that Netscape’s webpage, unlike typical examples of clickwrap, neither adequately alerted users to the
existence of SmartDownload’s license terms nor required users unambiguously to manifest
assent to those terms as a condition of downloading the product, the court held that the user
plaintiffs had not entered into the SmartDownload license agreement. Specht, 150 F. Supp. 2d at
595-96.

The district court also ruled that the separate license agreement governing use of
Communicator, even though the user plaintiffs had assented to its terms, involved an independent
transaction that made no mention of SmartDownload and so did not bind plaintiffs to arbitrate
their claims relating to SmartDownload. Id. at 596. The court further concluded that Fagan
could not be bound by the SmartDownload license agreement, because the shareware site from
which he allegedly obtained the plug-in program provided even less notice of SmartDownload’s
license terms than did Netscape’s page. Id. at 596-97. Finally, the court ruled that Specht was
not bound by the SmartDownload arbitration agreement as a noncontracting beneficiary, because
he (1) had no preexisting relationship with any of the parties, (2) was not an agent of any party,
and (3) received no direct benefit from users’ downloading of files from his site, even if those
users did employ SmartDownload to enhance their downloading. Id. at 597-98.

Defendants took this timely appeal pursuant to 9 U.S.C. § 16, and the district
court stayed all proceedings in the underlying cases pending resolution of the appeal. This Court
has jurisdiction pursuant to § 16(a)(1)(B), as this is an appeal from an order denying defendants’
motion to compel arbitration under the FAA. Mediterranean Shipping Co. S.A. Geneva v.
POL-Atlantic, 229 F.3d 397, 402 (2d Cir. 2000).
Whether This Court Should Remand for a Trial on Contract Formation

Defendants argue on appeal that the district court erred in deciding the question of contract formation as a matter of law. A central issue in dispute, according to defendants, is whether the user plaintiffs actually saw the notice of SmartDownload’s license terms when they downloaded the plug-in program. Although plaintiffs in their affidavits and depositions generally swore that they never saw the notice of terms on Netscape’s webpage, defendants point to deposition testimony in which some plaintiffs, under repeated questioning by defendants’ counsel, responded that they could not “remember” or be entirely “sure” whether the link to SmartDownload’s license terms was visible on their computer screens. Defendants argue that on some computers, depending on the configuration of the monitor and browser, SmartDownload’s license link “appears on the first screen, without any need for the user to scroll at all.” Thus, according to defendants, “a trial on the factual issues that Defendants raised about each and every Plaintiffs’ [sic] downloading experience” is required on remand to remedy the district court’s “error” in denying defendants’ motion as a matter of law.

Section 4 of the FAA provides, in relevant part, that “[i]f the making of the arbitration agreement . . . be in issue, the court shall proceed summarily to the trial thereof.” 9 U.S.C. § 4. We conclude for two reasons, however, that defendants are not entitled to a remand
for a full trial. First, during oral argument in the district court on the arbitrability of the five user plaintiffs’ claims, defendants’ counsel repeatedly insisted that the district court could decide “as a matter of law based on the uncontroverted facts in this case” whether “a reasonably prudent person could or should have known of the [license] terms by which acceptance would be signified.” “I don’t want you to try the facts,” defendants’ counsel told the court. “I think that the evidence in this case upon which this court can make a determination [of whether a contract existed] as a matter of law is uncontroverted.” Accordingly, the district court decided the issue of reasonable notice and objective manifestation of assent as a matter of law. “[I]t is a well-established general rule that an appellate court will not consider an issue raised for the first time on appeal.” Greene v. United States, 13 F.3d 577, 586 (2d Cir. 1994); see also Gurary v. Winehouse, 190 F.3d 37, 44 (2d Cir. 1999) (“Having failed to make the present argument to the district court, plaintiff will not be heard to advance it here.”). Nor would it cause injustice in this case for us to decline to accept defendants’ invitation to consider an issue that defendants did not advance below.

12 Later, when Judge Hellerstein suggested that it was “an issue of fact . . . to be tried” whether plaintiff Fagan downloaded SmartDownload from Netscape’s webpage or from the ZDNet shareware site, defendants’ counsel stated: “I am not sure there is an issue of fact. It is sort of a summary judgment kind of standard.” Still later, counsel remarked: “I think we established that there really is no genuine issue that Mr. Fagan got his smart download [sic] by visiting the Netscape webpage from which he] fairly had notice that there was a license agreement.” Defendants’ position that there was “no genuine issue” regarding reasonable notice of the existence of the license terms is consistent with this Circuit’s standard for determining whether a trial is required on the issue of the making of an arbitration agreement. See Doctor’s Assocs., Inc. v. Distajo, 107 F.3d 126, 129-30 (2d Cir. 1997) (“As when opposing a motion for summary judgment under Fed. R. Civ. P. 56, the party requesting a jury trial must submit evidentiary facts showing that there is a dispute of fact to be tried.” (quotation marks omitted)); Doctor’s Assocs., Inc. v. Stuart, 85 F.3d 975, 983-84 (2d Cir. 1996) (“To warrant a trial under 9 U.S.C. § 4, the issue raised must be ‘genuine.’” (quotation marks omitted)).
Second, after conducting weeks of discovery on defendants’ motion to compel arbitration, the parties placed before the district court an ample record consisting of affidavits and extensive deposition testimony by each named plaintiff; numerous declarations by counsel and witnesses for the parties; dozens of exhibits, including computer screen shots and other visual evidence concerning the user plaintiffs’ experience of the Netscape webpage; oral argument supplemented by a computer demonstration; and additional briefs following oral argument. This well-developed record contrasts sharply with the meager records that on occasion have caused this Court to remand for trial on the issue of contract formation pursuant to 9 U.S.C. § 4. See, e.g., Interbras Cayman Co. v. Orient Victory Shipping Co., S.A., 663 F.2d 4, 5 (2d Cir. 1981) (record consisted of affidavits and other papers); Interocean Shipping, 462 F.2d at 676 (record consisted of pleadings, affidavits, and documentary attachments). We are satisfied that the unusually full record before the district court in this case constituted “a hearing where evidence is received.” Interocean Shipping, 462 F.2d at 677. Moreover, upon the record assembled, a fact-finder could not reasonably find that defendants prevailed in showing that any of the user plaintiffs had entered into an agreement on defendants’ license terms.

In sum, we conclude that the district court properly decided the question of reasonable notice and objective manifestation of assent as a matter of law on the record before it, and we decline defendants’ request to remand for a full trial on that question.

III. Whether the User Plaintiffs Had Reasonable Notice of and Manifested Assent to the SmartDownload License Agreement

Whether governed by the common law or by Article 2 of the Uniform Commercial Code (“UCC”), a transaction, in order to be a contract, requires a manifestation of
agreement between the parties. See Windsor Mills, Inc. v. Collins & Aikman Corp., 101 Cal. Rptr. 347, 350 (Cal. Ct. App. 1972) (“[C]onsent to, or acceptance of, the arbitration provision [is] necessary to create an agreement to arbitrate.”); see also Cal. Com. Code § 2204(1) (“A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract.”).\textsuperscript{13} Mutual

\textsuperscript{13} The district court concluded that the SmartDownload transactions here should be governed by “California law as it relates to the sale of goods, including the Uniform Commercial Code in effect in California.” Specht, 150 F. Supp. 2d at 591. It is not obvious, however, that UCC Article 2 (“sales of goods”) applies to the licensing of software that is downloadable from the Internet. Cf. Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 675 (3d Cir. 1991) (“The increasing frequency of computer products as subjects of commercial litigation has led to controversy over whether software is a ‘good’ or intellectual property. The [UCC] does not specifically mention software.”); Lorin Brennan, \textit{Why Article 2 Cannot Apply to Software Transactions}, PLI Patents, Copyrights, Trademarks, & Literary Property Course Handbook Series (Feb.-Mar. 2001) (demonstrating the trend in case law away from application of UCC provisions to software sales and licensing and toward application of intellectual property principles). There is no doubt that a sale of tangible goods over the Internet is governed by Article 2 of the UCC. See, e.g., Butler v. Beer Across Am., 83 F. Supp. 2d 1261, 1263-64 & n.6 (N.D. Ala. 2000) (applying Article 2 to an Internet sale of bottles of beer). Some courts have also applied Article 2, occasionally with misgivings, to sales of off-the-shelf software in tangible, packaged formats. See, e.g., ProCD, 86 F.3d at 1450 (“[W]e treat the [database] licenses as ordinary contracts accompanying the sale of products, and therefore as governed by the common law of contracts and the Uniform Commercial Code. Whether there are legal differences between ‘contracts’ and ‘licenses’ (which may matter under the copyright doctrine of first sale) is a subject for another day.”); i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 332 (D. Mass. 2002) (stating, in the context of a dispute between business parties, that “Article 2 technically does not, and certainly will not in the future, govern software licenses, but for the time being, the Court will assume that it does”).

Downloadable software, however, is scarcely a “tangible” good, and, in part because software may be obtained, copied, or transferred effortlessly at the stroke of a computer key, licensing of such Internet products has assumed a vast importance in recent years. Recognizing that “a body of law based on images of the sale of manufactured goods ill fits licenses and other transactions in computer information,” the National Conference of Commissioners on Uniform State Laws has promulgated the Uniform Computer Information Transactions Act (“UCITA”), a code resembling UCC Article 2 in many respects but drafted to reflect emergent practices in the sale and licensing of computer information. UCITA, prefatory note (rev. ed. Aug. 23, 2001) (available at www.ucitaonline.com/ucita.html). UCITA—originally intended as a new Article 2B to supplement Articles 2 and 2A of the UCC but later proposed as an independent code—has
manifestation of assent, whether by written or spoken word or by conduct, is the touchstone of contract. *Binder v. Aetna Life Ins. Co.*, 89 Cal. Rptr. 2d 540, 551 (Cal. Ct. App. 1999); *cf.* Restatement (Second) of Contracts § 19(2) (1981) ("The conduct of a party is not effective as a manifestation of his assent unless he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents."). Although an onlooker observing the disputed transactions in this case would have seen each of the user plaintiffs click on the SmartDownload "Download" button, *see Cedars Sinai Med. Ctr. v. Mid-West Nat'l Life Ins. Co.*, 118 F. Supp. 2d 1002, 1008 (C.D. Cal. 2000) ("In California, a party’s intent to contract is judged objectively, by the party’s outward manifestation of consent.")], a consumer’s clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms, *see Windsor Mills*, 101 Cal. Rptr. at 351 ("[W]hen the offeree does not know that a proposal has been made to him this objective standard does not apply."). California’s common law is clear that "an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious." *Id.; see also Marin Storage & Trucking, Inc. v. Benco Contracting & Eng’g, Inc.*, 107 Cal. Rptr. 2d 645, 651 (Cal. Ct. App. 2001) (same).

Arbitration agreements are no exception to the requirement of manifestation of


We need not decide today whether UCC Article 2 applies to Internet transactions in downloadable products. The district court’s analysis and the parties’ arguments on appeal show that, for present purposes, there is no essential difference between UCC Article 2 and the common law of contracts. We therefore apply the common law, with exceptions as noted.
assent. "This principle of knowing consent applies with particular force to provisions for arbitration." *Windsor Mills*, 101 Cal. Rptr. at 351. Clarity and conspicuousness of arbitration terms are important in securing informed assent. "If a party wishes to bind in writing another to an agreement to arbitrate future disputes, such purpose should be accomplished in a way that each party to the arrangement will fully and clearly comprehend that the agreement to arbitrate exists and binds the parties thereto." *Commercial Factors Corp. v. Kurtzman Bros.*, 280 P.2d 146, 147-48 (Cal. Dist. Ct. App. 1955) (internal quotation marks omitted). Thus, California contract law measures assent by an objective standard that takes into account both what the offeree said, wrote, or did and the transactional context in which the offeree verbalized or acted.

A. The Reasonably Prudent Offeree of Downloadable Software

Defendants argue that plaintiffs must be held to a standard of reasonable prudence and that, because notice of the existence of SmartDownload license terms was on the next scrollable screen, plaintiffs were on "inquiry notice" of those terms.14 We disagree with the proposition that a reasonably prudent offeree in plaintiffs’ position would necessarily have known or learned of the existence of the SmartDownload license agreement prior to acting, so that plaintiffs may be held to have assented to that agreement with constructive notice of its terms. *See* Cal. Civ. Code § 1589 ("A voluntary acceptance of the benefit of a transaction is equivalent to a consent to all the obligations arising from it, so far as the facts are known, or ought to be known, to the person accepting."). It is true that "[a] party cannot avoid the terms of a contract on the ground that he or she failed to read it before signing." *Marin Storage &

---

Trucking, 107 Cal. Rptr. 2d at 651. But courts are quick to add: “An exception to this general rule exists when the writing does not appear to be a contract and the terms are not called to the attention of the recipient. In such a case, no contract is formed with respect to the undisclosed term.” Id.; cf. Cory v. Golden State Bank, 157 Cal. Rptr. 538, 541 (Cal. Ct. App. 1979) (“[T]he provision in question is effectively hidden from the view of money order purchasers until after the transactions are completed. . . . Under these circumstances, it must be concluded that the Bank’s money order purchasers are not chargeable with either actual or constructive notice of the service charge provision, and therefore cannot be deemed to have consented to the provision as part of their transaction with the Bank.”).

Most of the cases cited by defendants in support of their inquiry-notice argument are drawn from the world of paper contracting. See, e.g., Taussig v. Bode & Haslett, 66 P. 259, 265-66 (Cal. 1901) (where party had opportunity to read leakage disclaimer printed on warehouse receipt, he had duty to do so); In re First Capital Life Ins. Co., 40 Cal. Rptr. 2d 816, 820 (Cal. Ct. App. 1995) (purchase of insurance policy after opportunity to read and understand policy terms creates binding agreement); King v. Larsen Realty, Inc., 175 Cal. Rptr. 226, 231 (Cal. Ct. App. 1981) (where realtors’ board manual specifying that party was required to arbitrate was “readily available,” party was “on notice” that he was agreeing to mandatory arbitration); Cal. State Auto. Ass’n Inter-Ins. Bureau v. Barrett Garages, Inc., 64 Cal. Rptr. 699, 703 (Cal. Ct. App. 1967) (recipient of airport parking claim check was bound by terms printed on claim check, because a “ordinarily prudent” person would have been alerted to the terms); Larrus v. First Nat’l Bank, 266 P.2d 143, 147 (Cal. Dist. Ct. App. 1954) (“clearly printed” statement on bank card stating that depositor agreed to bank’s regulations provided sufficient notice to create
agreement, where party had opportunity to view statement and to ask for full text of regulations, but did not do so); see also Hux v. Butler, 339 F.2d 696, 700 (6th Cir. 1964) (constructive notice found where “slightest inquiry” would have disclosed relevant facts to offeree); Walker v. Carnival Cruise Lines, 63 F. Supp. 2d 1083, 1089 (N.D. Cal. 1999) (under California and federal law, “conspicuous notice” directing the attention of parties to existence of contract terms renders terms binding) (quotation marks omitted); Shacket v. Roger Smith Aircraft Sales, Inc., 651 F. Supp. 675, 691 (N.D. Ill. 1986) (constructive notice found where “minimal investigation” would have revealed facts to offeree).

As the foregoing cases suggest, receipt of a physical document containing contract terms or notice thereof is frequently deemed, in the world of paper transactions, a sufficient circumstance to place the offeree on inquiry notice of those terms. “Every person who has actual notice of circumstances sufficient to put a prudent man upon inquiry as to a particular fact, has constructive notice of the fact itself in all cases in which, by prosecuting such inquiry, he might have learned such fact.” Cal. Civ. Code § 19. These principles apply equally to the emergent world of online product delivery, pop-up screens, hyperlinked pages, clickwrap licensing, scrollable documents, and urgent admonitions to “Download Now!” What plaintiffs saw when they were being invited by defendants to download this fast, free plug-in called SmartDownload was a screen containing praise for the product and, at the very bottom of the screen, a “Download” button. Defendants argue that under the principles set forth in the cases cited above, a “fair and prudent person using ordinary care” would have been on inquiry notice of SmartDownload’s license terms. Shacket, 651 F. Supp. at 690.

We are not persuaded that a reasonably prudent offeree in these circumstances
would have known of the existence of license terms. Plaintiffs were responding to an offer that did not carry an immediately visible notice of the existence of license terms or require unambiguous manifestation of assent to those terms. Thus, plaintiffs’ “apparent manifestation of . . . consent” was to terms “contained in a document whose contractual nature [was] not obvious.” *Windsor Mills*, 101 Cal. Rptr. at 351. Moreover, the fact that, given the position of the scroll bar on their computer screens, plaintiffs may have been aware that an unexplored portion of the Netscape webpage remained below the download button does not mean that they reasonably should have concluded that this portion contained a notice of license terms. In their deposition testimony, plaintiffs variously stated that they used the scroll bar “[o]nly if there is something that I feel I need to see that is on—that is off the page,” or that the elevated position of the scroll bar suggested the presence of “mere[] formalities, standard lower banner links” or “that the page is bigger than what I can see.” Plaintiffs testified, and defendants did not refute, that plaintiffs were in fact unaware that defendants intended to attach license terms to the use of SmartDownload.

We conclude that in circumstances such as these, where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms. 15 The SmartDownload webpage screen was “printed in such a manner that it tended to conceal the fact that it was an express acceptance of [Netscape’s] rules and

15 We do not address the district court’s alternative holding that notice was further vitiated by the fact that the reference to SmartDownload’s license terms, even if scrolled to, was couched in precatory terms (“a mild request”) rather than mandatory ones. *Specht*, 150 F. Supp. 2d at 596.
regulations.” Larrus, 266 P.2d at 147. Internet users may have, as defendants put it, “as much time as they need[]” to scroll through multiple screens on a webpage, but there is no reason to assume that viewers will scroll down to subsequent screens simply because screens are there. When products are “free” and users are invited to download them in the absence of reasonably conspicuous notice that they are about to bind themselves to contract terms, the transactional circumstances cannot be fully analogized to those in the paper world of arm’s-length bargaining. In the next two sections, we discuss case law and other legal authorities that have addressed the circumstances of computer sales, software licensing, and online transacting. Those authorities tend strongly to support our conclusion that plaintiffs did not manifest assent to SmartDownload’s license terms.

B. Shrinkwrap Licensing and Related Practices

Defendants cite certain well-known cases involving shrinkwrap licensing and related commercial practices in support of their contention that plaintiffs became bound by the SmartDownload license terms by virtue of inquiry notice. For example, in Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997), the Seventh Circuit held that where a purchaser had ordered a computer over the telephone, received the order in a shipped box containing the computer along with printed contract terms, and did not return the computer within the thirty days required by the terms, the purchaser was bound by the contract. Id. at 1148-49. In ProCD, Inc. v. Zeidenberg, the same court held that where an individual purchased software in a box containing license terms which were displayed on the computer screen every time the user executed the software program, the user had sufficient opportunity to review the terms and to return the software, and so was contractually bound after retaining the product. ProCD, 86 F.3d at 1452;
cf. Moore v. Microsoft Corp., 293 A.D.2d 587, 587, 741 N.Y.S.2d 91, 92 (2d Dep’t 2002) (software user was bound by license agreement where terms were prominently displayed on computer screen before software could be installed and where user was required to indicate assent by clicking “I agree”); Brower v. Gateway 2000, Inc., 246 A.D.2d 246, 251, 676 N.Y.S.2d 569, 572 (1st Dep’t 1998) (buyer assented to arbitration clause shipped inside box with computer and software by retaining items beyond date specified by license terms); M.A. Mortenson Co. v. Timberline Software Corp., 970 P.2d 803, 809 (Wash. Ct. App. 1999) (buyer manifested assent to software license terms by installing and using software), aff’d, 998 P.2d 305 (Wash. 2000); see also i.LAN Sys., 183 F. Supp. 2d at 338 (business entity “explicitly accepted the clickwrap license agreement [contained in purchased software] when it clicked on the box stating ‘I agree’”).

These cases do not help defendants. To the extent that they hold that the purchaser of a computer or tangible software is contractually bound after failing to object to printed license terms provided with the product, Hill and Brower do not differ markedly from the cases involving traditional paper contracting discussed in the previous section. Insofar as the purchaser in ProCD was confronted with conspicuous, mandatory license terms every time he ran the software on his computer, that case actually undermines defendants’ contention that downloading in the absence of conspicuous terms is an act that binds plaintiffs to those terms. In Mortenson, the full text of license terms was printed on each sealed diskette envelope inside the software box, printed again on the inside cover of the user manual, and notice of the terms appeared on the computer screen every time the purchaser executed the program. Mortenson, 970 P.2d at 806. In sum, the foregoing cases are clearly distinguishable from the facts of the
present action.

C. Online Transactions

Cases in which courts have found contracts arising from Internet use do not assist defendants, because in those circumstances there was much clearer notice than in the present case that a user’s act would manifest assent to contract terms. See, e.g., *Hotmail Corp. v. Van* $\text{Money Pie Inc., 47 U.S.P.Q.2d 1020, 1025 (N.D. Cal. 1998) (granting preliminary injunction based in part on breach of “Terms of Service” agreement, to which defendants had assented); America Online, Inc. v. Booker, 781 So. 2d 423, 425 (Fla. Dist. Ct. App. 2001) (upholding forum selection clause in “freely negotiated agreement” contained in online terms of service); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 530, 532-33 (N.J. Super. Ct. App. Div. 1999) (upholding forum selection clause where subscribers to online software were required to review license terms in scrollable window and to click “I Agree” or “I Don’t Agree”); Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 203-04 (Tex. App. 2001) (upholding forum selection clause in online contract for registering Internet domain names that required users to scroll through terms before accepting or rejecting them); cf. Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 981-82 (E.D. Cal. 2000) (expressing concern that notice of license terms had appeared in small, gray text on a gray background on a linked webpage, but concluding that it was too early}

\[\text{16} \] Defendants place great importance on *Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000)*, which held that a user of the Internet domain-name database, Register.com, had “manifested its assent to be bound” by the database’s terms of use when it electronically submitted queries to the database. *Id.* at 248. But *Verio* is not helpful to defendants. There, the plaintiff’s terms of use of its information were well known to the defendant, which took the information daily with full awareness that it was using the information in a manner prohibited by the terms of the plaintiff’s offer. The case is not closely analogous to ours.
in the case to order dismissal). 17

17 Although the parties here do not refer to it, California’s consumer fraud statute, Cal. Bus. & Prof. Code § 17538, is one of the few state statutes to regulate online transactions in goods or services. The statute provides that in disclosing information regarding return and refund policies and other vital consumer information, online vendors must legibly display the information either:

(i) on the first screen displayed when the vendor’s electronic site is accessed, (ii) on the screen on which goods or services are first offered, (iii) on the screen on which a buyer may place the order for goods or services, (iv) on the screen on which the buyer may enter payment information, such as a credit card account number, or (v) for nonbrowser-based technologies, in a manner that gives the user a reasonable opportunity to review that information.

Id. § 17538(d)(2)(A). The statute’s clear purpose is to ensure that consumers engaging in online transactions have relevant information before they can be bound. Although consumer fraud as such is not alleged in the present action, and § 17538 protects only California residents, we note that the statute is consistent with the principle of conspicuous notice of the existence of contract terms that is also found in California’s common law of contracts.

In addition, the model code, UCITA, discussed above, generally recognizes the importance of conspicuous notice and unambiguous manifestation of assent in online sales and licensing of computer information. For example, § 112, which addresses manifestation of assent, provides that a user’s opportunity to review online contract terms exists if a “record” (or electronic writing) of the contract terms is “made available in a manner that ought to call it to the attention of a reasonable person and permit review.” UCITA, § 112(e)(1) (rev. ed. Aug. 23, 2001) (available at www.ucitaonline.com/ucita.html). Section 112 also provides, in pertinent part, that “[a] person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it . . . intentionally engages in conduct or makes statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that the person assents to the record or term.” Id. § 112(a)(2). In the case of a “mass-market license,” a party adopts the terms of the license only by manifesting assent “before or during the party’s initial performance or use of or access to the information.” Id. § 209(a).

UCITA § 211 sets forth a number of guidelines for “internet-type” transactions involving the supply of information or software. For example, a licensor should make standard terms “available for review” prior to delivery or obligation to pay (1) by “displaying prominently and in close proximity to a description of the computer information, or to instructions or steps for acquiring it, the standard terms or a reference to an electronic location from which they can be readily obtained,” or (2) by “disclosing the availability of the standard terms in a prominent place on the site from which the computer information is offered and promptly furnishing a copy of the standard terms on request before the transfer of the computer information.” Id. § 211(1)(A-B). The commentary to § 211 adds: “The intent of the close proximity standard is that the terms or
After reviewing the California common law and other relevant legal authority, we conclude that under the circumstances here, plaintiffs' downloading of SmartDownload did not constitute acceptance of defendants' license terms. Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility. We hold that a reasonably prudent offeree in plaintiffs' position would not have known or learned, prior to acting on the invitation to download, of the reference to SmartDownload's license terms hidden below the "Download" button on the next screen. We affirm the district court's conclusion that the user plaintiffs, including Fagan, are not bound by the arbitration clause contained in those terms.\textsuperscript{18}

\footnote{Because we conclude that the Netscape webpage did not provide reasonable notice of the existence of SmartDownload's license terms, it is irrelevant to our decision whether plaintiff Fagan obtained SmartDownload from that webpage, as defendants contend, or from a shareware}
IV. Whether Plaintiffs’ Assent to Communicator’s License Agreement Requires Them To Arbitrate Their Claims Regarding SmartDownload

Plaintiffs do not dispute that they assented to the license terms governing Netscape’s Communicator. The parties disagree, however, over the scope of that license’s arbitration clause. Defendants contend that the scope is broad enough to encompass plaintiffs’ claims regarding SmartDownload, even if plaintiffs did not separately assent to SmartDownload’s license terms and even though Communicator’s license terms did not expressly mention SmartDownload. Thus, defendants argue, plaintiffs must arbitrate.

The scope of an arbitration agreement is a legal issue that we review de novo. Oldroyd, 134 F.3d at 76. “[A]ny doubts concerning the scope of arbitrable issues should be resolved in favor of arbitration.” Genesco, 815 F.2d at 847 (quotation marks omitted). Although “the FAA does not require parties to arbitrate when they have not agreed to do so,” Volt Info. Sciences, Inc. v. Bd. of Trs. Of Leland Stanford Junior Univ., 489 U.S. 468, 478 (1989), arbitration is indicated unless it can be said “with positive assurance” that an arbitration clause is not susceptible to an interpretation that covers the asserted dispute. Thomas James Assocs., Inc. v. Jameson, 102 F.3d 60, 65 (2d Cir. 1996) (quotation marks omitted).

The Communicator license agreement, which required arbitration of “all disputes

website that provided less or no notice of that program’s license terms, as Fagan maintains. In either case, Fagan could not be bound by the SmartDownload license agreement. Further, because we find that the California common law disposes of the issue of notice and assent, we do not address plaintiffs’ arguments based on California’s Commercial Code § 2207, the UCC Article 2 provision governing the “battle of the forms.” Moreover, having determined that the parties did not enter into the SmartDownload license agreement, we do not reach plaintiffs’ alternative arguments concerning unconscionability.
relating to this Agreement (excepting any dispute relating to intellectual property rights),” must be classified as “broad.” Corregis Ins. Co. v. Am. Health Found., 241 F.3d 123, 128-29 (2d Cir. 2001). Where the scope of an arbitration agreement is broad,

there arises a presumption of arbitrability; if, however, the dispute is in respect of a matter that, on its face, is clearly collateral to the contract, then a court should test the presumption by reviewing the allegations underlying the dispute and by asking whether the claim alleged implicates issues of contract construction or the parties’ rights and obligations under it . . . [C]laims that present no question involving construction of the contract, and no questions in respect of the parties’ rights and obligations under it, are beyond the scope of the arbitration agreement.

Collins & Aikman, 58 F.3d at 23. In determining whether a particular claim falls within the scope of the parties’ arbitration agreement, this Court “focus[es] on the factual allegations in the complaint rather than the legal causes of action asserted.” Genesco, 815 F.2d at 846. If those allegations “touch matters” covered by the Netscape license agreement, plaintiffs’ claims must be arbitrated. Id.

19 A question not raised by the parties is whether this dispute involves “intellectual property rights.” Certainly, Netscape’s intellectual property (“IP”) rights would not seem to be implicated, even though Netscape may in some sense employ its IP—in the form of computer software—to plant cookies and, as plaintiffs allege, harvest users’ personal information. But do plaintiffs have IP rights in their personal information? Certain cases have recognized, mostly under a trespass-to-chattels theory, that computer and database owners enjoy possessory interests in their computer equipment, bandwidth, and server capacity, but these interests are analyzed in terms of traditional personal property, not IP. See, e.g., Verio, 126 F. Supp. 2d at 249-53; eBay, Inc. v. Bidder’s Edge, Inc., 100 F. Supp. 2d 1058, 1069-72 (N.D. Cal. 2000). Moreover, plaintiffs’ personal information, stored in cookies, is the sort of factual data that are expressly excluded from federal copyright protection. See Nihon Keizai Shim bun, Inc. v. Comline Bus. Data, Inc., 166 F.3d 65, 70 (2d Cir. 1999) (“That copyright does not extend to facts is a ‘most fundamental axiom of copyright law.’” (quoting Feist Publ’ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344 (1991)). Thus, copyrights are not implicated here. Nor are trade secrets, goodwill, or other valuable intangibles. In consequence, plaintiffs’ claims would not appear to be shielded from arbitration on the ground that this is a “dispute relating to intellectual property rights.” This is not an issue that we decide today, however.
To begin with, we find that the underlying dispute in this case—whether defendants violated plaintiffs’ rights under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act—involves matters that are clearly collateral to the Communicator license agreement. While the SmartDownload license agreement expressly applied “to Netscape Communicator, Netscape Navigator, and Netscape SmartDownload,” the Communicator license agreement expressly applied only “to Netscape Communicator and Netscape Navigator.” Thus, on its face, the Communicator license agreement governed disputes concerning Netscape’s browser programs only, not disputes concerning a plug-in program like SmartDownload. Moreover, Communicator’s license terms included a merger or integration clause stating that “[t]his Agreement constitutes the entire agreement between the parties concerning the subject matter hereof.” SmartDownload’s license terms contained the same clause. Such provisions are recognized by California courts as a means of excluding prior or contemporaneous parol evidence from the scope of a contract. See Franklin v. USX Corp., 105 Cal. Rptr. 2d 11, 15 (Cal. Ct. App. 2001). Although the presence of merger clauses is not dispositive here, we note that defendants’ express desire to limit the reach of the respective license agreements, combined with the absence of reference to SmartDownload in the Communicator license agreement, suggests that a dispute regarding defendants’ allegedly unlawful use of SmartDownload is clearly collateral to the Communicator license agreement.

This conclusion is reinforced by the other terms of the Communicator license agreement, which include a provision describing the non-exclusive nature of the grant and permission to reproduce the software for personal and internal business purposes; restrictions on modification, decompilation, redistribution or other sale or transfer, and removal or alteration of
trademarks or other intellectual property; provisions for the licensor's right to terminate and its proprietary rights; a complete disclaimer of warranties ("as is") and an entire-risk clause; a limitation of liability clause for consequential and other damages, together with a liquidated damages term; clauses regarding encryption and export; a disklamer of warranties for high risk activities; and a miscellaneous paragraph that contains merger, choice-of-law, arbitration, and severability clauses, non-waiver and non-assignment provisions, a force majeure term, and a clause providing for reimbursement of the prevailing party in any dispute. Apart from the potential generic applicability of the warranty and liability disclaimers, a dispute concerning alleged electronic eavesdropping via transmissions from a separate plug-in program would not appear to fall within Communicator's license terms. We conclude, therefore, that this dispute concerns matters that, on their face, are clearly collateral to the Communicator license agreement.

Having determined this much, we next must test the presumption of arbitrability by asking whether plaintiffs' allegations implicate or touch on issues of contract construction or the parties' rights and obligations under the contract. Collins & Aikman, 58 F.3d at 23; Genesco, 815 F.2d at 846. That is, even though the parties' dispute concerns matters clearly collateral to the Communicator license terms, we must determine whether plaintiffs by their particular allegations have brought the dispute within the license terms. Defendants argue that plaintiffs' complaints "literally bristled with allegations that Communicator and SmartDownload operated in conjunction with one another to eavesdrop on Plaintiffs' Internet communications." We disagree. Plaintiffs' allegations nowhere collapse or blur the distinction between Communicator and SmartDownload, but instead consistently separate the two software programs and assert that SmartDownload alone is responsible for unlawful eavesdropping. Plaintiffs begin by alleging

32
that “SmartDownload facilitates the transfer of large files over the Internet by permitting a transfer to be resumed if it is interrupted.” Plaintiffs then explain that “[o]nce SmartDownload is downloaded and running on a Web user’s computer, it automatically connects to Netscape’s file servers and downloads the installation program for Communicator.” Plaintiffs add that defendants also encourage visitors to Netscape’s website “to download and install SmartDownload even if they are not installing or upgrading Communicator.”

Plaintiffs go on to point out that installing Communicator “automatically creates and stores on the Web user’s computer a small text file known as a ‘cookie.’” There follow two paragraphs essentially alleging that cookies were originally intended to perform such innocuous tasks as providing “temporary identification for purposes such as electronic commerce,” and that the Netscape cookie performs this original identifying, and entirely lawful, function. Separate paragraphs then describe the “Key” or “UserID” that SmartDownload allegedly independently places on user’s computers, and point out that “SmartDownload assumes from Communicator the task of downloading various files. Communicator itself could and would perform these downloading tasks if SmartDownload were not installed.” “Thereafter,” the complaints continue, each time a Web user downloads any file from any site on the Internet using SmartDownload, SmartDownload automatically transmits to defendants the name and Internet address of the file and the Web site from which it is being sent. Within the same transmission, SmartDownload also includes the contents of the Netscape cookie previously created by Communicator and the “Key” previously created by SmartDownload.

In the course of their description of the installation and downloading process, plaintiffs keep SmartDownload separate from Communicator and clearly indicate that it is SmartDownload that performed the allegedly unlawful eavesdropping and made use of the
otherwise innocuous Communicator cookie as well as its own “Key” and “UserID” to transmit plaintiffs’ information to Netscape. The complaints refer to “SmartDownload’s spying” and explain that “Defendants are using SmartDownload to eavesdrop.” Plaintiffs’ allegations consistently distinguish and isolate the functions of SmartDownload in such a way as to make it clear that it is through SmartDownload, not Communicator, that defendants committed the abuses that are the subject of the complaints.

After careful review of these allegations, we conclude that plaintiffs’ claims “present no question involving construction of the [Communicator license agreement], and no questions in respect of the parties’ rights and obligations under it.” Collins & Aikman, 58 F.3d at 23. It follows that the claims of the five user plaintiffs are beyond the scope of the arbitration clause contained in the Communicator license agreement. Because those claims are not arbitrable under that agreement or under the SmartDownload license agreement, to which plaintiffs never assented, we affirm the district court’s holding that the five user plaintiffs may not be compelled to arbitrate their claims.

V. Whether Plaintiff Specht Can Be Required To Arbitrate as a Nonparty Beneficiary

Plaintiff Specht operated a website that he claims defendants electronically spied on every time users employing SmartDownload to enhance their browser software downloaded, from his site, software files that he provided for setting up an account with a separate service called WhyWeb. Defendants counter that Specht received a “direct benefit” under the “Netscape license agreement,” which they say authorized consumers to use SmartDownload and Communicator to obtain Specht’s files. Defendants contend that if a user who obtained a file
from Specht's site subsequently subscribed to WhyWeb's service, Specht would receive a commission from WhyWeb. Thus, according to defendants, if users employing SmartDownload accessed his site and obtained WhyWeb files, Specht would receive a direct benefit "because the software assisted in obtaining a WhyWeb file and increased the likelihood of success in the download process." Specht, however, claims that he received no commissions from providing WhyWeb software.

We note at the outset that defendants do not argue, as indeed they could not, that Specht benefited from SmartDownload license agreements entered into by the named user plaintiffs or the putative class that they represent. A contract theory of third-party benefits requires a predicate contract, and we have already determined that the user plaintiffs did not assent to the SmartDownload license agreement. We are thus asked, in effect, to imagine a class of users who, having obtained SmartDownload and/or Communicator after properly assenting to license terms, visited Specht's website by means of Communicator or a non-Netscape browser enhanced by SmartDownload and, while there, downloaded WhyWeb files which they proceeded to use to subscribe to WhyWeb, in turn triggering a commission fee from WhyWeb for Specht.

Even accepting arguendo this strained and roundabout hypothesis, we must reject defendants' legal conclusion. Typically, whether a contract benefits or accords rights to a third party (most often, the right to enforce the contract) depends significantly on the intention of the original contracting parties. See Sessions Payroll Mgmt., Inc. v. Noble Constr. Co, Inc., 101 Cal. Rptr. 2d 127, 133 (Cal. Ct. App. 2000) (explaining that a third-party beneficiary may enforce a contract made expressly for its benefit and has the burden of proving that the contracting parties actually promised the performance). Clearly, Netscape and these unknown visitors to Specht's
website did not expressly confer or intend to confer any contractual benefits on Specht or website operators generally (other than defendants). Defendants therefore take a different tack, arguing that they need only show that Specht received some direct benefit, knowingly or not, under a Netscape license agreement.

To support this claim, defendants cite *American Bureau of Shipping v. Tencara Shipyards S.P.A.*, 170 F.3d 349 (2d Cir. 1999). But the benefit at issue in *American Bureau of Shipping* was much more direct than that described by defendants. There, a ship classification society, which had issued an interim certification of classification (ICC) for a racing yacht that later suffered hull damage allegedly resulting from defective design, sought to compel the yacht’s builder, owners, and insurers to arbitrate pursuant to arbitration clauses contained in the ICC and other contracts. The owners never signed any arbitration agreement, but this Court noted that a nonsignatory could be “estopped from denying its obligation to arbitrate when it receives a ‘direct benefit’ from a contract containing an arbitration clause.” *Id.* at 353 (citing *Thomson-CSF, S.A. v. Am. Arbitration Ass'n*, 64 F.3d 773, 778-79 (2d Cir. 1995)).

The Court held that the yacht owners had received the following direct benefits under the relevant contracts: (1) significantly lower insurance rates on the yacht; (2) the ability to sail under the French flag; and possibly (3) the ability to register the yacht. *Id.*; cf. *Deloitte Noraudit A/S v. Deloitte Haskins & Sells, U.S.*, 9 F.3d 1060 (2d Cir. 1993) (holding that a nonsignatory to an arbitration agreement was bound to arbitrate because it knowingly received direct benefits, which included the right to

---

20 *Cf. County of Contra Costa v. Kaiser Found. Health Plan, Inc.*, 54 Cal. Rptr. 2d 628, 631 (Cal. Ct. App. 1996) (noting that California cases binding nonsignatories to arbitrate their claims fall into two categories: (1) where a benefit was conferred on the nonsignatory as a result of a contract; and (2) where a preexisting relationship existed between the nonsignatory and one of the parties to the arbitration agreement).
use a trade name, under the relevant contract).

Even if defendants' theory of Specht's SmartDownload-enhanced potential for earning commissions were more convincing, such an abstract advantage is not remotely as tangible and definite as the benefits that have led this Court to compel nonsignatories to arbitrate. Nor does the intricate, Rube Goldberg-like chain of events postulated by defendants constitute a "direct" benefit in the sense contemplated by _American Bureau of Shipping_ and _Deloitte Noraudit_. Because we conclude that Specht was not a direct beneficiary under SmartDownload's license agreement or any other Netscape agreement, we affirm the district court's refusal to compel arbitration of his claims.\(^{21}\)

**CONCLUSION**

For the foregoing reasons, we affirm the district court's denial of defendants' motion to compel arbitration and to stay court proceedings.

---

\(^{21}\) Plaintiffs argue in the alternative that their claims are inarbitrable because the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act reflect a congressional intent to preclude arbitration of claims arising under those statutes. In view of our disposition of this case, we need not address that argument.
Defendant, Verio, Inc. ("Verio") appeals from an order of the United States District Court for the Southern District of New York (Barbara S. Jones, J.) granting the motion of plaintiff Register.com, Inc. ("Register") for a preliminary injunction. The court's order enjoined Verio from (1) using Register's trademarks; (2) representing or otherwise suggesting to third parties that Verio's services have the sponsorship, endorsement, or approval of Register; (3) accessing Register's computers by use of automated software programs performing multiple successive queries; and (4) using data obtained from Register's database of contact information of registrants of Internet domain names to solicit the registrants for the sale of web site development services by electronic mail, telephone calls, or direct mail. We affirm.¹

BACKGROUND

This plaintiff Register is one of over fifty companies serving as registrars for the issuance of domain names on the world wide web. As a registrar, Register issues domain names to

¹ Judge Parker was not in agreement with this disposition. Deliberations have followed an unusual course. Judge Parker initially was assigned to prepare a draft opinion affirming the district court. In the course of preparing the draft, Judge Parker changed his mind and proposed to rule in favor of the defendant, overturning the injunction in most respects. Judge Parker's draft opinion, however, failed to convince the other members of the panel, who adhered to the view that the injunction should be affirmed. Judge Parker died shortly thereafter, prior to the circulation of a draft opinion affirming the injunction, from which Judge Parker presumably would have dissented.

We attach Judge Parker's draft opinion as an Appendix. We do so for two reasons: One is to expose Judge Parker's views, which would have been set forth in a dissenting opinion, but for his death; the second is because his opinion contains an exceptionally thorough, detailed and useful statement of facts, including a comprehensive description of the functioning of the domain name system. We have stated the facts more briefly, mentioning only those points necessary to the arguments discussed, inviting the reader to consult Judge Parker's very thorough fact statement for a more detailed account.
persons and entities preparing to establish web sites on the Internet. Web sites are identified and
accessed by reference to their domain names.

Register was appointed a registrar of domain names by the Internet Corporation for
Assigned Names and Numbers, known by the acronym “ICANN.” ICANN is a private, non-
profit public benefit corporation which was established by agencies of the U.S. government to
administer the Internet domain name system. To become a registrar of domain names, Register
was required to enter into a standard form agreement with ICANN, designated as the ICANN
Registrar Accreditation Agreement, November 1999 version (referred to herein as the “ICANN
Agreement”).

Applicants to register a domain name submit to the registrar contact information,
including at a minimum, the applicant’s name, postal address, telephone number, and electronic
mail address. The ICANN Agreement, referring to this registrant contact information under the
rubric “WHOIS information,” requires the registrar, under terms discussed in greater detail
below, to preserve it, update it daily, and provide for free public access to it through the Internet
as well as through an independent access port, called port 43. See ICANN Agreement § II.F.1.

Section II.F.5 of the ICANN Agreement (which furnishes a major basis for the appellant
Verio’s contentions on this appeal) requires that the registrar “not impose terms and conditions”
on the use made by others of its WHOIS data “except as permitted by ICANN-adopted policy.”
In specifying what restrictions may be imposed, the ICANN Agreement requires the registrar to
permit use of its WHOIS data “for any lawful purposes except to: . . . support the transmission of
mass unsolicited, commercial advertising or solicitations via email (spam); [and other listed
purposes not relevant to this appeal].” (emphasis added).

Another section of the ICANN Agreement (upon which appellee Register relies) provides as follows,

No Third-Party Beneficiaries: This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement . . .

ICANN Agreement § II.S.2. Third parties could nonetheless seek enforcement of a registrar’s obligations set forth in the ICANN Agreement by resort to a grievance process under ICANN’s auspices.

In compliance with § II.F.1 of the ICANN Agreement, Register updated the WHOIS information on a daily basis and established Internet and port 43 service, which allowed free public query of its WHOIS information. An entity making a WHOIS query through Register’s Internet site or port 43 would receive a reply furnishing the requested WHOIS information, captioned by a legend devised by Register, which stated,

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to . . . support the transmission of mass unsolicited, commercial advertising or solicitation via email.

The terms of that legend tracked § II.F.5 of the ICANN Agreement in specifying the restrictions Register imposed on the use of its WHOIS data. Subsequently, as explained below, Register amended the terms of this legend to impose more stringent restrictions on the use of the information gathered through such queries.

In addition to performing the function of a registrar of domain names, Register also
engages in the business of selling web-related services to entities that maintain web sites. These
services cover various aspects of web site development. In order to solicit business for the
services it offers, Register sends out marketing communications. Among the entities it solicits
for the sale of such services are entities whose domain names it registered. However, during the
registration process, Register offers registrants the opportunity to elect whether or not they will
receive marketing communications from it.

The defendant Verio, against whom the preliminary injunction was issued, is engaged in
the business of selling a variety of web site design, development and operation services. In the
sale of such services, Verio competes with Register’s web site development business. To
facilitate its pursuit of customers, Verio undertook to obtain daily updates of the WHOIS
information relating to newly registered domain names. To achieve this, Verio devised an
automated software program, or robot, which each day would submit multiple successive
WHOIS queries through the port 43 accesses of various registrars. Upon acquiring the WHOIS
information of new registrants, Verio would send them marketing solicitations by email,
telemarketing and direct mail. To the extent that Verio’s solicitations were sent by email, the
practice was inconsistent with the terms of the restrictive legend Register attached to its
responses to Verio’s queries.

At first, Verio’s solicitations addressed to Register’s registrants made explicit reference
to their recent registration through Register. This led some of the recipients of Verio’s
solicitations to believe the solicitation was initiated by Register (or an affiliate), and was sent in
violation of the registrant’s election not to receive solicitations from Register. Register began to
receive complaints from registrants. Register in turn complained to Verio and demanded that
Verio cease and desist from this form of marketing. Register asserted that Verio was harming
Register's goodwill, and that by soliciting via email, was violating the terms to which it had
agreed on submitting its queries for WHOIS information. Verio responded to the effect that it
had stopped mentioning Register in its solicitation message.

In the meantime, Register changed the restrictive legend it attached to its responses to
WHOIS queries. While previously the legend conformed to the terms of § II F.5, which
authorized Register to prohibit use of the WHOIS information for mass solicitations "via email,"
its new legend undertook to bar mass solicitation "via direct mail, electronic mail, or by
telephone."² Section II.F.5 of Register's ICANN Agreement, as noted above, required Register
to permit use of the WHOIS data "for any lawful purpose except to . . . support the transmission
of mass unsolicited solicitations via email (spam). Thus, by undertaking to prohibit Verio from
using the WHOIS information for solicitations "via direct mail . . . or by telephone," Register
was acting in apparent violation of this term of its ICANN Agreement.

Register wrote to Verio demanding that it cease using WHOIS information derived from
Register not only for email marketing, but also for marketing by direct mail and telephone.
Verio ceased using the information in email marketing, but refused to stop marketing by direct
mail and telephone.

² The new legend stated:

By submitting a WHOIS query, you agree that . . . under no circumstances will
you use this data to . . . support the transmission of mass unsolicited . . .
advancing or solicitations via direct mail, electronic mail, or by telephone.
Register brought this suit on August 3, 2000, and moved for a temporary restraining order and a preliminary injunction. Regsiter asserted, among other claims, that Verio was (a) causing confusion among customers, who were led to believe Verio was affiliated with Register; (b) accessing Register's computers without authorization, a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; and, (c) trespassing on Register's chattels in a manner likely to harm Register's computer systems by the use of Verio's automated robot software programs. On December 8, 2000, the district court entered a preliminary injunction. The injunction barred Verio from the following activities:

1. Using or causing to be used the "Register.com" mark or the "first step on the web" mark or any other designation similar thereto, on or in connection with the advertising, marketing, or promotion of Verio and/or any of Verio's services;

2. Representing, or committing any act which is calculated to or is likely to cause third parties to believe that Verio and/or Verio's services are sponsored by, or have the endorsement or approval of Register.com;

3. Accessing Register.com's computers and computer networks in any manner, including, but not limited to, by software programs performing multiple, automated, successive queries, provided that nothing in this Order shall prohibit Verio from accessing Register.com's WHOIS database in accordance with the terms and conditions thereof; and

4. Using any data currently in Verio's possession, custody or control, that using its best efforts, Verio can identify as having been obtained from Register.com's computers and computer networks to enable the transmission of unsolicited commercial electronic mail, telephone calls, or direct mail to the individuals listed in said data, provided that nothing in this Order shall prohibit Verio from (i) communicating with any of its existing customers, (ii) responding to communications received from any Register.com customer initially contacted before August 4, 2000, or (iii) communicating with any Register.com customer whose contact information is obtained by Verio from any source other than Register.com's computers and computer networks.

**DISCUSSION**

**Standard of review and preliminary injunction standard**

A grant of a preliminary injunction is reviewed on appeal for abuse of discretion, see SEC v. Cavanagh, 155 F.3d 129, 132 (2d Cir. 1998), which will be found if the district court “applies legal standards incorrectly or relies upon clearly erroneous findings of fact,” id., or “proceed[s] on the basis of an erroneous view of the applicable law,” Donovan v. Bierwirth, 680 F.2d 263, 269 (2d Cir. 1982).

Verio advances a plethora of arguments why the preliminary injunction should be vacated. We find them to be without merit. We address the most substantial of Verio’s arguments.

(a) Verio’s enforcement of the restrictions placed on Register by the ICANN Agreement

Verio conceded that it knew of the restrictions Register placed on the use of the WHOIS data and knew that, by using Register’s WHOIS data for direct mail and telemarketing solicitations, it was violating Register’s restrictions. Verio’s principal argument is that Register was not authorized to forbid Verio from using the data for direct mail and telemarketing solicitation because the ICANN Agreement prohibited Register from imposing any “terms and conditions” on use of WHOIS data, “except as permitted by ICANN-adopted policy,” which specified that Register was required to permit “any lawful purpose, except . . . mass solicitation[.]”
Register does not deny that the restrictions it imposed contravened this requirement of
the ICANN Agreement. Register contends, however, that the question whether it violated
§ II.F.5 of its Agreement with ICANN is a matter between itself and ICANN, and that Verio
cannot enforce the obligations placed on Register by the ICANN Agreement. Register points to
§ II.S.2 of the ICANN Agreement, captioned "No Third-Party Beneficiaries," which, as noted,
states that the agreement is not to be construed "to create any obligation by either ICANN or
Registrar to any non-party." Register asserts that Verio, a non-party, is asking the court to
construe § II.F.5 as creating an obligation owed by Register to Verio, and that the Agreement
expressly forbids such a construction.

ICANN intervened in the district court as an amicus curiae and strongly supports
Register's position, opposing Verio's right to invoke Register's contractual promises to ICANN.
ICANN explained that ICANN has established a remedial process for the resolution of such
disputes through which Verio might have sought satisfaction. "If Verio had concerns regarding
Register.com's conditions for access to WHOIS data, it should have raised them within the
ICANN process rather [than] simply taking Register.com's data, violating the conditions
[imposed by Register], and then seeking to justify its violation in this Court . . . . [Verio's claim
was] intended to be addressed only within the ICANN process."

ICANN asserted that the No Third-Party Beneficiary provision, barring third parties from
seeking to enforce promises made by a registrar to ICANN through court proceedings, was "vital
to the overall scheme of [its] various agreements."
This is because proper expression of the letter and spirit of ICANN policies is
most appropriately achieved through the ICANN process itself, and not through
forums that lack the every day familiarity with the intricate technical and policy
issues that the ICANN process was designed to address.

ICANN's brief went on to state:

[Enforcement of agreements with ICANN [was to] be informed by the judgment
of the various segments of the internet community as expressed through ICANN.
In the fast-paced environment of the Internet, new issues and situations arise
quickly, and sometimes the language of contractual provisions does not perfectly
match the underlying policies. For this and other reasons, hard-and-fast
enforcement [by courts] of the letter of every term of every agreement is not
always appropriate. An integral part of the agreements that the registrars . . .
entered with ICANN is the understanding that these situations would be handled
through consultation and consideration within the ICANN process . . . . Allowing
issues under the agreements registrars make with ICANN to be diverted from
[ICANN's] carefully crafted remedial scheme to the courts, at the behest of third
parties . . . , would seriously threaten the Internet community's ability, under the
auspices of ICANN, to achieve a proper balance of the competing policy values
that are so frequently involved.

We are persuaded by the arguments Register and ICANN advance. It is true Register
incurred a contractual obligation to ICANN not to prevent the use of its WHOIS data for direct
mail and telemarketing solicitation. But ICANN deliberately included in the same contract that
persons aggrieved by Register's violation of such a term should seek satisfaction within the
framework of ICANN's grievance policy, and should not be heard in courts of law to plead
entitlement to enforce Register's promise to ICANN. As experience develops in the fast
changing world of the Internet, ICANN, informed by the various constituencies in the Internet
community, might well no longer consider it salutary to enforce a policy which it earlier
expressed in the ICANN Agreement. For courts to undertake to enforce promises made by
registrars to ICANN at the instance of third parties might therefore be harmful to ICANN's
efforts to develop well-informed and sound Internet policy.

Verio’s invocation of the ICANN Agreement necessarily depends on its entitlement to enforce Register’s promises to ICANN in the role of third party beneficiary. The ICANN Agreement specified that it should be deemed to have been made in California, where ICANN is located. Under § 1559 of the California Civil Code, a “contract, made expressly for the benefit of a third person, may be enforced by him.” Cal. Civ. Code § 1559. For Verio to seek to enforce Register’s promises it made to ICANN in the ICANN Agreement, Verio must show that the Agreement was made for its benefit. See Am. Home Ins. Co. v. Travelers Indemnity Co., 175 Cal. Rptr. 826, 834 (Cal. App. 1981). Verio did not meet this burden. To the contrary, the Agreement expressly and intentionally excluded non-parties from claiming rights under it in court proceedings.

We are not persuaded by the arguments Judge Parker advanced in his draft. Although acknowledging that Verio could not claim third party beneficiary rights to enforce Register’s promises to ICANN, Judge Parker nonetheless found three reasons for enforcing Verio’s claim: (i) “public policy interests at stake,” (ii) Register’s “indisputable obligations to ICANN as a registrar,” and (iii) the equities, involving Register’s “unclean hands” in imposing a restriction it was contractually bound not to impose. We respectfully disagree. As for the first argument, that Register’s restriction violated public policy, it is far from clear that this is so.\(^3\) It is true that the

\(^3\) We note in passing, Judge Parker’s characterization of the public policy — that WHOIS information should be “free as air” — is a rhetorical oversimplification; the public policy as set forth in the ICANN Agreement expressly contemplated that the WHOIS data not be available for use in mass email solicitation. It also imposed another restriction not pertinent to this appeal and expressly reserved the possibility that further restrictions might be imposed if and when “ICANN adopts a different policy.” ICANN Agreement § II.F.5.
ICANN Agreement at the time ICANN presented it to Register permitted mass solicitation by means other than email. But it is not clear that at the time of this dispute, ICANN intended to adhere to that policy. As ICANN’s amicus brief suggested, the world of the Internet changes rapidly, and public policy as to how that world should be governed may change rapidly as well. ICANN in fact has since changed the terms of its standard agreement for the accreditation of registrars to broaden the uses of WHOIS information that registrars may prohibit to include not only mass email solicitations but also mass telephone and fax solicitations. See ICANN Registrar Accreditation Agreement § 3.3.5 (May 18, 2001). It is far from clear that ICANN continues to view public policy the way it did at the time it crafted Register’s agreement. In any event, if Verio wished to have the dispute resolved in accordance with public policy, it was free to bring its grievance to ICANN. Verio declined to do so. ICANN included the “No Third-Party Beneficiary” provision precisely so that it would retain control of enforcement of policy, rather than yielding it to courts.

As for Judge Parker’s second argument, Register’s “indisputable obligation to ICANN as a registrar” to permit Verio to use the WHOIS information for mass solicitation by mail and telephone, we do not see how this argument differs from Verio’s claim of entitlement as a third party beneficiary, which § II.S.2 explicitly negates. The fact that Register owed a contractual obligation to ICANN not to impose certain restrictions on use of WHOIS information does not mean that it owed an obligation to Verio not to impose such restrictions. As ICANN’s brief in the district court indicates, ICANN was well aware of Register’s deviation from the restrictions imposed by the ICANN Agreement, but ICANN chose not to take steps to compel Register to
adhere to its contract.

Nor are we convinced by Judge Parker’s third argument of Register’s “unclean hands.” Judge Parker characterizes Register’s failure to honor its contractual obligation to ICANN as unethical conduct, making Register ineligible for equitable relief. But Register owed no duty in that regard to anyone but ICANN, and ICANN has expressed no dissatisfaction with Register’s failure to adhere to that term of the contract. Verio was free to seek ICANN’s intervention on its behalf, but declined to do so, perhaps because it knew or suspected that ICANN would decline to compel Register to adhere to the contract term. Under the circumstances, we see no reason to assume on appeal that Register’s conduct should be considered unethical, especially where the district court made no such finding.

(b) Verio’s assent to Register’s contract terms

Verio’s next contention assumes that Register was legally authorized to demand that takers of WHOIS data from its systems refrain from using it for mass solicitation by mail and telephone, as well as by email. Verio contends that it nonetheless never became contractually bound to the conditions imposed by Register’s restrictive legend because, in the case of each query Verio made, the legend did not appear until after Verio had submitted the query and received the WHOIS data. Accordingly, Verio contends that in no instance did it receive legally enforceable notice of the conditions Register intended to impose. Verio therefore argues it should not be deemed to have taken WHOIS data from Register’s systems subject to Register’s conditions.
Verio’s argument might well be persuasive if its queries addressed to Register’s computers had been sporadic and infrequent. If Verio had submitted only one query, or even if it had submitted only a few sporadic queries, that would give considerable force to its contention that it obtained the WHOIS data without being conscious that Register intended to impose conditions, and without being deemed to have accepted Register’s conditions. But Verio was daily submitting numerous queries, each of which resulted in its receiving notice of the terms Register exacted. Furthermore, Verio admits that it knew perfectly well what terms Register demanded. Verio’s argument fails.

The situation might be compared to one in which plaintiff P maintains a roadside fruit stand displaying bins of apples. A visitor, defendant D, takes an apple and bites into it. As D turns to leave, D sees a sign, visible only as one turns to exit, which says “Apples – 50 cents apiece.” D does not pay for the apple. D believes he has no obligation to pay because he had no notice when he bit into the apple that 50 cents was expected in return. D’s view is that he never agreed to pay for the apple. Thereafter, each day, several times a day, D revisits the stand, takes an apple, and eats it. D never leaves money.

P sues D in contract for the price of the apples taken. D defends on the ground that on no occasion did he see P’s price notice until after he had bitten into the apples. D may well prevail as to the first apple taken. D had no reason to understand upon taking it that P was demanding the payment. In our view, however, D cannot continue on a daily basis to take apples for free, knowing full well that P is offering them only in exchange for 50 cents in compensation, merely because the sign demanding payment is so placed that on each occasion D does not see it until he
has bitten into the apple.

Verio’s circumstance is effectively the same. Each day Verio repeatedly enters Register’s computers and takes that day’s new WHOIS data. Each day upon receiving the requested data, Verio receives Register’s notice of the terms on which it makes the data available—that the data not be used for mass solicitation via direct mail, email, or telephone. Verio acknowledges that it continued drawing the data from Register’s computers with full knowledge that Register offered access subject to these restrictions. Verio is no more free to take Register's data without being bound by the terms on which Register offers it, than D was free, in the example, once he became aware of the terms of P’s offer, to take P’s apples without obligation to pay the 50 cent price at which P offered them.

Verio seeks support for its position from cases that have dealt with the formation of contracts on the Internet. An excellent example, although decided subsequent to the submission of this case, is Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002). The dispute was whether users of Netscape’s software, who downloaded it from Netscape’s web site, were bound by an agreement to arbitrate disputes with Netscape, where Netscape had posted the terms of its offer of the software (including the obligation to arbitrate disputes) on the web site from which they downloaded the software. We ruled against Netscape and in favor of the users of its software because the users would not have seen the terms Netscape exacted without scrolling down their computer screens, and there was no reason for them to do so. The evidence did not demonstrate that one who had downloaded Netscape’s software had necessarily seen the terms of its offer.
Verio, however, cannot avail itself of the reasoning of *Specht*. In *Specht*, the users in
whose favor we decided visited Netscape’s web site one time to download its software.
Netscape’s posting of its terms did not compel the conclusion that its downloaders took the
software subject to those terms because there was no way to determine that any downloader had
seen the terms of the offer. There was no basis for imputing to the downloaders of Netscape’s
software knowledge of the terms on which the software was offered. This case is crucially
different. Verio visited Register’s computers daily to access WHOIS data and each day saw the
terms of Register’s offer; Verio admitted that, in entering Register’s computers to get the data, it
was fully aware of the terms on which Register offered the access.

Verio’s next argument is that it was not bound by Register’s terms because it rejected
them. Even assuming Register is entitled to demand compliance with its terms in exchange for
Verio’s entry into its systems to take WHOIS data, and even acknowledging that Verio was fully
aware of Register’s terms, Verio contends that it still is not bound by Register’s terms because it
did not agree to be bound. In support of its claim, Verio cites a district court case from the
WL 1887522 (C.D. Cal. Aug. 10, 2000), in which the court rejected Ticketmaster’s application
for a preliminary injunction to enforce posted terms of use of data available on its website
against a regular user. Noting that the user of Ticketmaster’s web site is not required to check an
“I agree” box before proceeding, the court concluded that there was insufficient proof of
agreement to support a preliminary injunction. Id. at *5.

We acknowledge that the *Ticketmaster* decision gives Verio some support, but not
enough. In the first place, the Ticketmaster court was not making a definitive ruling rejecting Ticketmaster’s contract claim. It was rather exercising a district court’s discretion to deny a preliminary injunction because of a doubt whether the movant had adequately shown likelihood of success on the merits.

But more importantly, we are not inclined to agree with the Ticketmaster court’s analysis. There is a crucial difference between the circumstances of Specht, where we declined to enforce Netscape’s specified terms against a user of its software because of inadequate evidence that the user had seen the terms when downloading the software, and those of Ticketmaster, where the taker of information from Ticketmaster’s site knew full well the terms on which the information was offered but was not offered an icon marked, “I agree,” on which to click. Under the circumstances of Ticketmaster, we see no reason why the enforceability of the offeror’s terms should depend on whether the taker states (or clicks), “I agree.”

We recognize that contract offers on the Internet often require the offeree to click on an “I agree” icon. And no doubt, in many circumstances, such a statement of agreement by the offeree is essential to the formation of a contract. But not in all circumstances. While new commerce on the Internet has exposed courts to many new situations, it has not fundamentally changed the principles of contract. It is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree. See, e.g., Restatement (Second) of Contracts § 69 (1)(a) (1981) (“[S]ilence and inaction operate as an acceptance . . . [w]here an offeree takes the benefit of
offered services with reasonable opportunity to reject them and reason to know that they were
offered with the expectation of compensation.”); 2 Richard A. Lord, Williston on Contracts § 6:9
(4th ed. 1991) (“[T]he acceptance of the benefit of services may well be held to imply a promise
to pay for them if at the time of acceptance the offeree has a reasonable opportunity to reject the
service and knows or has reason to know that compensation is expected.”); Arthur Linton
Corbin, Corbin on Contracts § 71 (West 1 vol. ed. 1952) (“The acceptance of the benefit of the
services is a promise to pay for them, if at the time of accepting the benefit the offeree has a
reasonable opportunity to reject it and knows that compensation is expected.”); Jones v. Brisbin,
41 Wash. 2d 167, 172 (1952) (“Where a person, with reasonable opportunity to reject offered
services, takes the benefit of them under circumstances which would indicate, to a reasonable
man, that they were offered with the expectation of compensation, a contract, complete with
mutual assent, results.”); Markstein Bros. Millinery Co. v. J.A. White & Co., 151 Ark. 1 (1921)
(buyer of hats was bound to pay for hats when buyer failed to return them to seller within five
days of inspection as seller requested in clear and obvious notice statement).

Returning to the apple stand, the visitor, who sees apples offered for 50 cents apiece and
takes an apple, owes 50 cents, regardless whether he did or did not say, “I agree.” The choice
offered in such circumstances is to take the apple on the known terms of the offer or not to take
the apple. As we see it, the defendant in Ticketmaster and Verio in this case had a similar
choice. Each was offered access to information subject to terms of which they were well aware.
Their choice was either to accept the offer of contract, taking the information subject to the terms
of the offer, or, if the terms were not acceptable, to decline to take the benefits.
We find that the district court was within its discretion in concluding that Register showed likelihood of success on the merits of its contract claim.

(c) Irreparable harm

Verio contends that an injunction is not appropriate to enforce the terms of a contract. It is true that specific relief is not the conventional remedy for breach of contract, but there is certainly no ironclad rule against its use. Specific relief may be awarded in certain circumstances.

If an injury can be appropriately compensated by an award of monetary damages, then an adequate remedy at law exists, and no irreparable injury may be found to justify specific relief. *Borey v. Nat'l Union Fire Ins. Co.*, 934 F.2d 30, 34 (2d Cir. 1991). But, irreparable harm may be found where damages are difficult to establish and measure. *Ticor Title Ins. Co. v. Cohen*, 173 F.3d 63, 69 (2d Cir. 1999). We have found, for example, that injunctive relief is appropriate where it would be “very difficult to calculate monetary damages that would successfully redress the loss of a relationship with a client that would produce an indeterminate amount of business in years to come.” *Id.* at 69.

The district court found it impossible to estimate “with any precision the amount of the monetary loss which has resulted and which would result in the future from the loss of Register.com's relationships with customers and co-brand partners,” by reason of Verio’s actions. *Register.com*, 126 F. Supp. 2d at 248. In our view, the district court did not abuse its discretion in finding that, unless specific relief were granted, Verio’s actions would cause
Register irreparable harm through loss of reputation, good will, and business opportunities.

(d) Trespass to chattels

Verio also attacks the grant of the preliminary injunction against its accessing Register’s computers by automated software programs performing multiple successive queries. This prong of the injunction was premised on Register’s claim of trespass to chattels. Verio contends the ruling was in error because Register failed to establish that Verio’s conduct resulted in harm to Register’s servers and because Verio’s robot access to the WHOIS database through Register was “not unauthorized.” We believe the district court’s findings were within the range of its permissible discretion.

“A trespass to a chattel may be committed by intentionally . . . using or intermeddling with a chattel in the possession of another,” Restatement (Second) of Torts § 217(b) (1965), where “the chattel is impaired as to its condition, quality, or value,” id. § 218(b); see also City of Amsterdam v. Goldreyer Ltd., 882 F. Supp. 1273, 1281 (E.D.N.Y. 1995) (citing the Restatement definition as New York law).

The district court found that Verio’s use of search robots, consisting of software programs performing multiple automated successive queries, consumed a significant portion of the capacity of Register’s computer systems. While Verio’s robots alone would not incapacitate Register’s systems, the court found that if Verio were permitted to continue to access Register’s computers through such robots, it was “highly probable” that other Internet service providers would devise similar programs to access Register’s data, and that the system would be overtaxed.
and would crash. We cannot say these findings were unreasonable.

Nor is there merit to Verio’s contention that it cannot be engaged in trespass when Register had never instructed it not to use its robot programs. As the district court noted, Register’s complaint sufficiently advised Verio that its use of robots was not authorized and, according to Register’s contentions, would cause harm to Register’s systems.

(e) Lanham Act

On Register’s claim for trademark infringement and unfair competition under the Lanham Act, the district court enjoined Verio from using Register’s marks, including “Register.com” and “first step on the web,” as well as from committing acts “calculated to or . . . likely to cause third parties to believe that Verio” is sponsored, endorsed or approved by Register. By letter submitted after oral argument, Register agreed to the deletion of the prohibition concerning use of “first step on the web.” See Letter from William Patry, Counsel for Register, to the U.S. Court of Appeals for the Second Circuit (May 22, 2001). We accordingly direct the district court to modify the preliminary injunction by deleting the prohibition of use of “first step on the web.”

Verio contends there was no adequate basis for the portion of the injunction based on the Lanham Act. We disagree. In our view, the injunction was within the scope of the court’s permitted discretion.

The district court found two bases for the injunction. The first was that in its early calls to recent registrants to solicit the sale of web site development services, Verio explicitly referred
§ 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)

(i) 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;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(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 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) except as provided in subparagraph (B), 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)(A)(ii), 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, 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; and

(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), or an attempt to commit an offense punishable under this subparagraph, if—

(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;

(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) 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)(ii), 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;

(4)

(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)

(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y))), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

(3) Such authority 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, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) [2] of the Federal Reserve Act;
(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;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(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;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) 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. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(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).
IN THE SUPREME COURT OF CALIFORNIA

INTEL CORPORATION,

Plaintiff and Respondent,

v.

KOUROSH KENNETH HAMIDI,

Defendant and Appellant.

S103781

Ct.App. 3 C033076

Sacramento County
Super. Ct. No. 98AS05067

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel’s employment practices to numerous current employees on Intel’s electronic mail system. Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so wished. Hamidi’s communications to individual Intel employees caused neither physical damage nor functional disruption to the company’s computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused discussion among employees and managers.
On these facts, Intel brought suit, claiming that by communicating with its employees over the company's e-mail system Hamidi committed the tort of trespass to chattels. The trial court granted Intel’s motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed.

After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor’s use or possession of, or any other legally protected interest in, the personal property itself. (See Zaslow v. Kroenert (1946) 29 Cal.2d 541, 551; Ticketmaster Corp. v. Tickets.com, Inc. (C.D.Cal., Aug. 10, 2000, No. 99CV7654) 2000 WL 1887522, p. *4; Rest.2d Torts, § 218.) The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi’s messages and company efforts to block the messages, is not an injury to the company’s interest in its computers—which worked as intended and were unharmed by the communications—any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient’s mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient’s telephone equipment.

Our conclusion does not rest on any special immunity for communications by electronic mail; we do not hold that messages transmitted through the Internet are exempt from the ordinary rules of tort liability. To the contrary, e-mail, like other forms of communication, may in some circumstances cause legally
cognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories. Indeed, on facts somewhat similar to those here, a company or its employees might be able to plead causes of action for interference with prospective economic relations (see *Guillory v. Godfrey* (1955) 134 Cal.App.2d 628, 630-632 [defendant berated customers and prospective customers of plaintiffs’ cafe with disparaging and racist comments]), interference with contract (see *Blender v. Superior Court* (1942) 55 Cal.App.2d 24, 25-27 [defendant made false statements about plaintiff to his employer, resulting in plaintiff’s discharge]) or intentional infliction of emotional distress (see *Kisesky v. Carpenters’ Trust for So. California* (1983) 144 Cal.App.3d 222, 229-230 [agents of defendant union threatened life, health, and family of employer if he did not sign agreement with union].) And, of course, as with any other means of publication, third party subjects of e-mail communications may under appropriate facts make claims for defamation, publication of private facts, or other speech-based torts. (See, e.g., *Southridge Capital Management v. Lowry* (S.D.N.Y. 2002) 188 F.Supp.2d 388, 394-396 [allegedly false statements in e-mail sent to several of plaintiff’s clients support actions for defamation and interference with contract].) Intel’s claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort—unlike the causes of action just mentioned—may not, in California, be proved without evidence of an injury to the plaintiff’s personal property or legal interest therein.

Nor does our holding affect the legal remedies of Internet service providers (ISP’s) against senders of unsolicited commercial bulk e-mail (UCE), also known as “spam.” (See *Ferguson v. Friendfinders, Inc.* (2002) 94 Cal.App.4th 1255, 1267.) A series of federal district court decisions, beginning with *CompuServe, Inc. v. Cyber Promotions, Inc.* (S.D.Ohio 1997) 962 F.Supp. 1015, has approved the use of trespass to chattels as a theory of spammers’ liability to ISP’s, based
upon evidence that the vast quantities of mail sent by spammers both
overburdened the ISP’s own computers and made the entire computer system
harder to use for recipients, the ISP’s customers. (See id. at pp. 1022-1023.) In
those cases, discussed in greater detail below, the underlying complaint was that
the extraordinary quantity of UCE impaired the computer system’s functioning. In
the present case, the claimed injury is located in the disruption or distraction
caused to recipients by the contents of the e-mail messages, an injury entirely
separate from, and not directly affecting, the possession or value of personal
property.

**FACTUAL AND PROCEDURAL BACKGROUND**

We review a grant of summary judgment de novo; we must decide
independently whether the facts not subject to triable dispute warrant judgment for
the moving party as a matter of law. (Galanty v. Paul Revere Life Ins. Co. (2000)
Proc., § 437c, subd. (c).) The pertinent undisputed facts are as follows.

Hamidi, a former Intel engineer, together with others, formed an
organization named Former and Current Employees of Intel (FACE-Intel) to
disseminate information and views critical of Intel’s employment and personnel
policies and practices. FACE-Intel maintained a Web site (which identified
Hamidi as Webmaster and as the organization’s spokesperson) containing such
material. In addition, over a 21-month period Hamidi, on behalf of FACE-Intel,
sent six mass e-mails to employee addresses on Intel’s electronic mail system.
The messages criticized Intel’s employment practices, warned employees of the
dangers those practices posed to their careers, suggested employees consider
moving to other companies, solicited employees’ participation in FACE-Intel, and
urged employees to inform themselves further by visiting FACE-Intel’s Web site.
The messages stated that recipients could, by notifying the sender of their wishes,
be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's Web site), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had occurred.\(^1\) Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff

\(^1\) To the extent, therefore, that Justice Mosk suggests Hamidi breached the security of Intel's internal computer network by "circumvent[ing]" Intel's "security measures" and entering the company's "intranet" (dis. opn. of Mosk, J., post, at p. 1), the evidence does not support such an implication. An "intranet" is "a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization." (<http://www.webopedia.com/TERM/i/intranet.html [as of June 30, 2003].) Hamidi used only a part of Intel's computer network accessible to outsiders.
time was consumed in attempts to block further messages from FACE-Intel. According to the FACE-Intel Web site, moreover, the messages had prompted discussions between “[e]xcited and nervous managers” and the company’s human resources department.

Intel sued Hamidi and FACE-Intel, pleading causes of action for trespass to chattels and nuisance, and seeking both actual damages and an injunction against further e-mail messages. Intel later voluntarily dismissed its nuisance claim and waived its demand for damages. The trial court entered default against FACE-Intel upon that organization’s failure to answer. The court then granted Intel’s motion for summary judgment, permanently enjoining Hamidi, FACE-Intel, and their agents “from sending unsolicited e-mail to addresses on Intel’s computer systems.” Hamidi appealed; FACE-Intel did not.²

The Court of Appeal, with one justice dissenting, affirmed the grant of injunctive relief. The majority took the view that the use of or intermeddling with another’s personal property is actionable as a trespass to chattels without proof of any actual injury to the personal property; even if Intel could not show any damages resulting from Hamidi’s sending of messages, “it showed he was disrupting its business by using its property and therefore is entitled to injunctive relief based on a theory of trespass to chattels.” The dissenting justice warned that the majority’s application of the trespass to chattels tort to “unsolicited electronic mail that causes no harm to the private computer system that receives it” would

² For the first time, in this court, Intel argues Hamidi’s appeal is moot because, as FACE-Intel’s agent, Hamidi is bound, whatever the outcome of his own appeal, by the unappealed injunction against FACE-Intel. But as Hamidi points out in response, he could avoid the unappealed injunction simply by resigning from FACE-Intel; his own appeal is therefore not moot.
“expand the tort of trespass to chattel in untold ways and to unanticipated circumstances.”

We granted Hamidi’s petition for review.³

DISCUSSION

I. Current California Tort Law

Dubbed by Prosser the “little brother of conversion,” the tort of trespass to chattels allows recovery for interferences with possession of personal property “not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered.” (Prosser & Keeton, Torts (5th ed. 1984) § 14, pp. 85-86.)

Though not amounting to conversion, the defendant’s interference must, to be actionable, have caused some injury to the chattel or to the plaintiff’s rights in it. Under California law, trespass to chattels “lies where an intentional interference with the possession of personal property has proximately caused injury.” (Thrifty-Tel, Inc. v. Bezenek (1996) 46 Cal.App.4th 1559, 1566, italics added.) In cases of interference with possession of personal property not amounting to conversion, “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, supra, 29 Cal.2d at p. 551, italics added; accord, Jordan v. Talbot (1961) 55 Cal.2d 597, 610.) In modern American law generally, “[t]respass remains as an occasional remedy for

³ We grant both parties’ requests for notice of legislative history materials relating to California laws on spam and on injunctions in labor dispute cases. Hamidi’s further request for notice of the “undisputed” fact that “e-mail messages that travel into computer equipment consist of electromagnetic waves” is denied as irrelevant.
minor interferences, *resulting in some damage*, but not sufficiently serious or sufficiently important to amount to the greater tort" of conversion. (Prosser & Keeton, Torts, *supra*, § 15, p. 90, italics added.)

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable. Under section 218 of the Restatement Second of Torts, dispossession alone, without further damages, is actionable (see *id.*, par. (a) & com. d, pp. 420-421), but other forms of interference require some additional harm to the personal property or the possessor's interests in it. (*Id.*, pars. (b)-(d).) "The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c). Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference." (*Id.*, com. e, pp. 421-422, italics added.)

The Court of Appeal (quoting 7 Speiser et al., American Law of Torts (1990) Trespass, § 23:23, p. 667) referred to "'a number of very early cases [showing that] any unlawful interference, however slight, with the enjoyment by another of his personal property, is a trespass.'" But while a harmless use or touching of personal property may be a technical trespass (see Rest.2d Torts,
§ 217), an interference (not amounting to dispossessing) is not actionable, under modern California and broader American law, without a showing of harm. As already discussed, this is the rule embodied in the Restatement (Rest.2d Torts, § 218) and adopted by California law (Zaslow v. Kroenert, supra, 29 Cal.2d at p. 551; Thrifty-Tel, Inc. v. Bezenek, supra, 46 Cal.App.4th at p. 1566).

In this respect, as Prosser explains, modern day trespass to chattels differs both from the original English writ and from the action for trespass to land:

“Another departure from the original rule of the old writ of trespass concerns the necessity of some actual damage to the chattel before the action can be maintained. Where the defendant merely interferes without doing any harm—as where, for example, he merely lays hands upon the plaintiff’s horse, or sits in his car—there has been a division of opinion among the writers, and a surprising dearth of authority. By analogy to trespass to land there might be a technical tort in such a case . . . Such scanty authority as there is, however, has considered that the dignitary interest in the inviolability of chattels, unlike that as to land, is not sufficiently important to require any greater defense than the privilege of using reasonable force when necessary to protect them. Accordingly it has been held that nominal damages will not be awarded, and that in the absence of any actual damage the action will not lie.” (Prosser & Keeton, Torts, supra, § 14, p. 87, italics added, fns. omitted.)

Intel suggests that the requirement of actual harm does not apply here because it sought only injunctive relief, as protection from future injuries. But as Justice Kolkey, dissenting below, observed, “[T]he fact the relief sought is injunctive does not excuse a showing of injury, whether actual or threatened.” Indeed, in order to obtain injunctive relief the plaintiff must ordinarily show that the defendant’s wrongful acts threaten to cause irreparable injuries, ones that cannot be adequately compensated in damages. (5 Witkin, Cal. Procedure (4th ed.
1997) Pleading, § 782, p. 239.) Even in an action for trespass to real property, in which damage to the property is not an element of the cause of action, “the extraordinary remedy of injunction” cannot be invoked without showing the likelihood of irreparable harm. (Mechanics' Foundry v. Ryall (1888) 75 Cal. 601, 603; see Mendelson v. McCabe (1904) 144 Cal. 230, 232-233 [injunction against trespass to land proper where continued trespasses threaten creation of prescriptive right and repetitive suits for damages would be inadequate remedy].) A fortiori, to issue an injunction without a showing of likely irreparable injury in an action for trespass to chattels, in which injury to the personal property or the possessor’s interest in it is an element of the action, would make little legal sense.

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi’s actions caused or threatened to cause damage to Intel’s computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed evidence revealed no actual or threatened damage to Intel’s computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi’s messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi’s electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel’s computers. In sum, no evidence suggested that in sending messages through Intel’s Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from FACE-Intel’s mailing list was not honored. The evidence did show, however, that some employees who found the messages unwelcome asked management to stop them
and that Intel technical staff spent time and effort attempting to block the messages. A statement on the FACE-Intel Web site, moreover, could be taken as an admission that the messages had caused “[e]xcited and nervous managers” to discuss the matter with Intel’s human resources department.

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi’s messages, its interest in the “physical condition, quality or value” (Rest.2d Torts, § 218, com. e, p. 422) of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers’ functioning.

In Thrifty-Tel, Inc. v. Bezenek, supra, 46 Cal.App.4th at pages 1566-1567 (Thrifty-Tel), the California Court of Appeal held that evidence of automated searching of a telephone carrier’s system for authorization codes supported a cause of action for trespass to chattels. The defendant’s automated dialing program “overburdened the [plaintiff’s] system, denying some subscribers access to phone lines” (Thrifty-Tel, supra, 46 Cal.App.4th at p. 1564), showing the requisite injury.


In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In *CompuServe*, the plaintiff ISP’s mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed “a tremendous burden” on the ISP’s equipment, using “disk space and drain[ing] the processing power,” making those resources unavailable to serve subscribers. (*CompuServe, supra,* 962 F.Supp. at p. 1022.) Similarly, in *Hotmail Corp. v. Van$ Money Pie, Inc., supra,* 1998 WL 388389 at page *7, the court found the evidence supported a finding that the defendant’s mailings “fill[ed] up Hotmail’s computer storage space and threaten[ed] to damage Hotmail’s ability to service its legitimate customers.” *America Online, Inc. v. IMS,* decided on summary judgment, was deemed factually indistinguishable from *CompuServe;* the court observed that in both cases the plaintiffs “alleged that processing the bulk e-mail cost them time and money and burdened their equipment.” (*America Online, Inc. v. IMS, supra,* 24 F.Supp.2d at p. 550.) The same court, in *America Online, Inc. v. LCGM, Inc., supra,* 46 F.Supp.2d at page 452, simply followed *CompuServe* and its earlier *America Online* decision, quoting the former’s explanation that UCE burdened the computer’s processing power and memory.

Building on the spamming cases, in particular *CompuServe*, three even more recent district court decisions addressed whether unauthorized robotic data collection from a company’s publicly accessible Web site is a trespass on the

---

4 Data search and collection robots, also known as “Web bots” or “spiders,” are programs designed to rapidly search numerous Web pages or sites, collecting, (Footnote continued on next page.)
company's computer system. (eBay, Inc. v. Bidder's Edge, Inc., supra, 100 F.Supp.2d at pp. 1069-1072 (eBay); Register.com, Inc. v. Verio, Inc. (S.D.N.Y. 2000) 126 F.Supp.2d 238, 248-251; Ticketmaster Corp. v. Tickets.com, Inc., supra, 2000 WL 1887522, at p. *4.) The two district courts that found such automated data collection to constitute a trespass relied, in part, on the deleterious impact this activity could have, especially if replicated by other searchers, on the functioning of a Web site's computer equipment.

In the leading case, eBay, the defendant Bidder's Edge (BE), operating an auction aggregation site, accessed the eBay Web site about 100,000 times per day, accounting for between 1 and 2 percent of the information requests received by eBay and a slightly smaller percentage of the data transferred by eBay. (eBay, supra, 100 F.Supp.2d at pp. 1061, 1063.) The district court rejected eBay's claim that it was entitled to injunctive relief because of the defendant's unauthorized presence alone, or because of the incremental cost the defendant had imposed on operation of the eBay site (id. at pp. 1065-1066), but found sufficient proof of threatened harm in the potential for others to imitate the defendant's activity: "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." (Id. at p. 1066.) Again, in addressing the

likelihood of eBay’s success on its trespass to chattels cause of action, the court held the evidence of injury to eBay’s computer system sufficient to support a preliminary injunction: “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.” (Id. at pp. 1071-1072.)

Another district court followed eBay on similar facts—a domain name registrar’s claim against a Web hosting and development site that robotically searched the registrar’s database of newly registered domain names in search of business leads—in Register.com, Inc. v. Verio, Inc., supra, 126 F.Supp.2d at pages 249-251. Although the plaintiff was unable to measure the burden the defendant’s searching had placed on its system (id. at pp. 249-250), the district court, quoting the declaration of one of the plaintiff’s officers, found sufficient evidence of threatened harm to the system in the possibility the defendant’s activities would be copied by others: “I believe that if Verio’s searching of Register.com’s WHOIS database were determined to be lawful, then every purveyor of Internet-based services would engage in similar conduct.” (Id. at p. 250.) Like eBay, the court observed, Register.com had a legitimate fear “that its servers will be flooded by search robots.” (Id. at p. 251.)

In the third decision discussing robotic data collection as a trespass, Ticketmaster Corp. v. Tickets.com, Inc., supra, 2000 WL 1887522 (Ticketmaster), the court, distinguishing eBay, found insufficient evidence of harm to the chattel to constitute an actionable trespass: “A basic element of trespass to chattels must be physical harm to the chattel (not present here) or some obstruction of its basic function (in the court’s opinion not sufficiently shown here). . . . The comparative
use [by the defendant of the plaintiff’s computer system] appears very small and there is no showing that the use interferes to any extent with the regular business of [the plaintiff]. . . . Nor here is the specter of dozens or more parasites joining the fray, the cumulative total of which could affect the operation of [the plaintiff’s] business.” (Id. at p. *4, italics added.)

In the decisions so far reviewed, the defendant’s use of the plaintiff’s computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power. In Ticketmaster, supra, 2000 WL 1887522, the one case where no such effect, actual or threatened, had been demonstrated, the court found insufficient evidence of harm to support a trespass action. These decisions do not persuade us to Intel’s position here, for Intel has demonstrated neither any appreciable effect on the operation of its computer system from Hamidi’s messages, nor any likelihood that Hamidi’s actions will be replicated by others if found not to constitute a trespass.

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi’s activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. The individual advertisers sued in America Online, Inc. v. IMS, supra, 24 F.Supp.2d at page 549, and America Online, Inc. v. LCGM, Inc., supra, 46 F.Supp.2d at page 448, were alleged to have sent more than 60 million messages over 10 months and more than 92 million messages over seven months, respectively. Collectively, UCE has reportedly come to constitute about 45 percent of all e-mail. (Hansell, Internet Is Losing Ground in Battle Against Spam,
N.Y. Times (Apr. 22, 2003) p. A1, col. 3.) The functional burden on Intel’s computers, or the cost in time to individual recipients, of receiving Hamidi’s occasional advocacy messages cannot be compared to the burdens and costs caused ISP’s and their customers by the ever-rising deluge of commercial e-mail.

Intel relies on language in the ebay decision suggesting that unauthorized use of another’s chattel is actionable even without any showing of injury: “Even if, as [defendant] 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.” (ebay, supra, 100 F.Supp.2d at p. 1071.) But as the eBay court went on immediately to find that the defendant’s conduct, if widely replicated, would likely impair the functioning of the plaintiff’s system (id. at pp. 1071-1072), we do not read the quoted remarks as expressing the court’s complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no right temporarily to use another’s personal property, such use is actionable as a trespass only if it “has proximately caused injury.” (Thrifty-Tel, supra, 46 Cal.App.4th at p. 1566.) “[I]n the absence of any actual damage the action will not lie.” (Prosser & Keeton, Torts, supra, § 14, p. 87.) Short of dispossession, personal injury, or physical damage (not present here), intermeddling is actionable only if “the chattel is impaired as to its condition, quality, or value, or [¶] . . . the possessor is deprived of the use of the chattel for a substantial time.” (Rest.2d Torts, § 218, pars. (b), (c).) In particular, an actionable deprivation of use “must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession . . . .” (Id., com. i, p. 423.) That Hamidi’s messages temporarily used some portion of the Intel computers’
processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system.\(^5\)

In addition to impairment of system functionality, CompuServe and its progeny also refer to the ISP's loss of business reputation and customer goodwill, resulting from the inconvenience and cost that spam causes to its members, as harm to the ISP's legally protected interests in its personal property. (See CompuServe, supra, 962 F.Supp.2d at p. 1023; Hotmail Corp. v. Van$ Money Pie, Inc., supra, 1998 WL 388389 at p. *7; America Online, Inc. v. IMS, supra, 24 F.Supp.2d at p. 550.) Intel argues that its own interest in employee productivity, assertedly disrupted by Hamidi's messages, is a comparable protected interest in its computer system. We disagree.

Whether the economic injuries identified in CompuServe were properly considered injuries to the ISP's possessory interest in its personal property, the type of property interest the tort is primarily intended to protect (see Rest.2d Torts, § 218 & com. e, pp. 421-422; Prosser & Keeton, Torts, supra, § 14, p. 87), has

\(^5\) In the most recent decision relied upon by Intel, Oyster Software, Inc. v. Forms Processing, Inc. (N.D.Cal., Dec. 6, 2001, No. C-00-0724 JCS) 2001 WL 1736382, pages *12-*13, a federal magistrate judge incorrectly read eBay as establishing, under California law, that mere unauthorized use of another's computer system constitutes an actionable trespass. The plaintiff accused the defendant, a business competitor, of copying the metatags (code describing the contents of a Web site to a search engine) from the plaintiff's Web site, resulting in diversion of potential customers for the plaintiff's services. (Id. at pp. *1-*2.) With regard to the plaintiff's trespass claim (the plaintiff also pleaded causes of action for, inter alia, misappropriation, copyright and trademark infringement), the magistrate judge concluded that eBay imposed no requirement of actual damage and that the defendant's conduct was sufficient to establish a trespass "simply because [it] amounted to 'use' of Plaintiff's computer." (Id. at p. *13.) But as just explained, we do not read eBay, supra, 100 F.Supp.2d 1058, as holding that the actual injury requirement may be dispensed with, and such a suggestion would, in any event, be erroneous as a statement of California law.
been questioned.6 "[T]he court broke the chain between the trespass and the harm, allowing indirect harms to CompuServe's business interests—reputation, customer goodwill, and employee time—to count as harms to the chattel (the server)." (Quilter, The Continuing Expansion of Cyberspace Trespass to Chattels, supra, 17 Berkeley Tech. L.J. at pp. 429-430.) "[T]his move cuts trespass to chattels free from its moorings of dispossession or the equivalent, allowing the court free reign [sic] to hunt for 'impairment.'" (Burk, The Trouble with Trespass (2000) 4 J. Small & Emerging Bus.L. 27, 35.) But even if the loss of goodwill identified in CompuServe were the type of injury that would give rise to a trespass to chattels claim under California law, Intel's position would not follow, for Intel's claimed injury has even less connection to its personal property than did CompuServe's.

CompuServe's customers were annoyed because the system was inundated with unsolicited commercial messages, making its use for personal communication more difficult and costly. (CompuServe, supra, 962 F.Supp. at p. 1023.) Their complaint, which allegedly led some to cancel their CompuServe service, was about the functioning of CompuServe's electronic mail service. Intel's workers, in contrast, were allegedly distracted from their work not because of the frequency or quantity of Hamidi's messages, but because of assertions and opinions the

---

6 In support of its reasoning, the CompuServe court cited paragraph (d) of section 218 of the Restatement Second of Torts, which refers to harm "to some person or thing in which the possessor has a legally protected interest." As the comment to this paragraph explains, however, it is intended to cover personal injury to the possessor or another person in whom the possessor has a legal interest, or injury to "other chattel or land" in which the possessor of the chattel subject to the trespass has a legal interest. (Rest.2d Torts, § 218, com. j, p. 423.) No personal injury was claimed either in CompuServe or in the case at bar, and neither the lost goodwill in CompuServe nor the loss of employee efficiency claimed in the present case is chattel or land.
messages conveyed. Intel’s complaint is thus about the contents of the messages rather than the functioning of the company’s e-mail system. Even accepting CompuServe’s economic injury rationale, therefore, Intel’s position represents a further extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication’s contents on recipients as an impairment to the device which transmitted the message.

This theory of “impairment by content” (Burk, The Trouble with Trespass, supra, 4 J. Small & Emerging Bus.L. at p. 37) threatens to stretch trespass law to cover injuries far afield from the harms to possession the tort evolved to protect. Intel’s theory would expand the tort of trespass to chattels to cover virtually any unconsented-to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter. As the dissenting justice below explained, “‘Damage’ of this nature—the distraction of reading or listening to an unsolicited communication—is not within the scope of the injury against which the trespass-to-chattel tort protects, and indeed trivializes it. After all, ‘[t]he property interest protected by the old action of trespass was that of possession; and this has continued to affect the character of the action.’ (Prosser & Keeton on Torts, supra, § 14, p. 87.) Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment. [¶] Indeed, if a chattel’s receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program.” We agree. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort
law; in order to address them, we need not create a fiction of injury to the communication system.

Nor may Intel appropriately assert a property interest in its employees' time. "The Restatement test clearly speaks in the first instance to the impairment of the chattel. . . . But employees are not chattels (at least not in the legal sense of the term)." (Burk, The Trouble with Trespass, supra, 4 J. Small & Emerging Bus.L. at p. 36.) Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort."

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose—to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented
undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be extended to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi’s messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes—here, Intel—for any consequential injury flowing from the contents of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, “extending the rules of trespass to real property to all interactive Web sites and servers.” The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company’s server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.
Epstein’s argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: “cyberspace,” “the information superhighway,” e-mail “addresses,” and the like. Of course, the Internet is also frequently called simply the “Net,” a term, Hamidi points out, “evoking a fisherman’s chattel.” A major component of the Internet is the World Wide “Web,” a descriptive term suggesting neither personal nor real property, and “cyberspace” itself has come to be known by the oxymoronic phrase “virtual reality,” which would suggest that any real property “located” in “cyberspace” must be “virtually real” property. Metaphor is a two-edged sword.

Indeed, the metaphorical application of real property rules would not, by itself, transform a physically harmless electronic intrusion on a computer server into a trespass. That is because, under California law, intangible intrusions on land, including electromagnetic transmissions, are not actionable as trespasses (though they may be as nuisances) unless they cause physical damage to the real property. (San Diego Gas & Electric Co. v. Superior Court (1996) 13 Cal.4th 893, 936-937.) Since Intel does not claim Hamidi’s electronically transmitted messages physically damaged its servers, it could not prove a trespass to land even were we to treat the computers as a type of real property. Some further extension of the conceit would be required, under which the electronic signals Hamidi sent would be recast as tangible intruders, perhaps as tiny messengers rushing through the “hallways” of Intel’s computers and bursting out of employees’ computers to read them Hamidi’s missives. But such fictions promise more confusion than clarity in the law. (See eBay, supra, 100 F.Supp.2d at pp. 1065-1066 [rejecting eBay’s argument that the defendant’s automated data searches “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”].)
The plain fact is that computers, even those making up the Internet, are—like such older communications equipment as telephones and fax machines—personal property, not realty. Professor Epstein observes that “[a]lthough servers may be moved in real space, they cannot be moved in cyberspace,” because an Internet server must, to be useful, be accessible at a known address. But the same is true of the telephone: to be useful for incoming communication, the telephone must remain constantly linked to the same number (or, when the number is changed, the system must include some forwarding or notification capability, a qualification that also applies to computer addresses). Does this suggest that an unwelcome message delivered through a telephone or fax machine should be viewed as a trespass to a type of real property? We think not: As already discussed, the contents of a telephone communication may cause a variety of injuries and may be the basis for a variety of tort actions (e.g., defamation, intentional infliction of emotional distress, invasion of privacy), but the injuries are not to an interest in property, much less real property, and the appropriate tort is not trespass.7

7 The tort law discussion in Justice Brown’s dissenting opinion similarly suffers from an overreliance on metaphor and analogy. Attempting to find an actionable trespass, Justice Brown analyzes Intel’s e-mail system as comparable to the exterior of an automobile (dis. opn. of Brown, J., post, at p. 1), a plot of land (id., at pp. 14–15), the interior of an automobile (p. 18), a toothbrush (pp. 22-23), a head of livestock (p. 23), and a mooring buoy (pp. 24-25), while Hamidi is characterized as a vandal damaging a school building (p. 21) or a prankster unplugging and moving employees’ computers (p. 23). These colorful analogies tend to obscure the plain fact that this case involves communications equipment, used by defendant to communicate. Intel’s e-mail system was equipment designed for speedy communication between employees and the outside world; Hamidi communicated with Intel employees over that system in a manner entirely consistent with its design; and Intel objected not because of an offense against the integrity or dignity of its computers, but because the communications themselves.

(Footnote continued on next page.)
More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create “the right social result.” In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, Web site searching, and page linking because they benefit by that open access. When a Web site owner does deny access to a particular sending, searching, or linking computer, a system of “simple one-on-one negotiations” will arise to provide the necessary individual licenses.

Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, “each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel.” The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. As Professor Dan Hunter of the University of Pennsylvania asks rhetorically: “Does this mean that

(Footnote continued from previous page.)

affected employee-recipient in a manner Intel found undesirable. The proposal that we extend trespass to chattels to cover any communication that the owner of the communications equipment considers annoying or distracting raises, moreover, concerns about control over the flow of information and views that would not be presented by, for example, an injunction against chasing another’s cattle or sleeping in her car.
one must read the ‘Terms of Acceptable Email Usage’ of every email system that one emails in the course of an ordinary day? If the University of Pennsylvania had a policy that sending a joke by email would be an unauthorized use of their system, then under the logic of [the lower court decision in this case], you commit ‘trespass’ if you emailed me a . . . cartoon.” (Hunter, Cyberspace as Place, and the Tragedy of the Digital Anticommons (2003) 91 Cal. L.Rev. 439, 508-509.)

Web site linking, Professor Lemley further observes, “would exist at the sufferance of the linked-to party, because a Web user who followed a ‘disapproved’ link would be trespassing on the plaintiff’s server, just as sending an e-mail is trespass under the [lower] court’s theory.” Another writer warns that “[c]yber-trespass theory will curtail the free flow of price and product information on the Internet by allowing website owners to tightly control who and what may enter and make use of the information housed on its Internet site.” (Chang, Bidding on Trespass: eBay, Inc. v. Bidder’s Edge, Inc. and the Abuse of Trespass Theory in Cyberspace Law (2001) 29 AIPLA Q.J. 445, 459.) A leading scholar of Internet law and policy, Professor Lawrence Lessig of Stanford University, has criticized Professor Epstein’s theory of the computer server as quasi-real property, previously put forward in the eBay case (eBay, supra, 100 F.Supp.2d 1058), on the ground that it ignores the costs to society in the loss of network benefits: “eBay benefits greatly from a network that is open and where access is free. It is this general feature of the Net that makes the Net so valuable to users and a source of great innovation. And to the extent that individual sites begin to impose their own rules of exclusion, the value of the network as a network declines. If machines must negotiate before entering any individual site, then the costs of using the network climb.” (Lessig, The Future of Ideas: The Fate of the Commons in a Connected World (2001) p. 171; see also Hunter, Cyberspace as Place, and the Tragedy of the Digital Anticommons, supra, 91 Cal. L.Rev. at p. 512 [“If we
continue to mark out anticommmons claims in cyberspace, not only will we
preclude better, more innovative uses of cyberspace resources, but we will lose
sight of what might be possible”].

We discuss this debate among the amici curiae and academic writers only
to note its existence and contours, not to attempt its resolution. Creating an
absolute property right to exclude undesired communications from one’s e-mail
and Web servers might help force spammers to internalize the costs they impose
on ISP’s and their customers. But such a property rule might also create
substantial new costs, to e-mail and e-commerce users and to society generally, in
lost ease and openness of communication and in lost network benefits. In light of
the unresolved controversy, we would be acting rashly to adopt a rule treating
computer servers as real property for purposes of trespass law.

The Legislature has already adopted detailed regulations governing UCE.
(Bus. & Prof. Code, §§ 17538.4, 17538.45; see generally Ferguson v.
Friendfinders, Inc., supra, 94 Cal.App.4th 1255.) It may see fit in the future also
to regulate noncommercial e-mail, such as that sent by Hamidi, or other kinds of
unwanted contact between computers on the Internet, such as that alleged in eBay,
supra, 100 F.Supp.2d 1058. But we are not persuaded that these perceived
problems call at present for judicial creation of a rigid property rule of computer
server inviolability. We therefore decline to create an exception, covering
Hamidi’s unwanted electronic messages to Intel employees, to the general rule that
a trespass to chattels is not actionable if it does not involve actual or threatened
injury to the personal property or to the possessor’s legally protected interest in the
personal property. No such injury having been shown on the undisputed facts,
Intel was not entitled to summary judgment in its favor.
III. Constitutional Considerations

Because we conclude no trespass to chattels was shown on the summary judgment record, making the injunction improper on common law grounds, we need not address at length the dissenters’ constitutional arguments. A few clarifications are nonetheless in order.

Justice Mosk asserts that this case involves only “a private entity seeking to enforce private trespass rights.” (Dis. opn. of Mosk, J., post, at p. 14.) But the injunction here was issued by a state court. While a private refusal to transmit another’s electronic speech generally does not implicate the First Amendment, because no governmental action is involved (see Cyber Promotions, Inc. v. America Online, Inc. (E.D.Penn. 1996) 948 F.Supp. 436, 441-445 [spammer could not force private ISP to carry its messages]), the use of government power, whether in enforcement of a statute or ordinance or by an award of damages or an injunction in a private lawsuit, is state action that must comply with First Amendment limits. (Cohen v. Cowles Media Co. (1991) 501 U.S. 663, 668; NAACP v. Claiborne Hardware Co. (1982) 458 U.S. 886, 916, fn. 51; New York Times v. Sullivan (1964) 376 U.S. 254, 265.) Nor does the nonexistence of a “constitutional right to trespass” (dis. opn. of Mosk, J., post, at p. 14) make an injunction in this case per se valid. Unlike, for example, the trespasser-to-land defendant in Church of Christ in Hollywood v. Superior Court (2002) 99 Cal.App.4th 1244, Hamidi himself had no tangible presence on Intel property, instead speaking from his own home through his computer. He no more invaded Intel’s property than does a protester holding a sign or shouting through a bullhorn outside corporate headquarters, posting a letter through the mail, or telephoning to complain of a corporate practice. (See Madsen v. Women’s Health Center (1994)
512 U.S. 753, 765 [injunctions restraining such speakers must "burden no more speech than necessary to serve a significant government interest"].)

Justice Brown relies upon a constitutional "right not to listen," rooted in the listener's "personal autonomy" (dis. opn. of Brown, J., post, at p. 11), as compelling a remedy against Hamidi's messages, which she asserts were sent to "unwilling" listeners (id., at p. 4). Even assuming a corporate entity could under some circumstances claim such a personal right, here the intended and actual recipients of Hamidi's messages were individual Intel employees, rather than Intel itself. The record contains no evidence Hamidi sent messages to any employee who notified him such messages were unwelcome. In any event, such evidence would, under the dissent's rationale of a right not to listen, support only a narrow injunction aimed at protecting individual recipients who gave notice of their rejection. (See Bolger v. Youngs Drug Products Corp. (1983) 463 U.S. 60, 72 [government may not act on behalf of all addressees by generally prohibiting mailing of materials related to contraception, where those recipients who may be offended can simply ignore and discard the materials]; Martin v. City of Struthers (1943) 319 U.S. 141, 144 [anti-canvassing ordinance improperly "substitutes the judgment of the community for the judgment of the individual householder"]; cf. Rowan v. U.S. Post Office Dept. (1970) 397 U.S. 728, 736 ["householder" may

---

8 Justice Brown would distinguish Madsen v. Women's Health Cente, supra, on the ground that the operators of the health center in that case would not have been entitled to "drive[] [the protesters] from the public streets," whereas Intel was entitled to block Hamidi's messages as best it could. (Dis. opn. of Brown, J., post, at p. 6, fn. 1.) But the health center operators were entitled to block protesters' messages—as best they could—by closing windows and pulling blinds. That a property owner may take physical measures to prevent the transmission of others' speech into or across the property does not imply that a court order enjoining the speech is not subject to constitutional limitations.
exercise "individual autonomy" by refusing delivery of offensive mail.

The principal of a right not to listen, founded in personal autonomy, cannot justify the sweeping injunction issued here against all communication to Intel addresses, for such a right, logically, can be exercised only by, or at the behest of, the recipient himself or herself.

**DISPOSITION**

The judgment of the Court of Appeal is reversed.

WERDEGAR, J.

WE CONCUR:

KENNARD, J.
MORENO, J.
PERREN, J.*

* Associate Justice of the Court of Appeal, Second Appellate District, Division Six, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

Kennard concurrence & Brown dissent omitted
DISSENTING OPINION BY MOSK, J.

The majority hold that the California tort of trespass to chattels does not encompass the use of expressly unwanted electronic mail that causes no physical damage or impairment to the recipient’s computer system. They also conclude that because a computer system is not like real property, the rules of trespass to real property are also inapplicable to the circumstances in this case. Finally, they suggest that an injunction to preclude mass, noncommercial, unwelcome e-mails may offend the interests of free communication.

I respectfully disagree and would affirm the trial court’s decision. In my view, the repeated transmission of bulk e-mails by appellant Kourosh Kenneth Hamidi (Hamidi) to the employees of Intel Corporation (Intel) on its proprietary confidential e-mail lists, despite Intel’s demand that he cease such activities, constituted an actionable trespass to chattels. The majority fail to distinguish open communication in the public “commons” of the Internet from unauthorized intermeddling on a private, proprietary intranet. Hamidi is not communicating in the equivalent of a town square or of an unsolicited “junk” mailing through the United States Postal Service. His action, in crossing from the public Internet into a private intranet, is more like intruding into a private office mailroom, commandeering the mail cart, and dropping off unwanted broadsides on 30,000 desks. Because Intel’s security measures have been circumvented by Hamidi, the majority leave Intel, which has exercised all reasonable self-help efforts, with no recourse unless he causes a malfunction or systems “crash.” Hamidi’s repeated intrusions did more than merely “prompt[] discussions between ‘[e]xcited and
nervous managers’ and the company’s human resource department” (maj. opn., ante, at p. 6); they also constituted a misappropriation of Intel’s private computer system contrary to its intended use and against Intel’s wishes.

The law of trespass to chattels has not universally been limited to physical damage. I believe it is entirely consistent to apply that legal theory to these circumstances — that is, when a proprietary computer system is being used contrary to its owner’s purposes and expressed desires, and self-help has been ineffective. Intel correctly expects protection from an intruder who misuses its proprietary system, its nonpublic directories, and its supposedly controlled connection to the Internet to achieve his bulk mailing objectives — incidentally, without even having to pay postage.

I

Intel maintains an intranet — a proprietary computer network — as a tool for transacting and managing its business, both internally and for external business communications.¹ The network and its servers constitute a tangible entity that has value in terms of the costs of its components and its function in enabling and enhancing the productivity and efficiency of Intel’s business operations. Intel has

¹ The Oxford English Dictionary defines an intranet as “A local or restricted computer network; spec. a private or corporate network that uses Internet protocols. An intranet may (but need not) be connected to the Internet and be accessible externally to authorized users.” (OED Online, new ed., draft entry, Mar. 2003, <http://dictionary.oed.com/>) [as of June 30, 2003]; see also Kokka, Property Rights on an Intranet, 3-Spring 1998 J. Tech.L. & Policy 3, WL 3 UFLJITLP 3 at *3, *6 [defining an intranet as “an internal network of computers, servers, routers and browser software designed to organize, secure, distribute and collect information within an organization” which in large organizations generally includes a wide range of services, including e-mail].) Contrary to the majority’s assertion, there is nothing incorrect about characterizing Hamidi’s unauthorized bulk e-mails as intrusions onto Intel’s intranet.
established costly security measures to protect the integrity of its system, including policies about use, proprietary internal e-mail addresses that it does not release to the public for use outside of company business, and a gateway for blocking unwanted electronic mail — a so-called firewall.

The Intel computer usage guidelines, which are promulgated for its employees, state that the computer system is to be “used as a resource in conducting business. Reasonable personal use is permitted, but employees are reminded that these resources are the property of Intel and all information on these resources is also the property of Intel.” Examples of personal use that would not be considered reasonable expressly include “use that adversely affects productivity.” Employee e-mail communications are neither private nor confidential.

Hamidi, a former Intel employee who had sued Intel and created an organization to disseminate negative information about its employment practices, sent bulk electronic mail on six occasions to as many as 35,000 Intel employees on its proprietary computer system, using Intel’s confidential employee e-mail lists and adopting a series of different origination addresses and encoding strategies to elude Intel’s blocking efforts. He refused to stop when requested by Intel to do so, asserting that he would ignore its demands: “I don’t care. I have grown deaf.” Intel sought injunctive relief, alleging that the disruptive effect of the bulk electronic mail, including expenses from administrative and management personnel, damaged its interest in the proprietary nature of its network.

The trial court, in its order granting summary judgment and a permanent injunction, made the following pertinent findings regarding Hamidi’s transmission of bulk electronic mail: “Intel has requested that Hamidi stop sending the messages, but Hamidi has refused, and has employed surreptitious means to circumvent Intel’s efforts to block entry of his messages into Intel’s system. . . .
The e-mail system is dedicated for use in conducting business, including communications between Intel employees and its customers and vendors. Employee e-mail addresses are not published for use outside company business. The intrusion by Hamidi into the Intel e-mail system has resulted in the expenditure of company resources to seek to block his mailings and to address employee concerns about the mailings. Given Hamidi’s evasive techniques to avoid blocking, the self help remedy available to Intel is ineffective.” The trial court concluded that “the evidence establishes (without dispute) that Intel has been injured by diminished employee productivity and in devoting company resources to blocking efforts and to addressing employees about Hamidi’s e-mails.” The trial court further found that the “massive” intrusions “impaired the value to Intel of its e-mail system.”

The majority agree that an impairment of Intel’s system would result in an action for trespass to chattels, but find that Intel suffered no injury. As did the trial court, I conclude that the undisputed evidence establishes that Intel was substantially harmed by the costs of efforts to block the messages and diminished employee productivity. Additionally, the injunction did not affect Hamidi’s ability to communicate with Intel employees by other means; he apparently continues to maintain a Web site to publicize his messages concerning the company. Furthermore, I believe that the trial court and the Court of Appeal correctly determined that the tort of trespass to chattels applies in these circumstances.

The Restatement Second of Torts explains that a trespass to a chattel occurs if “the chattel is impaired as to its condition, quality, or value” or if “harm is caused to some . . . thing in which the possessor has a legally protected interest.” (Rest.2d Torts, § 218, subds. (b) & (d), p. 420, italics added.) As to this tort, a current prominent treatise on the law of torts explains that “[t]he defendant may interfere with the chattel by interfering with the plaintiff’s access or use” and
observes that the tort has been applied so as “to protect computer systems from
electronic invasions by way of unsolicited email or the like.” (1 Dobbs, The Law
of Torts (2001) § 60, pp. 122-123.) Moreover, “[t]he harm necessary to trigger
liability for trespass to chattels can be . . . harm to something other than the chattel
itself.” (Id. at pp. 124-125; see also 1 Harper et al., The Law of Torts (3d ed. 1996
& 2003 supp.) § 2.3, pp. 2:14-2:18.) The Restatement points out that, unlike a
 possessor of land, a possessor of a chattel is not given legal protection from
harmless invasion, but “the actor” may be liable if the conduct affects “some other
and more important interest of the possessor.” (Rest.2d Torts, § 218, com. (e),
p. 421, italics added.)

The Restatement explains that the rationale for requiring harm for trespass
to a chattel but not for trespass to land is the availability and effectiveness of self-
help in the case of trespass to a chattel. “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.” (Rest.2d Torts, § 218, com. (e), p. 422.) Obviously, “force” is not
available to prevent electronic trespasses. As shown by Intel’s inability to prevent
Hamidi’s intrusions, self-help is not an adequate alternative to injunctive relief.

The common law tort of trespass to chattels does not require physical
disruption to the chattel. It also may apply when there is impairment to the
“quality” or “value” of the chattel. (Rest.2d Torts, § 218, subd. (b), p. 420; see
also id., com. (e), pp. 421-422 [liability if “intermeddling is harmful to the
possessor’s materially valuable interest in the physical condition, quality, or value
of the chattel”].) Moreover, as we held in Zaslow v. Kroenert (1946) 29 Cal.2d
541, 551, it also applies “[w]here the conduct complained of does not amount to a
substantial interference with possession or the right thereto, but consists of intermeddlig with or use of or damages to the personal property."²

Here, Hamidi's deliberate and continued intermeddling, and threatened intermeddling, with Intel's proprietary computer system for his own purposes that were hostile to Intel, certainly impaired the quality and value of the system as an internal business device for Intel and forced Intel to incur costs to try to maintain the security and integrity of its server — efforts that proved ineffective. These included costs incurred to mitigate injuries that had already occurred. It is not a matter of "bootstrap[ing]" (maj. opn., ante, at p. 20) to consider those costs a damage to Intel. Indeed, part of the value of the proprietary computer system is the ability to exclude intermeddlers from entering it for significant uses that are disruptive to its owner's business operations.

If Intel, a large business with thousands of former employees, is unable to prevent Hamidi from continued intermeddling, it is not unlikely that other outsiders who obtain access to its proprietary electronic mail addresses would engage in similar conduct, further reducing the value of, and perhaps debilitating, the computer system as a business productivity mechanism. Employees understand that a firewall is in place and expect that the messages they receive are from senders permitted by the corporation. Violation of this expectation increases the internal disruption caused by messages that circumvent the company's attempt to exclude them. The time that each employee must spend to evaluate, delete or

² In Zaslow, we observed that when the trespass involves "intermeddling with or use of" another's property, the owner "may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." (Zaslow v. Kroenert, supra, 29 Cal.2d at p. 551.) We did not state that such damages were a requirement for a cause of action; nor did we address the availability of injunctive relief.
respond to the message, when added up, constitutes an amount of compensated
time that translates to quantifiable financial damage.\textsuperscript{3}

All of these costs to protect the integrity of the computer system and to deal
with the disruptive effects of the transmissions and the expenditures attributable to
employee time, constitute damages sufficient to establish the existence of a
trespass to chattels, even if the computer system was not overburdened to the point
of a “crash” by the bulk electronic mail.

The several courts that have applied the tort of trespass to chattels to
deliberate intermeddling with proprietary computer systems have, for the most
part, used a similar analysis. Thus, the court in \textit{CompuServe Inc. v. Cyber
Promotions, Inc.} (S.D. Ohio 1997) 962 F.Supp. 1015, 1022, applied the
Restatement to conclude that mass mailings and evasion of the server’s filters

\textsuperscript{3} As the recent spate of articles on “spam” — unsolicited bulk e-mail —
suggests, the effects on business of such unwanted intrusions are not trivial.
“Spam is not just a nuisance. It absorbs bandwidth and overwhelsms Internet
service providers. Corporate tech staffs labor to deploy filtering technology to
protect their networks. The cost is now widely estimated (though all such
estimates are largely guesswork) at billions of dollars a year. The social costs are
immeasurable. . . . [4] ‘Spam has become the organized crime of the Internet.’ . . .
‘[M]ore and more it’s becoming a systems and engineering and networking
problem.’ ” (Gleick, \textit{Tangled Up in Spam}, N.Y. Times (Feb. 9, 2003) magazine
p. 1 \langlehttp://www.nytimes.com/2003/02/09/> [as of June 30, 2003]; see also
Cooper & Shogren, \textit{U.S. States Turn Focus to Curbing Spam}, L.A. Times (May 1,
2003) p. A21, col. 2 (“Businesses are losing money with every moment that
employees spend deleting”); Turley, \textit{Congress Must Send Spammers a Message},
about $9 billion a year in lost productivity and screening”); Taylor, \textit{Spam’s Big
Bang!} (June 16, 2003) Time magazine, at p. 51 (“The time we spend deleting or
defeating spam costs an estimated $8.9 billion a year in lost productivity”].) But
the occasional spam addressed to particular employees does not pose nearly the
same threat of impaired value as the concerted bulk mailings into one e-mail
system at issue here, which mailings were sent to thousands of employees with the
express purpose of disrupting business as usual.
diminished the value of the mail processing computer equipment to CompuServe “even though it is not physically damaged by defendant’s conduct.” The inconvenience to users of the system as a result of the mass messages “decrease[d] the utility of CompuServe’s e-mail service” and was actionable as a trespass to chattels. (Id. at p. 1023.)

The court in *America Online, Inc. v. IMS* (E.D.Va. 1998) 24 F.Supp.2d 548, on facts similar to those in the present case, also applied the Restatement in a trespass to chattels claim. There, defendant sent unauthorized e-mails to America Online’s computer system, persisting after receiving notice to desist and causing the company “to spend technical resources and staff time to ‘defend’ its computer system and its membership” against the unwanted messages. (Id. at p. 549.) The company was not required to show that its computer system was overwhelmed or suffered a diminution in performance; mere use of the system by the defendant was sufficient to allow the plaintiff to prevail on the trespass to chattels claim.

Similarly, the court in *eBay, Inc. v. Bidder’s Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058 determined that there was a trespass to chattels when the quality or value of a computer system was diminished by unauthorized “web crawlers,” despite the fact that eBay had not alleged any “particular service disruption” (id. at p. 1065) or “specific incremental damages” (id. at p. 1063) to the computer system. Intermeddling with eBay’s private property was sufficient to establish a cause of action: “A trespasser is liable when the trespass diminishes the condition, quality or value of personal property”; “[e]ven if [defendant’s intrusions] use only a small amount of eBay’s computer . . . capacity, [defendant]

---

4 A “web crawler” is a computer program that operates across the Internet to obtain information from the websites of others. (*eBay, Inc. v. Bidder’s Edge, supra*, 100 F.Supp.2d at p. 1061, fn. 2.)
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.” (Id. at p. 1071; see also, e.g., *Oyster Software, Inc. v. Forms Processing, Inc.* (N.D.Cal. Dec. 6, 2001, No. C-00-0724 JCS) 2001 WL 1736382 at *12-*13 [trespass to chattels claim did not require company to demonstrate physical damage]; *Register.com, Inc. v. Verio, Inc.* (S.D.N.Y. 2000) 126 F.Supp.2d 238, 250 [accord]; cf. *Thrifty-Tel, Inc. v. Bezenek* (1996) 46 Cal.App.4th 1559, 1566-1567 [unconsented electronic access to a computer system constituted a trespass to chattels].)

These cases stand for the simple proposition that owners of computer systems, like owners of other private property, have a right to prevent others from using their property against their interests. That principle applies equally in this case. By his repeated intermeddling, Hamidi converted Intel’s private employee e-mail system into a tool for harming productivity and disrupting Intel’s workplace. Intel attempted to put a stop to Hamidi’s intrusions by increasing its electronic screening measures and by requesting that he desist. Only when self-help proved futile, devolving into a potentially endless joust between attempted prevention and circumvention, did Intel request and obtain equitable relief in the form of an injunction to prevent further threatened injury.

The majority suggest that Intel is not entitled to injunctive relief because it chose to allow its employees access to e-mail through the Internet and because Hamidi has apparently told employees that he will remove them from his mailing list if they so request. They overlook the proprietary nature of Intel’s intranet system; Intel’s system is not merely a conduit for messages to its employees. As the owner of the computer system, it is Intel’s request that Hamidi stop that must be respected. The fact that, like most large businesses, Intel’s intranet includes external e-mail access for essential business purposes does not logically mean, as
the majority suggest, that Intel has forfeited the right to determine who has access to its system. Its intranet is not the equivalent of a common carrier or public communications licensee that would be subject to requirements to provide service and access. Just as Intel can, and does, regulate the use of its computer system by its employees, it should be entitled to control its use by outsiders and to seek injunctive relief when self-help fails.

The majority also propose that Intel has sufficient avenues for legal relief outside of trespass to chattels, such as interference with prospective economic relations, interference with contract, intentional infliction of emotional distress, and defamation; Hamidi urges that an action for nuisance is more appropriate. Although other causes of action may under certain circumstances also apply to Hamidi’s conduct, the remedy based on trespass to chattels is the most efficient and appropriate. It simply requires Hamidi to stop the unauthorized use of property without regard to the content of the transmissions. Unlike trespass to chattels, the other potential causes of action suggested by the majority and Hamidi would require an evaluation of the transmissions’ content and, in the case of a nuisance action, for example, would involve questions of degree and value judgments based on competing interests. (See Hellman v. La Cumbre Golf & Country Club (1992) 6 Cal.App.4th 1224, 1230-1231; 11 Witkin, Summary of Cal. Law (9th ed. 1990) Equity, § 153, p. 833; Rest.2d Torts, § 840D).

II

As discussed above, I believe that existing legal principles are adequate to support Intel’s request for injunctive relief. But even if the injunction in this case amounts to an extension of the traditional tort of trespass to chattels, this is one of those cases in which, as Justice Cardozo suggested, “[t]he creative element in the
judicial process finds its opportunity and power” in the development of the law. (Cardozo, Nature of the Judicial Process (1921) p. 165.)

The law has evolved to meet economic, social, and scientific changes in society. The industrial revolution, mass production, and new transportation and communication systems all required the adaptation and evolution of legal doctrines.

The age of computer technology and cyberspace poses new challenges to legal principles. As this court has said, “the so-called Internet revolution has spawned a host of new legal issues as courts have struggled to apply traditional legal frameworks to this new communication medium.” (Pavlovich v. Superior Court (2002) 29 Cal.4th 262, 266.) The court must now grapple with proprietary interests, privacy, and expression arising out of computer-related disputes. Thus, in this case the court is faced with “that balancing of judgment, that testing and sorting of considerations of analogy and logic and utility and fairness” that Justice Cardozo said he had “been trying to describe.” (Cardozo, Nature of the Judicial Process, supra, at pp. 165-166.) Additionally, this is a case in which equitable relief is sought. As Bernard Witkin has written, “equitable relief is flexible and expanding, and the theory that ‘for every wrong there is a remedy’ [Civ. Code, § 3523] may be invoked by equity courts to justify the invention of new methods of relief for new types of wrongs.” (11 Witkin, Summary of Cal. Law, supra, Equity, § 3, p. 681.) That the Legislature has dealt with some aspects of commercial unsolicited bulk e-mail (Bus. & Prof. Code, §§ 17538.4, 17538.45; see maj. opn., ante, at p. 25) should not inhibit the application of common law tort

\[5\] “It is revolting to have no better reason for a rule of law than that so it was laid down in the time of Henry IV.” (Holmes, The Path of the Law (1897) 10 Harv.L.Rev. 457, 469.)

Before the computer, a person could not easily cause significant disruption to another’s business or personal affairs through methods of communication without significant cost. With the computer, by a mass mailing, one person can at no cost disrupt, damage, and interfere with another’s property, business, and personal interests. Here, the law should allow Intel to protect its computer-related property from the unauthorized, harmful, free use by intruders.

III

As the Court of Appeal observed, connecting one’s driveway to the general system of roads does not invite demonstrators to use the property as a public forum. Not mindful of this precept, the majority blur the distinction between public and private computer networks in the interest of “ease and openness of communication.” (Maj. opn., ante, at p. 26.) By upholding Intel’s right to exercise self-help to restrict Hamidi’s bulk e-mails, they concede that he did not have a right to send them through Intel’s proprietary system. Yet they conclude that injunctive relief is unavailable to Intel because it connected its e-mail system to the Internet and thus, “necessarily contemplated” unsolicited communications to its employees. (Maj. opn., ante, at p. 20.) Their exposition promotes unpredictability in a manner that could be as harmful to open communication as it is to property rights. It permits Intel to block Hamidi’s e-mails entirely, but offers no recourse if he succeeds in breaking through its security barriers, unless he physically or functionally degrades the system.

By making more concrete damages a requirement for a remedy, the majority has rendered speech interests dependent on the impact of the e-mails.
The sender will never know when or if the mass e-mails sent by him (and perhaps others) will use up too much space or cause a crash in the recipient system, so as to fulfill the majority's requirement of damages. Thus, the sender is exposed to the risk of liability because of the possibility of damages. If, as the majority suggest, such a risk will deter "ease and openness of communication" (maj. opn., ante, at p. 26), the majority's formulation does not eliminate such deterrence. Under the majority's position, the lost freedom of communication still exists. In addition, a business could never reliably invest in a private network that can only be kept private by constant vigilance and inventiveness, or by simply shutting off the Internet, thus limiting rather than expanding the flow of information. Moreover, Intel would have less incentive to allow employees reasonable use of its equipment to send and receive personal e-mails if such allowance is justification for preventing restrictions on unwanted intrusions into its computer system. I believe the best approach is to clearly delineate private from public networks and identify as a trespass to chattels the kind of intermeddling involved here.

The views of the amici curiae group of intellectual property professors that a ruling in favor of Intel will interfere with communication are similarly misplaced because here, Intel, contrary to most users, expressly informed appellant that it did not want him sending messages through its system. Moreover, as noted above, all of the problems referred to will exist under the apparently accepted law that there is a cause of action if there is some actionable damage.

---

6 Thus, the majority's approach creates the perverse incentive for companies to invest less in computer capacity in order to protect its property. In the view of the majority, Hamidi's massive e-mails would be actionable only if Intel had insufficient server or storage capacity to manage them.
Hamidi and other amici curiae raise, for the first time on appeal, certain labor law issues, including the matter of protected labor-related communications. Even assuming that these issues are properly before this court (see Cal. Rules of Court, rule 28(c)(1)), to the extent the laws allow what would otherwise be trespasses for some labor-related communications, my position does not exclude that here too. But there has been no showing that the communications are labor law protected.7

Finally, with regard to alleged constitutional free speech concerns raised by Hamidi and others, this case involves a private entity seeking to enforce private rights against trespass. Unlike the majority, I have concluded that Hamidi did invade Intel’s property. His actions constituted a trespass — in this case a trespass to chattels. There is no federal or state constitutional right to trespass. (Adderley v. Florida (1966) 385 U.S. 39, 47 [“Nothing in the Constitution of the United States prevents Florida from even-handed enforcement of its general trespass statute. . . .”]; Church of Christ in Hollywood v. Superior Court (2002) 99 Cal.App.4th 1244, 1253-1254 [affirming a restraining order preventing former church member from entering church property: “[the United States Supreme Court] has never held that a trespasser or an uninvited guest may exercise general rights of free speech on property privately owned”]; see also CompuServe Inc. v. Cyber Promotions, Inc., supra, 962 F.Supp. at p. 1026 [“the mere judicial enforcement of neutral trespass laws by the private owner of property does not alone render it a state actor”]; Cyber Promotions, Inc. v. America Online, Inc.

7 The bulk e-mail messages from Hamidi, a nonemployee, did not purport to spur employees into any collective action; he has conceded that “[t]his is not a drive to unionize.” Nor was his disruptive conduct part of any bona fide labor dispute.
(E.D.Pa. 1996) 948 F.Supp. 436, 456 ["a private company such as Cyber simply does not have the unfettered right under the First Amendment to invade AOL’s private property . . . "].) Accordingly, the cases cited by the majority regarding restrictions on speech, not trespass, are not applicable. Nor does the connection of Intel’s e-mail system to the Internet transform it into a public forum any more than any connection between private and public properties. Moreover, as noted above, Hamidi had adequate alternative means for communicating with Intel employees so that an injunction would not, under any theory, constitute a free speech violation. (Lloyd Corp. v. Tanner (1972) 407 U.S. 551, 568-569.)

IV

The trial court granted an injunction to prevent threatened injury to Intel. That is the purpose of an injunction. (Ernst & Ernst v. Carlson (1966) 247 Cal.App.2d 125, 128.) Intel should not be helpless in the face of repeated and threatened abuse and contamination of its private computer system. The undisputed facts, in my view, rendered Hamidi’s conduct legally actionable. Thus, the trial court’s decision to grant a permanent injunction was not “a clear abuse of discretion” that may be “disturbed on appeal.” (Shapiro v. San Diego City Council (2002) 96 Cal.App.4th 904, 912; see also City of Vernon v. Central Basin Mun. Water Dist. (1999) 69 Cal.App.4th 508, 516 [in an appeal of summary judgment, the trial court’s decision to deny a permanent injunction was “governed by the abuse of discretion standard of review”].)

The injunction issued by the trial court simply required Hamidi to refrain from further trespassory conduct, drawing no distinction based on the content of his e-mails. Hamidi remains free to communicate with Intel employees and others outside the walls — both physical and electronic — of the company.
For these reasons, I respectfully dissent.

MOSK, J.*

I CONCUR:

GEORGE, C.J.

* Associate Justice, Court of Appeal, Second Appellate District, Division Five, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.
Copyright Basics

What Is Copyright?

Copyright is a form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of “original works of authorship,” including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:

- To reproduce the work in copies or phonorecords;
- To prepare derivative works based upon the work;
- To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- To perform the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works;
- To display the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work; and
- In the case of sound recordings, to perform the work publicly by means of a digital audio transmission.

In addition, certain authors of works of visual art have the rights of attribution and integrity as described in section 106A of the 1976 Copyright Act. For further information, request Circular 40, Copyright Registration for Works of the Visual Arts.

It is illegal for anyone to violate any of the rights provided by the copyright law to the owner of copyright. These rights, however, are not unlimited in scope. Sections 107 through 121 of the 1976 Copyright Act establish limitations on these rights. In some cases, these limitations are specified exemptions from copyright liability. One major limitation is the doctrine of “fair use,” which is given a statutory basis in section 107 of the 1976 Copyright Act. In other instances, the limitation takes the form of a “compulsory license” under which certain limited uses of copyrighted works are permitted upon payment of specified royalties and compliance with statutory conditions. For further information about the limitations of any of these rights, consult the copyright law or write to the Copyright Office.

Who Can Claim Copyright?

Copyright protection subsists from the time the work is created in fixed form. The copyright in the work of authorship immediately becomes the property of
the author who created the work. Only the author or those deriving their rights through the author can rightfully claim copyright.

In the case of works made for hire, the employer and not the employee is considered to be the author. Section 101 of the copyright law defines a “work made for hire” as:

1. a work prepared by an employee within the scope of his or her employment; or
2. a work specially ordered or commissioned for use as:
   - a contribution to a collective work
   - a part of a motion picture or other audiovisual work
   - a translation
   - a supplementary work
   - a compilation
   - an instructional text
   - a test
   - answer material for a test
   - an atlas

if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.

The authors of a joint work are co-owners of the copyright in the work, unless there is an agreement to the contrary. Copyright in each separate contribution to a periodical or other collective work is distinct from copyright in the collective work as a whole and vests initially with the author of the contribution.

**Two General Principles**

- Mere ownership of a book, manuscript, painting, or any other copy or phonorecord does not give the possessor the copyright. The law provides that transfer of ownership of any material object that embodies a protected work does not of itself convey any rights in the copyright.
- Minors may claim copyright, but state laws may regulate the business dealings involving copyrights owned by minors. For information on relevant state laws, consult an attorney.

**Copyright and National Origin of the Work**

Copyright protection is available for all unpublished works, regardless of the nationality or domicile of the author.

Published works are eligible for copyright protection in the United States if any one of the following conditions is met:

- On the date of first publication, one or more of the authors is a national or domiciliary of the United States, or is a national, domiciliary, or sovereign authority of a treaty party,* or is a stateless person wherever that person may be domiciled; or
- The work is first published in the United States or in a foreign nation that, on the date of first publication, is a treaty party. For purposes of this condition, a work that is published in the United States or a treaty party within 30 days after publication in a foreign nation that is not a treaty party shall be considered to be first published in the United States or such treaty party, as the case may be; or
- The work is a sound recording that was first fixed in a treaty party; or
- The work is a pictorial, graphic, or sculptural work that is incorporated in a building or other structure, or an architectural work that is embodied in a building and the building or structure is located in the United States or a treaty party; or
- The work is first published by the United Nations or any of its specialized agencies, or by the Organization of American States; or
- The work is a foreign work that was in the public domain in the United States prior to 1996 and its copyright was restored under the Uruguay Round Agreements Act (URAA), Request Circular 38b, Highlights of Copyright Amendments Contained in the Uruguay Round Agreements Act (URAA-GATT), for further information.
- The work comes within the scope of a Presidential proclamation.

*A treaty party is a country or intergovernmental organization other than the United States that is a party to an international agreement.

**What Works Are Protected?**

Copyright protects "original works of authorship" that are fixed in a tangible form of expression. The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device. Copyrightable works include the following categories:

1. literary works
2. musical works, including any accompanying words
3. dramatic works, including any accompanying music
4. pantomimes and choreographic works
5. pictorial, graphic, and sculptural works
motion pictures and other audiovisual works
sound recordings
architectural works

These categories should be viewed broadly. For example, computer programs and most "compilations" may be registered as "literary works"; maps and architectural plans may be registered as "pictorial, graphic, and sculptural works."

What Is Not Protected by Copyright?

Several categories of material are generally not eligible for federal copyright protection. These include among others:

- Works that have not been fixed in a tangible form of expression (for example, choreographic works that have not been notated or recorded, or improvisational speeches or performances that have not been written or recorded)
- Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listings of ingredients or contents
- Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, as distinguished from a description, explanation, or illustration
- Works consisting entirely of information that is common property and containing no original authorship (for example: standard calendars, height and weight charts, tape measures and rulers, and lists or tables taken from public documents or other common sources)

How to Secure a Copyright

Copyright Secured Automatically upon Creation

The way in which copyright protection is secured is frequently misunderstood. No publication or registration or other action in the Copyright Office is required to secure copyright. (See following NOTE.) There are, however, certain definite advantages to registration. See "Copyright Registration" on page 7.

Copyright is secured automatically when the work is created, and a work is "created" when it is fixed in a copy or phonorecord for the first time. "Copies" are material objects from which a work can be read or visually perceived either directly or with the aid of a machine or device, such as books, manuscripts, sheet music, film, videotape, or microfilm. "Phonorecords" are material objects embodying fixations of sounds (excluding, by statutory definition, motion picture soundtracks), such as cassette tapes, CDs, or LPs. Thus, for example, a song (the "work") can be fixed in sheet music ("copies") or in phonograph disks ("phonorecords"), or both. If a work is prepared over a period of time, the part of the work that is fixed on a particular date constitutes the created work as of that date.

Publication

Publication is no longer the key to obtaining federal copyright as it was under the Copyright Act of 1909. However, publication remains important to copyright owners.

The 1976 Copyright Act defines publication as follows:

"Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display constitutes publication. A public performance or display of a work does not of itself constitute publication.

NOTE: Before 1978, federal copyright was generally secured by the act of publication with notice of copyright, assuming compliance with all other relevant statutory conditions. U.S. works in the public domain on January 1, 1978, (for example, works published without satisfying all conditions for securing federal copyright under the Copyright Act of 1909) remain in the public domain under the 1976 Copyright Act.

Certain foreign works originally published without notice had their copyrights restored under the Uruguay Round Agreements Act (URAA). Request Circular 381 and see the "Notice of Copyright" section on page 4 of this publication for further information.

Federal copyright could also be secured before 1978 by the act of registration in the case of certain unpublished works and works eligible for ad interim copyright. The 1976 Copyright Act automatically extends to full term (section 304 sets the term) copyright for all works, including those subject to ad interim copyright if ad interim registration has been made on or before June 30, 1978.

A further discussion of the definition of "publication" can be found in the legislative history of the 1976 Copyright Act. The legislative reports define "to the public" as distribution to persons under no explicit or implicit restrictions with respect to disclosure of the contents. The reports state that the definition makes it clear that the sale of phonorecords constitutes publication of the underlying work, for example, the musical, dramatic, or literary work embodied
in a phonorecord. The reports also state that it is clear that any form of dissemination in which the material object does not change hands, for example, performances or displays on television, is not a publication no matter how many people are exposed to the work. However, when copies or phonorecords are offered for sale or lease to a group of wholesalers, broadcasters, or motion picture theaters, publication does take place if the purpose is further distribution, public performance, or public display.

Publication is an important concept in the copyright law for several reasons:

- Works that are published in the United States are subject to mandatory deposit with the Library of Congress. See discussion on “Mandatory Deposit for Works Published in the United States” on page 9.
- Publication of a work can affect the limitations on the exclusive rights of the copyright owner that are set forth in sections 107 through 121 of the law.
- The year of publication may determine the duration of copyright protection for anonymous and pseudonymous works (when the author’s identity is not revealed in the records of the Copyright Office) and for works made for hire.
- Deposit requirements for registration of published works differ from those for registration of unpublished works. See discussion on “Registration Procedures” on page 7.
- When a work is published, it may bear a notice of copyright to identify the year of publication and the name of the copyright owner and to inform the public that the work is protected by copyright. Copies of works published before March 1, 1989, must bear the notice or risk loss of copyright protection. See discussion on “Notice of Copyright” below.

**Notice of Copyright**

The use of a copyright notice is no longer required under U.S. law, although it is often beneficial. Because prior law did contain such a requirement, however, the use of notice is still relevant to the copyright status of older works.

Notice was required under the 1976 Copyright Act. This requirement was eliminated when the United States adhered to the Berne Convention, effective March 1, 1989. Although works published without notice before that date could have entered the public domain in the United States, the Uruguay Round Agreements Act (URAA) restores copyright in certain foreign works originally published without notice. For further information about copyright amendments in the URAA, request Circular 38B.

The Copyright Office does not take a position on whether copies of works first published with notice before March 1, 1989, which are distributed on or after March 1, 1989, must bear the copyright notice.

Use of the notice may be important because it informs the public that the work is protected by copyright, identifies the copyright owner, and shows the year of first publication. Furthermore, in the event that a work is infringed, if a proper notice of copyright appears on the published copy or copies to which a defendant in a copyright infringement suit had access, then no weight shall be given to such a defendant’s interposition of a defense based on innocent infringement in mitigation of actual or statutory damages, except as provided in section 504(c)(2) of the copyright law. Innocent infringement occurs when the infringer did not realize that the work was protected.

The use of the copyright notice is the responsibility of the copyright owner and does not require advance permission from, or registration with, the Copyright Office.

**Form of Notice for Visually Perceptible Copies**

The notice for visually perceptible copies should contain all the following three elements:

1. **The symbol ©** (the letter C in a circle), or the word “Copyright,” or the abbreviation “Copr.;” and

2. **The year of first publication** of the work. In the case of compilations or derivative works incorporating previously published material, the year date of first publication of the compilation or derivative work is sufficient. The year date may be omitted where a pictorial, graphic, or sculptural work, with accompanying textual matter, if any, is reproduced in or on greeting cards, postcards, stationery, jewelry, dolls, toys, or any useful article; and

3. **The name of the owner of copyright** in the work, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner.

Example: © 2004 John Doe

The “C in a circle” notice is used only on “visually perceptible copies.” Certain kinds of works—for example, musical, dramatic, and literary works—may be fixed not in “copies” but by means of sound in an audio recording. Since audio recordings such as audio tapes and phonograph disks are “phonorecords” and not “copies,” the “C in a circle” notice is not used to indicate protection of the underlying musical, dramatic, or literary work that is recorded.
Form of Notice for Phonorecords of Sound Recordings

The notice for phonorecords embodying a sound recording should contain all the following three elements:

1. The symbol © (the letter P in a circle); and
2. The year of first publication of the sound recording; and
3. The name of the owner of copyright in the sound recording, or an abbreviation by which the name can be recognized, or a generally known alternative designation of the owner. If the producer of the sound recording is named on the phonorecord label or container and if no other name appears in conjunction with the notice, the producer’s name shall be considered a part of the notice.

Example: © 2004 A.B.C. Records Inc.

NOTE: Since questions may arise from the use of variant forms of the notice, you may wish to seek legal advice before using any form of the notice other than those given here.

Position of Notice

The copyright notice should be affixed to copies or phonorecords in such a way as to “give reasonable notice of the claim of copyright.” The three elements of the notice should ordinarily appear together on the copies or phonorecords or on the phonorecord label or container. The Copyright Office has issued regulations concerning the form and position of the copyright notice in the Code of Federal Regulations (37 CFR Section 201.20). For more information, request Circular 3, Copyright Notice.

Publications Incorporating U.S. Government Works

Works by the U.S. Government are not eligible for U.S. copyright protection. For works published on and after March 1, 1989, the previous notice requirement for works consisting primarily of one or more U.S. Government works has been eliminated. However, use of a notice on such a work will defeat a claim of innocent infringement as previously described provided the notice also includes a statement that identifies either those portions of the work in which copyright is claimed or those portions that constitute U.S. Government material.

Example: © 2004 Jane Brown

Copyright claimed in Chapters 7–10, exclusive of U.S. Government maps

Copies of works published before March 1, 1989, that consist primarily of one or more works of the U.S. Government should have a notice and the identifying statement.

Unpublished Works

The author or copyright owner may wish to place a copyright notice on any unpublished copies or phonorecords that leave his or her control.

Example: Unpublished work © 2004 Jane Doe

Omission of Notice and Errors in Notice

The 1976 Copyright Act attempted to ameliorate the strict consequences of failure to include notice under prior law. It contained provisions that set out specific corrective steps to cure omissions or certain errors in notice. Under these provisions, an applicant had 5 years after publication to cure omission of notice or certain errors. Although these provisions are technically still in the law, their impact has been limited by the amendment making notice optional for all works published on and after March 1, 1989. For further information, request Circular 3.

How Long Copyright Protection Endures

Works Originally Created on or after January 1, 1978

A work that is created (fixed in tangible form for the first time) on or after January 1, 1978, is automatically protected from the moment of its creation and is ordinarily given a term enduring for the author’s life plus an additional 70 years after the author’s death. In the case of “a joint work prepared by two or more authors who did not work for hire,” the term lasts for 70 years after the last surviving author’s death. For works made for hire, and for anonymous and pseudonymous works (unless the author’s identity is revealed in Copyright Office records), the duration of copyright will be 95 years from publication or 120 years from creation, whichever is shorter.

Works Originally Created Before January 1, 1978, But Not Published or Registered by That Date

These works have been automatically brought under the statute and are now given federal copyright protection. The duration of copyright in these works will generally be computed in the same way as for works created on or after January 1, 1978: the life-plus-70 or 95/120-year terms will apply to them as well. The law provides that in no case will the term of copyright for works in this category expire before December 31, 2002, and for works published on or before December 31, 2002, the term of copyright will not expire before December 31, 2047.
Works Originally Created and Published or Registered before January 1, 1978

Under the law in effect before 1978, copyright was secured either on the date a work was published with a copyright notice or on the date of registration if the work was registered in unpublished form. In either case, the copyright endured for a first term of 28 years from the date it was secured. For the last (28th) year of the first term, the copyright was eligible for renewal. The Copyright Act of 1976 extended the renewal term from 28 to 47 years for copyrights that were subsisting on January 1, 1978, or for pre-1978 copyrights restored under the Uruguay Round Agreements Act (URAA), making these works eligible for a total term of protection of 75 years. Public Law 105-298, enacted on October 27, 1998, further extended the renewal term of copyrights still subsisting on that date by an additional 20 years, providing for a renewal term of 67 years and a total term of protection of 95 years.

Public Law 102-307, enacted on June 26, 1992, amended the 1976 Copyright Act to provide for automatic renewal of the term of copyrights secured between January 1, 1964, and December 31, 1977. Although the renewal term is automatically provided, the Copyright Office does not issue a renewal certificate for these works unless a renewal application and fee are received and registered in the Copyright Office.

Public Law 102-307 makes renewal registration optional. Thus, filing for renewal registration is no longer required in order to extend the original 28-year copyright term to the full 95 years. However, some benefits accrue from making a renewal registration during the 28th year of the original term.

For more detailed information on renewal of copyright and the copyright term, request Circular 15, Renewal of Copyright; Circular 15A, Duration of Copyright; and Circular 15T, Extension of Copyright Terms.

Transfer of Copyright

Any or all of the copyright owner’s exclusive rights or any subdivision of those rights may be transferred, but the transfer of exclusive rights is not valid unless that transfer is in writing and signed by the owner of the rights conveyed or such owner’s duly authorized agent. Transfer of a right on a nonexclusive basis does not require a written agreement.

A copyright may also be conveyed by operation of law and may be bequeathed by will or pass as personal property by the applicable laws of intestate succession.

Copyright is a personal property right, and it is subject to the various state laws and regulations that govern the ownership, inheritance, or transfer of personal property as well as terms of contracts or conduct of business. For information about relevant state laws, consult an attorney.

Transfers of copyright are normally made by contract. The Copyright Office does not have any forms for such transfers. The law does provide for the recordation in the Copyright Office of transfers of copyright ownership. Although, recordation is not required to make a valid transfer between the parties, it does provide certain legal advantages and may be required to validate the transfer against third parties. For information on recordation of transfers and other documents related to copyright, request Circular 12, Recordation of Transfers and Other Documents.

Termination of Transfers

Under the previous law, the copyright in a work reverted to the author, if living, or if the author was not living, to other specified beneficiaries, provided a renewal claim was registered in the 28th year of the original term. The present law drops the renewal feature except for works already in the first term of statutory protection when the present law took effect. Instead, the present law permits termination of a grant of rights after 35 years under certain conditions by serving written notice on the transferee within specified time limits.

For works already under statutory copyright protection before 1978, the present law provides a similar right of termination covering the newly added years that extended the former maximum term of the copyright from 56 to 95 years. For further information, request Circulars 15A and 15T.

*The copyright in works eligible for renewal on or after June 26, 1992, will vest in the name of the renewal claimant on the effective date of any renewal registration made during the 28th year of the original term. Otherwise, the renewal copyright will vest in the party entitled to claim renewal as of December 31st of the 28th year.

International Copyright Protection

There is no such thing as an “international copyright” that will automatically protect an author’s writings throughout the entire world. Protection against unauthorized use in a particular country depends, basically, on the national laws of that country. However, most countries do offer protection to foreign works under certain conditions, and these conditions have been greatly simplified by international copyright treaties and conventions. For further information and a list of countries that maintain copyright relations with the United States, request Circular 38A, International Copyright Relations of the United States.
Copyright Registration

In general, copyright registration is a legal formality intended to make a public record of the basic facts of a particular copyright. However, registration is not a condition of copyright protection. Even though registration is not a requirement for protection, the copyright law provides several inducements or advantages to encourage copyright owners to make registration. Among these advantages are the following:

• Registration establishes a public record of the copyright claim.

• Before an infringement suit may be filed in court, registration is necessary for works of U.S. origin.

• If made before or within 5 years of publication, registration will establish prima facie evidence in court of the validity of the copyright and of the facts stated in the certificate.

• If registration is made within 3 months after publication of the work or prior to an infringement of the work, statutory damages and attorney’s fees will be available to the copyright owner in court actions. Otherwise, only an award of actual damages and profits is available to the copyright owner.

• Registration allows the owner of the copyright to record the registration with the U.S. Customs Service for protection against the importation of infringing copies. For additional information, request Publication No. 563, How to Protect Your Intellectual Property Right, from: U.S. Customs Service, P.O. Box 7404, Washington, D.C. 20044. See the U.S. Customs Service website at www.customs.gov for online publications.

Registration may be made at any time within the life of the copyright. Unlike the law before 1978, when a work has been registered in unpublished form, it is not necessary to make another registration when the work becomes published, although the copyright owner may register the published edition, if desired.

Registration Procedures

Original Registration

To register a work, send the following three elements in the same envelope or package to:

Library of Congress
Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

1. A properly completed application form.

2. A nonrefundable filing fee of $50 for each application.

3. A nonreturnable deposit of the work being registered.

The deposit requirements vary in particular situations. The general requirements follow. Also note the information under “Special Deposit Requirements” on page 8.

• If the work is unpublished, one complete copy or phonorecord.

• If the work was first published in the United States on or after January 1, 1978, two complete copies or phonorecords of the best edition.

• If the work was first published in the United States before January 1, 1978, two complete copies or phonorecords of the work as first published.

• If the work was first published outside the United States, one complete copy or phonorecord of the work as first published.

• If sending multiple works, all applications, deposits, and fees should be sent in the same package. If possible, applications should be attached to the appropriate deposit. Whenever possible, number each package (e.g., 1 of 3, 2 of 4) to facilitate processing.

NOTE: For current information on fees, please write the Copyright Office, check the Copyright Office website at www.copyright.gov, or call (202) 707-3000.

What Happens if the Three Elements Are Not Received Together

Applications and fees received without appropriate copies, phonorecords, or identifying material will not be processed and ordinarily will be returned. Unpublished deposits without applications or fees ordinarily will be returned, also. In most cases, published deposits received without applications and fees can be immediately transferred to the collections of the Library of Congress. This practice is in accordance with section 406 of the law, which provides that the published deposit required for the collections of the Library of Congress may be used for registration only if the deposit is “accompanied by the prescribed application and fee…”

After the deposit is received and transferred to another service unit of the Library for its collections or other disposition, it is no longer available to the Copyright Office. If you wish to register the work, you must deposit additional copies or phonorecords with your application and fee.

Renewal Registration

To register a renewal, send:
United States Code Annotated Currentness
Title 17. Copyrights (Refs & Annos)
*§ Chapter 5. Copyright Infringement and Remedies (Refs & Annos)

§ 506. Criminal offenses

(a) Criminal infringement.--

(1) In general.--Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed--

(A) for purposes of commercial advantage or private financial gain;

(B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or

(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution.

(2) Evidence.--For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright.

(3) Definition.--In this subsection, the term "work being prepared for commercial distribution" means--

(A) a computer program, a musical work, a motion picture or other audiovisual work, or a sound recording, if, at the time of unauthorized distribution--

(i) the copyright owner has a reasonable expectation of commercial distribution; and

(ii) the copies or phonorecords of the work have not been commercially distributed; or

(B) a motion picture, if, at the time of unauthorized distribution, the motion picture--

(i) has been made available for viewing in a motion picture exhibition facility; and

(ii) has not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a motion picture exhibition facility.

(b) Forfeiture and Destruction.--When any person is convicted of any violation of subsection (a), the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction of other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.

BMG Music et al. v. Gonzalez

03 C 6276

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS

2005 U.S. Dist. LEXIS 910

January 7, 2005, Decided
January 12, 2005, Docketed

DISPOSITION: Summary judgment granted for plaintiffs.

COUNSEL: [*1] For BMG MUSIC, A NEW YORK GENERAL PARTNERSHIP, SONY MUSIC ENTERTAINMENT, INC., A DELAWARE CORPORATION, UMG RECORDINGS, INC., A DELAWARE CORPORATION, FONOUSA, INC., A CALIFORNIA CORPORATION, Plaintiffs: Charles B. Sklar, Clark Steven Tomashfsky, Darren J Schmidt, Jenner & Block, LLC, Chicago, IL; David A Steinberg, Mitchell, Silberberg & Knupp, Los Angeles, CA.

For ATLANTIC RECORDING CORPORATION, A DELAWARE CORPORATION, Plaintiff: Charles B. Sklar, Clark Steven Tomashfsky, Darren J Schmidt, Jenner & Block, LLC, Chicago, IL; David A Steinberg, Mitchell, Silberberg & Knupp, Los Angeles, CA; Geoffrey Andrew Baker, Dowell Baker, Oak Park, IL; Anthony E. Dowell, Jeffrey Allen Hammond, Dowell Baker, Lafayette, IN.

For CECILIA GONZALEZ, Defendant: Geoffrey Andrew Baker, Dowell Baker, Oak Park, IL.

JUDGES: BLANCHE M. MANNING.

OPINION: ORDER

Plaintiffs BMG Music, Sony Entertainment Inc., UMG Recordings, Inc., Fonovisa, Inc. and Atlantic Recording Corp. ("the Recording Companies") brought this action against Defendant Cecilia Gonzalez alleging that she infringed their copyrighted music recordings, in violation of 17 U.S.C. § 101 et seq. [*2] , by downloading 30 songs onto her home computer. After limited discovery, the Recording Companies now move for summary judgment.

The relevant facts in this case are not in dispute. Gonzalez admits that she infringed upon the Recording Companies' copyrights by downloading 30 songs from the internet which she did not own. Numerous courts have held that downloading music from the internet, which the user does not own, constitutes "direct infringement." In re Aimster Copyright Litig., 334 F.3d 643, 645 (7th Cir. 2003); A&M Records, Inc. v. Napster, 239 F.3d 1004, 1014 (9th Cir. 2001); Elektra Entertainment Group, Inc. v. Bryant, 2004 U.S. Dist. LEXIS 26700, 2004 WL 78123, at *4 (C.D. Cal. Feb. 13, 2004). Gonzalez, however, contends that summary judgment is not appropriate because there are genuine issues of fact as to whether: (1) the "fair use" defense (17 U.S.C. §
107) is applicable; and (2) she is entitled to assert the "innocent infringer" defense with respect to damages.

Gonzalez asserts that the "fair use" defense applies because she: (1) was just "sampling" the songs to determine if she wanted to purchase them; (2) already owned [*3] many of the songs she downloaded; and (3) did not cause any financial harm by downloading 30 songs. These contentions are without merit. First, the Ninth Circuit in A&M Records, Inc., 239 F.3d at 1014-19, rejected the argument that "sampling" by direct infringers is a "fair use." Second, the contention that Gonzalez already owned some of the recordings she downloaded is not relevant because the Recording Companies only seek redress for songs that Gonzalez admits she did not own. Finally, the court in A&M Records, Inc. held that the cumulative effect of direct infringers, like Gonzalez, harms the recording industry by reducing sales and "raising barriers" to the recording industry's "entry into the market for digital downloading of music." Id. at 1016. Accordingly, the Court GRANTS summary judgment on the infringement claim.

As for Gonzalez's contention that she is entitled to proceed to trial on damages, this argument likewise fails. She contends that even the minimum statutory damages, which are all the Recording Companies are seeking, are too high because there is an issue of fact as to whether she was an "innocent" infringer under 17 U.S.C. 504(c)(2) [*4], which gives courts "discretion" to award damages of only $ 200, where the infringer proves that she "was not aware and had no reason to believe that . . . her acts constituted infringement." Under section 402(d), however, the "innocent" infringement defense is not applicable "if a notice of copyright in the form and position specified by this section appears on the published [recordings] to which [the infringer] had access." (Emphasis added.) While it is undisputed that the copyrights of 30 songs at issue were properly noticed on the covers of CDs, Gonzalez contends that she has raised a question of fact as to whether she had access to the notice. Although it is true that Gonzalez did not have actual possession of these CDs, section 402(d) does not require proof that the infringer had "actual possession." 2 Nimmer on Copyright, §7.02[C][3], at 7-17 n.25 (2004). Instead, the plaintiff need only show that the CDs with notice "were in circulation [and] available" to the infringer. Id. See also Boisson v. Banian Ltd., 280 F. Supp. 2d 10, 17 (E.D.N.Y. 2003) ("innocent infringer" defense not applicable where defendant [*5] "had reason to be aware of the infringement"); Broadcast Music, Inc. v. Arios, 682 F. Supp. 1, 2 (D. Mass. 1986) (finding that simply claiming "ignorance" is not sufficient to raise a genuine issue of fact for a showing under section 402(d)”). Accordingly, because it is undisputed that the copyrights of the 30 songs at issue were properly noticed on the covers of the CDs, there is no question of fact as to whether Gonzalez had "access" to notice of the copyrights. Indeed, Gonzalez admits that she and her husband have legally purchased over 200 CDs. To allow Gonzalez to assert this defense based on her ignorance would eviscerate copyright protection and the old adage that "ignorance is no defense to the law." This Court thus holds that she is not entitled to the innocent infringer defense and awards the Record Companies $ 22,500 (30 songs times the minimum statutory penalty ($ 750)).

Finally, Gonzalez contends that injunctive relief is not appropriate because she no longer has online access, and therefore, she does not present a risk of future infringement. There is nothing, however, to stop her from reconnecting to the internet and resuming her infringement. Consequently, [*6] this Court follows the lead of other courts and issues an injunction, pursuant

BLANCHE M. MANNING

01-07-05
Opinion of the Court

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

SUPREME COURT OF THE UNITED STATES

No. 04-480

METRO-GOLDWYN-MAYER STUDIOS INC., ET AL.,
PETITIONERS v. GROKSTER, LTD., ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

[June 27, 2005]

JUSTICE SOUTER delivered the opinion of the Court.

The question is under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product. We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

I

A

Respondents, Grokster, Ltd., and StreamCast Networks, Inc., defendants in the trial court, distribute free software products that allow computer users to share electronic files through peer-to-peer networks, so called because users' computers communicate directly with each other, not through central servers. The advantage of peer-to-peer networks over information networks of other types shows up in their substantial and growing popularity. Because they need no central computer server to mediate the exchange of information or files among users, the high-
bandwidth communications capacity for a server may be dispensed with, and the need for costly server storage space is eliminated. Since copies of a file (particularly a popular one) are available on many users' computers, file requests and retrievals may be faster than on other types of networks, and since file exchanges do not travel through a server, communications can take place between any computers that remain connected to the network without risk that a glitch in the server will disable the network in its entirety. Given these benefits in security, cost, and efficiency, peer-to-peer networks are employed to store and distribute electronic files by universities, government agencies, corporations, and libraries, among others.\(^1\)

Other users of peer-to-peer networks include individual recipients of Grokster's and StreamCast's software, and although the networks that they enjoy through using the software can be used to share any type of digital file, they have prominently employed those networks in sharing copyrighted music and video files without authorization. A group of copyright holders (MGM for short, but including motion picture studios, recording companies, songwriters, and music publishers) sued Grokster and StreamCast for their users' copyright infringements, alleging that they knowingly and intentionally distributed their software to enable users to reproduce and distribute the copyrighted works in violation of the Copyright Act, 17 U. S. C. §101 et seq. (2000 ed. and Supp. II).\(^2\) MGM sought

---

\(^1\) Peer-to-peer networks have disadvantages as well. Searches on peer-to-peer networks may not reach and uncover all available files because search requests may not be transmitted to every computer on the network. There may be redundant copies of popular files. The creator of the software has no incentive to minimize storage or bandwidth consumption, the costs of which are borne by every user of the network. Most relevant here, it is more difficult to control the content of files available for retrieval and the behavior of users.

\(^2\) The studios and recording companies and the songwriters and music publishers filed separate suits against the defendants that were con-
Opinion of the Court

damages and an injunction.

Discovery during the litigation revealed the way the software worked, the business aims of each defendant company, and the predilections of the users. Grokster's eponymous software employs what is known as FastTrack technology, a protocol developed by others and licensed to Grokster. StreamCast distributes a very similar product except that its software, called Morpheus, relies on what is known as Gnutella technology. A user who downloads and installs either software possesses the protocol to send requests for files directly to the computers of others using software compatible with FastTrack or Gnutella. On the FastTrack network opened by the Grokster software, the user's request goes to a computer given an indexing capacity by the software and designated a supernode, or to some other computer with comparable power and capacity to collect temporary indexes of the files available on the computers of users connected to it. The supernode (or indexing computer) searches its own index and may communicate the search request to other supernodes. If the file is found, the supernode discloses its location to the computer requesting it, and the requesting user can download the file directly from the computer located. The copied file is placed in a designated sharing folder on the requesting user's computer, where it is available for other users to download in turn, along with any other file in that folder.

In the Gnutella network made available by Morpheus, the process is mostly the same, except that in some versions of the Gnutella protocol there are no supernodes. In these versions, peer computers using the protocol commu-

solidated by the District Court.

3 Subsequent versions of Morpheus, released after the record was made in this case, apparently rely not on Gnutella but on a technology called Neonet. These developments are not before us.
nicate directly with each other. When a user enters a search request into the Morpheus software, it sends the request to computers connected with it, which in turn pass the request along to other connected peers. The search results are communicated to the requesting computer, and the user can download desired files directly from peers' computers. As this description indicates, Grokster and StreamCast use no servers to intercept the content of the search requests or to mediate the file transfers conducted by users of the software, there being no central point through which the substance of the communications passes in either direction.\(^4\)

Although Grokster and StreamCast do not therefore know when particular files are copied, a few searches using their software would show what is available on the networks the software reaches. MGM commissioned a statistician to conduct a systematic search, and his study showed that nearly 90% of the files available for download on the FastTrack system were copyrighted works.\(^5\) Grokster and StreamCast dispute this figure, raising methodological problems and arguing that free copying even of copyrighted works may be authorized by the rightholders. They also argue that potential noninfringing uses of their software are significant in kind, even if infrequent in practice. Some musical performers, for example, have gained new audiences by distributing their copyrighted works for free across peer-to-peer networks, and some

\(^4\)There is some evidence that both Grokster and StreamCast previously operated supernodes, which compiled indexes of files available on all of the nodes connected to them. This evidence, pertaining to previous versions of the defendants' software, is not before us and would not affect our conclusions in any event.

\(^5\)By comparison, evidence introduced by the plaintiffs in *A & M Records, Inc. v. Napster, Inc.*, 239 F. 3d 1004 (CA9 2001), showed that 87% of files available on the Napster filesharing network were copyrighted, *id.*, at 1013.
distributors of unprotected content have used peer-to-peer networks to disseminate files, Shakespeare being an example. Indeed, StreamCast has given Morpheus users the opportunity to download the briefs in this very case, though their popularity has not been quantified.

As for quantification, the parties' anecdotal and statistical evidence entered thus far to show the content available on the FastTrack and Gnutella networks does not say much about which files are actually downloaded by users, and no one can say how often the software is used to obtain copies of unprotected material. But MGM's evidence gives reason to think that the vast majority of users' downloads are acts of infringement, and because well over 100 million copies of the software in question are known to have been downloaded, and billions of files are shared across the FastTrack and Gnutella networks each month, the probable scope of copyright infringement is staggering.

Grokker and StreamCast concede the infringement in most downloads, Brief for Respondents 10, n. 6, and it is uncontested that they are aware that users employ their software primarily to download copyrighted files, even if the decentralized FastTrack and Gnutella networks fail to reveal which files are being copied, and when. From time to time, moreover, the companies have learned about their users' infringement directly, as from users who have sent e-mail to each company with questions about playing copyrighted movies they had downloaded, to whom the companies have responded with guidance.6 App. 559-563, 808-816, 939-954. And MGM notified the companies of 8 million copyrighted files that could be obtained using their software.

Grokker and StreamCast are not, however, merely passive recipients of information about infringing use.

---

6The Grokker founder contends that in answering these e-mails he often did not read them fully. App. 77, 769.
The record is replete with evidence that from the moment Grokster and StreamCast began to distribute their free software, each one clearly voiced the objective that recipients use it to download copyrighted works, and each took active steps to encourage infringement.

After the notorious file-sharing service, Napster, was sued by copyright holders for facilitation of copyright infringement, *A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (ND Cal. 2000), aff'd in part, rev'd in part, 239 F. 3d 1004 (CA9 2001), StreamCast gave away a software program of a kind known as OpenNap, designed as compatible with the Napster program and open to Napster users for downloading files from other Napster and OpenNap users' computers. Evidence indicates that "[i]t was always [StreamCast's] intent to use [its OpenNap network] to be able to capture email addresses of [its] initial target market so that [it] could promote [its] StreamCast Morpheus interface to them," App. 861; indeed, the OpenNap program was engineered "to leverage Napster's 50 million user base," *id.*, at 746.

StreamCast monitored both the number of users downloading its OpenNap program and the number of music files they downloaded. *Id.*, at 859, 863, 866. It also used the resulting OpenNap network to distribute copies of the Morpheus software and to encourage users to adopt it. *Id.*, at 861, 867, 1039. Internal company documents indicate that StreamCast hoped to attract large numbers of former Napster users if that company was shut down by court order or otherwise, and that StreamCast planned to be the next Napster. *Id.*, at 861. A kit developed by StreamCast to be delivered to advertisers, for example, contained press articles about StreamCast's potential to capture former Napster users, *id.*, at 568–572, and it introduced itself to some potential advertisers as a company "which is similar to what Napster was," *id.*, at 884. It broadcast banner advertisements to users of other
Opinion of the Court

Napster-compatible software, urging them to adopt its OpenNap. *Id.*, at 586. An internal e-mail from a company executive stated: “We have put this network in place so that when Napster pulls the plug on their free service . . . or if the Court orders them shut down prior to that . . . we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative.” *Id.*, at 588–589, 861.

Thus, StreamCast developed promotional materials to market its service as the best Napster alternative. One proposed advertisement read: “Napster Inc. has announced that it will soon begin charging you a fee. That’s if the courts don’t order it shut down first. What will you do to get around it?” *Id.*, at 897. Another proposed ad touted StreamCast’s software as the “#1 alternative to Napster” and asked “[w]hen the lights went off at Napster . . . where did the users go?” *Id.*, at 836 (ellipses in original).7 StreamCast even planned to flaunt the illegal uses of its software; when it launched the OpenNap network, the chief technology officer of the company averred that “[t]he goal is to get in trouble with the law and get sued. It’s the best way to get in the new[s].” *Id.*, at 916.

The evidence that Grokster sought to capture the market of former Napster users is sparser but revealing, for Grokster launched its own OpenNap system called Swap- tor and inserted digital codes into its Web site so that computer users using Web search engines to look for “Napster” or “free filesharing” would be directed to the Grokster Web site, where they could download the Grok- ster software. *Id.*, at 992–993. And Grokster’s name is an apparent derivative of Napster.

---

7The record makes clear that StreamCast developed these promotional materials but not whether it released them to the public. Even if these advertisements were not released to the public and do not show encouragement to infringe, they illuminate StreamCast’s purposes.
StreamCast's executives monitored the number of songs by certain commercial artists available on their networks, and an internal communication indicates they aimed to have a larger number of copyrighted songs available on their networks than other file-sharing networks. *Id.*, at 868. The point, of course, would be to attract users of a mind to infringe, just as it would be with their promotional materials developed showing copyrighted songs as examples of the kinds of files available through Morpheus. *Id.*, at 848. Morpheus in fact allowed users to search specifically for “Top 40” songs, *id.*, at 735, which were inevitably copyrighted. Similarly, Grokster sent users a newsletter promoting its ability to provide particular, popular copyrighted materials. Brief for Motion Picture Studio and Recording Company Petitioners 7–8.

In addition to this evidence of express promotion, marketing, and intent to promote further, the business models employed by Grokster and StreamCast confirm that their principal object was use of their software to download copyrighted works. Grokster and StreamCast receive no revenue from users, who obtain the software itself for nothing. Instead, both companies generate income by selling advertising space, and they stream the advertising to Grokster and Morpheus users while they are employing the programs. As the number of users of each program increases, advertising opportunities become worth more. Cf. App. 539, 804. While there is doubtless some demand for free Shakespeare, the evidence shows that substantive volume is a function of free access to copyrighted work. Users seeking Top 40 songs, for example, or the latest release by Modest Mouse, are certain to be far more numerous than those seeking a free Decameron, and Grokster and StreamCast translated that demand into dollars.

Finally, there is no evidence that either company made an effort to filter copyrighted material from users’ downloads or otherwise impede the sharing of copyrighted
files. Although Grokster appears to have sent e-mails warning users about infringing content when it received threatening notice from the copyright holders, it never blocked anyone from continuing to use its software to share copyrighted files. *Id.*, at 75–76. StreamCast not only rejected another company's offer of help to monitor infringement, *id.*, at 928–929, but blocked the Internet Protocol addresses of entities it believed were trying to engage in such monitoring on its networks, *id.*, at 917–922.

B

After discovery, the parties on each side of the case cross-moved for summary judgment. The District Court limited its consideration to the asserted liability of Grokster and StreamCast for distributing the current versions of their software, leaving aside whether either was liable "for damages arising from past versions of their software, or from other past activities." 259 F. Supp. 2d 1029, 1033 (CD Cal. 2003). The District Court held that those who used the Grokster and Morpheus software to download copyrighted media files directly infringed MGM's copyrights, a conclusion not contested on appeal, but the court nonetheless granted summary judgment in favor of Grokster and StreamCast as to any liability arising from distribution of the then current versions of their software. Distributing that software gave rise to no liability in the court's view, because its use did not provide the distributors with actual knowledge of specific acts of infringement. Case No. CV 01 08541 SVW (PJWx) (CD Cal., June 18, 2003), App. 1213.

The Court of Appeals affirmed. 380 F. 3d 1154 (CA9 2004). In the court's analysis, a defendant was liable as a contributory infringer when it had knowledge of direct infringement and materially contributed to the infringement. But the court read *Sony Corp. of America v. Uni-
versal City Studios, Inc., 464 U. S. 417 (1984), as holding that distribution of a commercial product capable of substantial noninfringing uses could not give rise to contributory liability for infringement unless the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge. The fact that the software was capable of substantial noninfringing uses in the Ninth Circuit’s view meant that Grokster and StreamCast were not liable, because they had no such actual knowledge, owing to the decentralized architecture of their software. The court also held that Grokster and StreamCast did not materially contribute to their users’ infringement because it was the users themselves who searched for, retrieved, and stored the infringing files, with no involvement by the defendants beyond providing the software in the first place.

The Ninth Circuit also considered whether Grokster and StreamCast could be liable under a theory of vicarious infringement. The court held against liability because the defendants did not monitor or control the use of the software, had no agreed-upon right or current ability to supervise its use, and had no independent duty to police infringement. We granted certiorari. 543 U. S. ___ (2004).

II

A

MGM and many of the amici fault the Court of Appeals’s holding for upsetting a sound balance between the respective values of supporting creative pursuits through copyright protection and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement. The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the trade-off. See Sony Corp. v. Universal City Studios, supra, at 442; see generally Gins-

The tension between the two values is the subject of this case, with its claim that digital distribution of copyrighted material threatens copyright holders as never before, because every copy is identical to the original, copying is easy, and many people (especially the young) use file-sharing software to download copyrighted works. This very breadth of the software’s use may well draw the public directly into the debate over copyright policy, Peters, Brace Memorial Lecture: Copyright Enters the Public Domain, 51 J. Copyright Soc. 701, 705–717 (2004) (address by Register of Copyrights), and the indications are that the ease of copying songs or movies using software like Grokster’s and Napster’s is fostering disdain for copyright protection, Wu, When Code Isn’t Law, 89 Va. L. Rev. 679, 724–726 (2003). As the case has been presented to us, these fears are said to be offset by the different concern that imposing liability, not only on infringers but on distributors of software based on its potential for unlawful use, could limit further development of beneficial technologies. See, e.g., Lemley & Reese, Reducing Digital Copyright Infringement Without Restricting Innovation, 56 Stan. L. Rev. 1345, 1386–1390 (2004); Brief for Innovation Scholars and Economists as Amici Curiae 15–20; Brief for Emerging Technology Companies as Amici Curiae 19–25; Brief for Intel Corporation as Amicus Curiae 20–22.8

8The mutual exclusivity of these values should not be overstated, however. On the one hand technological innovators, including those writing filesharing computer programs, may wish for effective copyright protections for their work. See, e.g., Wu, When Code Isn’t Law, 89 Va. L. Rev. 679, 750 (2003). (StreamCast itself was urged by an associate
The argument for imposing indirect liability in this case is, however, a powerful one, given the number of infringing downloads that occur every day using StreamCast's and Grokster's software. When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement. See In re Aimster Copyright Litigation, 334 F. 3d 643, 645–646 (CA7 2003).

One infringes contributorily by intentionally inducing or encouraging direct infringement, see Gershwin Pub. Corp. v. Columbia Artists Management, Inc., 443 F. 2d 1159, 1162 (CA2 1971), and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it, Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F. 2d 304, 307 (CA2 1963). Although to "get [its] technology written down and [its intellectual property] protected." App. 866.) On the other hand the widespread distribution of creative works through improved technologies may enable the synthesis of new works or generate audiences for emerging artists. See Eldred v. Ashcroft, 537 U. S. 186, 223–226 (2003) (STEVENS, J., dissenting); Van Houweling, Distributive Values in Copyright, 83 Texas L. Rev. 1535, 1539–1540, 1562–1564 (2005); Brief for Sovereign Artists et al. as Amici Curiae 11.

"We stated in Sony Corp. of America v. Universal City Studios, Inc., 464 U. S. 417 (1984), that "the lines between direct infringement, contributory infringement and vicarious liability are not clearly drawn' . . . . [R]easoned analysis of [the Sony plaintiffs' contributory infringement claim] necessarily entails consideration of arguments and case law which may also be forwarded under the other labels, and indeed the parties . . . rely upon such arguments and authority in support of their respective positions on the issue of contributory infringement," id., at 435, n. 17 (quoting Universal City Studios, Inc. v. Sony Corp., 480 F. Supp. 429, 457–458 (CD Cal. 1979)). In the present case MGM has argued a vicarious liability theory, which allows imposition of liability when the defendant profits directly from the infringement and has a right and ability to supervise the direct infringer, even if the
Opinion of the Court


B

Despite the currency of these principles of secondary liability, this Court has dealt with secondary copyright infringement in only one recent case, and because MGM has tailored its principal claim to our opinion there, a look at our earlier holding is in order. In Sony Corp. v. Universal City Studios, supra, this Court addressed a claim that secondary liability for infringement can arise from the very distribution of a commercial product. There, the product, novel at the time, was what we know today as the videocassette recorder or VCR. Copyright holders sued Sony as the manufacturer, claiming it was contributorily liable for infringement that occurred when VCR owners taped copyrighted programs because it supplied the means used to infringe, and it had constructive knowledge that infringement would occur. At the trial on the merits, the evidence showed that the principal use of the VCR was for "time-shifting," or taping a program for later viewing at a more convenient time, which the Court found to be a fair, not an infringing, use. Id., at 423–424. There was no defendant initially lacks knowledge of the infringement. See, e.g., Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F. 2d 304, 308 (CA2 1963); Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F. 2d 354, 355 (CA7 1929). Because we resolve the case based on an induction theory, there is no need to analyze separately MGM's vicarious liability theory.
evidence that Sony had expressed an object of bringing about taping in violation of copyright or had taken active steps to increase its profits from unlawful taping. *Id.*, at 438. Although Sony’s advertisements urged consumers to buy the VCR to “record favorite shows” or “build a library” of recorded programs, *id.*, at 459 (Blackmun, J., dissenting), neither of these uses was necessarily infringing, *id.*, at 424, 454–455.

On those facts, with no evidence of stated or indicated intent to promote infringing uses, the only conceivable basis for imposing liability was on a theory of contributory infringement arising from its sale of VCRs to consumers with knowledge that some would use them to infringe. *Id.*, at 439. But because the VCR was “capable of commercially significant noninfringing uses,” we held the manufacturer could not be faulted solely on the basis of its distribution. *Id.*, at 442.

This analysis reflected patent law’s traditional staple article of commerce doctrine, now codified, that distribution of a component of a patented device will not violate the patent if it is suitable for use in other ways. 35 U. S. C. §271(c); *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U. S. 476, 485 (1964) (noting codification of cases); *id.*, at 486, n. 6 (same). The doctrine was devised to identify instances in which it may be presumed from distribution of an article in commerce that the distributor intended the article to be used to infringe another’s patent, and so may justly be held liable for that infringement. “One who makes and sells articles which are only adapted to be used in a patented combination will be presumed to intend the natural consequences of his acts; he will be presumed to intend that they shall be used in the combination of the patent.” *New York Scaffolding Co. v. Whitney*, 224 F. 452, 459 (CA8 1915); see also *James Heekin Co. v. Baker*, 138 F. 63, 66 (CA8 1905); *Canda v. Michigan Malleable Iron Co.*, 124 F. 486, 489 (CA6 1903); *Thomson-
Opinion of the Court

_Houston Electric Co. v. Ohio Brass Co.,_ 80 F. 712, 720–721 (CA6 1897); _Red Jacket Mfg. Co. v. Davis_, 82 F. 432, 439 (CA7 1897); _Holly v. Vergennes Machine Co.,_ 4 F. 74, 82 (CC Vt. 1880); _Renwick v. Pond_, 20 F. Cas. 536, 541 (No. 11,702) (CC SDNY 1872).

In sum, where an article is “good for nothing else” but infringement, _Canda v. Michigan Malleable Iron Co._, _supra_, at 489, there is no legitimate public interest in its unlicensed availability, and there is no injustice in presuming or imputing an intent to infringe, see _Henry v. A. B. Dick Co._, 224 U. S. 1, 48 (1912), overruled on other grounds, _Motion Picture Patents Co. v. Universal Film Mfg. Co._, 243 U. S. 502 (1917). Conversely, the doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one’s products will be misused. It leaves breathing room for innovation and a vigorous commerce. See _Sony Corp. v. Universal City Studios, supra_, at 442; _Dawson Chemical Co. v. Rohm & Haas Co._, 448 U. S. 176, 221 (1980); _Henry v. A. B. Dick Co._, _supra_, at 48.

The parties and many of the amici in this case think the key to resolving it is the Sony rule and, in particular, what it means for a product to be “capable of commercially significant noninfringing uses.” _Sony Corp. v. Universal City Studios, supra_, at 442. MGM advances the argument that granting summary judgment to Grokster and StreamCast as to their current activities gave too much weight to the value of innovative technology, and too little to the copyrights infringed by users of their software, given that 90% of works available on one of the networks was shown to be copyrighted. Assuming the remaining 10% to be its noninfringing use, MGM says this should not qualify as “substantial,” and the Court should quantify Sony to the extent of holding that a product used “princi-
pally” for infringement does not qualify. See Brief for Motion Picture Studio and Recording Company Petitioners 31. As mentioned before, Grokster and StreamCast reply by citing evidence that their software can be used to reproduce public domain works, and they point to copyright holders who actually encourage copying. Even if infringement is the principal practice with their software today, they argue, the noninfringing uses are significant and will grow.

We agree with MGM that the Court of Appeals misapplied Sony, which it read as limiting secondary liability quite beyond the circumstances to which the case applied. Sony barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement. The Ninth Circuit has read Sony's limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had “specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information.” 380 F. 3d, at 1162 (internal quotation marks and alterations omitted). Because the Circuit found the StreamCast and Grokster software capable of substantial lawful use, it concluded on the basis of its reading of Sony that neither company could be held liable, since there was no showing that their software, being without any central server, afforded them knowledge of specific unlawful uses.

This view of Sony, however, was error, converting the case from one about liability resting on imputed intent to one about liability on any theory. Because Sony did not
displace other theories of secondary liability, and because we find below that it was error to grant summary judgment to the companies on MGM's inducement claim, we do not revisit Sony further, as MGM requests, to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur. It is enough to note that the Ninth Circuit's judgment rested on an erroneous understanding of Sony and to leave further consideration of the Sony rule for a day when that may be required.

C

Sony's rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in Sony requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law.10 Sony Corp. v. Universal City Studios, 464 U. S., at 439 (“If vicarious liability is to be imposed on Sony in this case, it must rest on the fact that it has sold equipment with constructive knowledge” of the potential for infringement). Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, Sony's staple-article rule will not preclude liability.

The classic case of direct evidence of unlawful purpose occurs when one induces commission of infringement by another, or “entic[es] or persuad[es] another” to infringe, Black's Law Dictionary 790 (8th ed. 2004), as by advertising. Thus at common law a copyright or patent defendant

---

10Nor does the Patent Act's exemption from liability for those who distribute a staple article of commerce, 35 U. S. C. §271(c), extend to those who induce patent infringement, §271(b).
who "not only expected but invoked [infringing use] by advertisement" was liable for infringement "on principles recognized in every part of the law." *Kalem Co. v. Harper Brothers*, 222 U.S., at 62–63 (copyright infringement). See also *Henry v. A. B. Dick Co.*, 224 U.S., at 48–49 (contributory liability for patent infringement may be found where a good's "most conspicuous use is one which will coöperate in an infringement when sale to such user is invoked by advertisement" of the infringing use); *Thomson-Houston Electric Co. v. Kelsey Electric R. Specialty Co.*, 75 F. 1005, 1007–1008 (CA2 1896) (relying on advertisements and displays to find defendant's "willingness ... to aid other persons in any attempts which they may be disposed to make towards [patent] infringement"); *Rumford Chemical Works v. Hecker*, 20 F. Cas. 1342, 1346 (No. 12,133) (CC N. J. 1876) (demonstrations of infringing activity along with "avowals of the [infringing] purpose and use for which it was made" supported liability for patent infringement).

The rule on inducement of infringement as developed in the early cases is no different today.\(^{11}\) Evidence of "active steps ... taken to encourage direct infringement," *Oak Industries, Inc. v. Zenith Electronics Corp.*, 697 F. Supp. 988, 992 (ND Ill. 1988), such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe, and a showing that infringement was encouraged overcomes the law's reluctance to find liability when a defendant merely sells a commercial product suitable for some lawful use, see, e.g., *Water Technologies Corp. v. Calco, Ltd.*, 850 F. 2d 660, 668 (CA Fed. 1988) (liability for inducement where one "actively and knowingly aid[s] and abet[s] another's direct infringement" (emphasis omitted)); *Fromberg, Inc. v. Thornhill*, 315 F. 2d 407, 412–413 (CA5

\(^{11}\) Inducement has been codified in patent law. *Ibid.*
1963) (demonstrations by sales staff of infringing uses supported liability for inducement); *Haworth Inc. v. Herman Miller Inc.*, 37 USPQ 2d 1080, 1090 (WD Mich. 1994) (evidence that defendant "demonstrate[d] and recommend[ed] infringing configurations" of its product could support inducement liability); *Sims v. Mack Trucks, Inc.*, 459 F. Supp. 1198, 1215 (ED Pa. 1978) (finding inducement where the use "depicted by the defendant in its promotional film and brochures infringes the ... patent"), overruled on other grounds, 608 F. 2d 87 (CA3 1979). Cf. W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser and Keeton on Law of Torts 37 (5th ed. 1984) ("There is a definite tendency to impose greater responsibility upon a defendant whose conduct was intended to do harm, or was morally wrong").

For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential. Accordingly, just as *Sony* did not find intentional inducement despite the knowledge of the VCR manufacturer that its device could be used to infringe, 464 U. S., at 439, n. 19, mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to
compromise legitimate commerce or discourage innovation having a lawful promise.

III

A

The only apparent question about treating MGM's evidence as sufficient to withstand summary judgment under the theory of inducement goes to the need on MGM's part to adduce evidence that StreamCast and Grokster communicated an inducing message to their software users. The classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations. MGM claims that such a message is shown here. It is undisputed that StreamCast beamed onto the computer screens of users of Napster-compatible programs ads urging the adoption of its OpenNap program, which was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement. Those who accepted StreamCast's OpenNap program were offered software to perform the same services, which a factfinder could conclude would readily have been understood in the Napster market as the ability to download copyrighted music files. Grokster distributed an electronic newsletter containing links to articles promoting its software's ability to access popular copyrighted music. And anyone whose Napster or free file-sharing searches turned up a link to Grokster would have understood Grokster to be offering the same file-sharing ability as Napster, and to the same people who probably used Napster for infringing downloads; that would also have been the understanding of anyone offered Grokster's suggestively named Swaptor software, its version of OpenNap. And both companies communicated a clear message by responding affirmatively to requests for help in locating and playing copyrighted materials.
Opinion of the Court

In StreamCast's case, of course, the evidence just described was supplemented by other unequivocal indications of unlawful purpose in the internal communications and advertising designs aimed at Napster users ("When the lights went off at Napster... where did the users go?" App. 836 (ellipsis in original)). Whether the messages were communicated is not to the point on this record. The function of the message in the theory of inducement is to prove by a defendant's own statements that his unlawful purpose disqualifies him from claiming protection (and incidentally to point to actual violators likely to be found among those who hear or read the message). See supra, at 17–19. Proving that a message was sent out, then, is the preeminent but not exclusive way of showing that active steps were taken with the purpose of bringing about infringing acts, and of showing that infringing acts took place by using the device distributed. Here, the summary judgment record is replete with other evidence that Grokster and StreamCast, unlike the manufacturer and distributor in Sony, acted with a purpose to cause copyright violations by use of software suitable for illegal use. See supra, at 6–9.

Three features of this evidence of intent are particularly notable. First, each company showed itself to be aiming to satisfy a known source of demand for copyright infringement, the market comprising former Napster users. StreamCast's internal documents made constant reference to Napster, it initially distributed its Morpheus software through an OpenNap program compatible with Napster, it advertised its OpenNap program to Napster users, and its Morpheus software functions as Napster did except that it could be used to distribute more kinds of files, including copyrighted movies and software programs. Grokster's name is apparently derived from Napster, it too initially offered an OpenNap program, its software's function is likewise comparable to Napster's, and it attempted to
divert queries for Napster onto its own Web site. Grokster and StreamCast's efforts to supply services to former Napster users, deprived of a mechanism to copy and distribute what were overwhelmingly infringing files, indicate a principal, if not exclusive, intent on the part of each to bring about infringement.

Second, this evidence of unlawful objective is given added significance by MGM's showing that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activity, we think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement.12

Third, there is a further complement to the direct evidence of unlawful objective. It is useful to recall that StreamCast and Grokster make money by selling advertising space, by directing ads to the screens of computers employing their software. As the record shows, the more the software is used, the more ads are sent out and the greater the advertising revenue becomes. Since the extent of the software's use determines the gain to the distributors, the commercial sense of their enterprise turns on high-volume use, which the record shows is infringing.13

---

12 Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the Sony safe harbor.

13 Grokster and StreamCast contend that any theory of liability based on their conduct is not properly before this Court because the rulings in the trial and appellate courts dealt only with the present versions of their software, not "past acts ... that allegedly encouraged infringement or assisted ... known acts of infringement." Brief for Respondents 14; see also id., at 34. This contention misapprehends the basis
Opinion of the Court

This evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear. The unlawful objective is unmistakable.

B

In addition to intent to bring about infringement and distribution of a device suitable for infringing use, the inducement theory of course requires evidence of actual infringement by recipients of the device, the software in this case. As the account of the facts indicates, there is evidence of infringement on a gigantic scale, and there is no serious issue of the adequacy of MGM's showing on this point in order to survive the companies' summary judgment requests. Although an exact calculation of infringing use, as a basis for a claim of damages, is subject to dispute, there is no question that the summary judgment evidence is at least adequate to entitle MGM to go forward with claims for damages and equitable relief.

* * *

In sum, this case is significantly different from Sony and reliance on that case to rule in favor of StreamCast and Grokster was error. Sony dealt with a claim of liability based solely on distributing a product with alternative lawful and unlawful uses, with knowledge that some users would follow the unlawful course. The case struck a bal-

for their potential liability. It is not only that encouraging a particular consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable act is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use. See Kalem Co. v. Harper Brothers, 222 U.S. 55, 62–63 (1911); Cable/Home Communication Corp. v. Network Productions, Inc., 902 F.2d 829, 846 (CA11 1990); A & M Records, Inc. v. Abdallah, 948 F. Supp. 1449, 1456 (CD Cal. 1996).
ance between the interests of protection and innovation by holding that the product's capability of substantial lawful employment should bar the imputation of fault and consequent secondary liability for the unlawful acts of others.

MGM's evidence in this case most obviously addresses a different basis of liability for distributing a product open to alternative uses. Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement. If liability for inducing infringement is ultimately found, it will not be on the basis of presuming or imputing fault, but from inferring a patently illegal objective from statements and actions showing what that objective was.

There is substantial evidence in MGM's favor on all elements of inducement, and summary judgment in favor of Grokster and StreamCast was error. On remand, reconsideration of MGM's motion for summary judgment will be in order.

The judgment of the Court of Appeals is vacated, and the case is remanded for further proceedings consistent with this opinion.

It is so ordered.
GINSBURG, J., concurring

SUPREME COURT OF THE UNITED STATES

No. 04-480

METRO-GOLDWYN-MAYER STUDIOS INC., ET AL.,
PETITIONERS v. GROKSTER, LTD., ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

[June 27, 2005]

JUSTICE GINSBURG, with whom THE CHIEF JUSTICE and JUSTICE KENNEDY join, concurring.

I concur in the Court’s decision, which vacates in full the judgment of the Court of Appeals for the Ninth Circuit, ante, at 24, and write separately to clarify why I conclude that the Court of Appeals misperceived, and hence misapplied, our holding in Sony Corp. of America v. Universal City Studios, Inc., 464 U. S. 417 (1984). There is here at least a “genuine issue as to [a] material fact,” Fed. Rule Civ. Proc. 56(c), on the liability of Grokster or StreamCast, not only for actively inducing copyright infringement, but also or alternatively, based on the distribution of their software products, for contributory copyright infringement. On neither score was summary judgment for Grokster and StreamCast warranted.

At bottom, however labeled, the question in this case is whether Grokster and StreamCast are liable for the direct infringing acts of others. Liability under our jurisprudence may be predicated on actively encouraging (or inducing) infringement through specific acts (as the Court’s opinion develops) or on distributing a product distributees use to infringe copyrights, if the product is not capable of “substantial” or “commercially significant” noninfringing uses. Sony, 464 U. S., at 442; see also 3 M. Nimmer & D. Nimmer, Nimmer on Copyright §12.04[A][2] (2005). While
the two categories overlap, they capture different culpable behavior. Long coexisting, both are now codified in patent law. Compare 35 U.S.C. §271(b) (active inducement liability), with §271(c) (contributory liability for distribution of a product not "suitable for substantial noninfringing use").

In Sony, 464 U.S. 417, the Court considered Sony's liability for selling the Betamax video cassette recorder. It did so enlightened by a full trial record. Drawing an analogy to the staple article of commerce doctrine from patent law, the Sony Court observed that the "sale of an article ... adapted to [a patent] infringing use" does not suffice "to make the seller a contributory infringer" if the article "is also adapted to other and lawful uses." Id., at 441 (quoting Henry v. A. B. Dick Co., 224 U.S. 1, 48 (1912), overruled on other grounds, Motion Picture Patents Co. v. Universal Film Mfg. Co., 243 U.S. 502, 517 (1917)).

"The staple article of commerce doctrine" applied to copyright, the Court stated, "must strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce." Sony, 464 U.S., at 442. "Accordingly," the Court held, "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses." Ibid. Thus, to resolve the Sony case, the Court explained, it had to determine "whether the Betamax is capable of commercially significant noninfringing uses." Ibid.

To answer that question, the Court considered whether "a significant number of [potential uses of the Betamax were] noninfringing." Ibid. The Court homed in on one potential use—private, noncommercial time-shifting of
television programs in the home (i.e., recording a broadcast TV program for later personal viewing). Time-shifting was noninfringing, the Court concluded, because in some cases trial testimony showed it was authorized by the copyright holder, id., at 443–447, and in others it qualified as legitimate fair use, id., at 447–455. Most purchasers used the Betamax principally to engage in time-shifting, id., at 421, 423, a use that "plainly satisfies" the Court’s standard, id., at 442. Thus, there was no need in Sony to "give precise content to the question of how much [actual or potential] use is commercially significant." Ibid. Further development was left for later days.

1 Justice Breyer finds in Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), a "clear" rule permitting contributory liability for copyright infringement based on distribution of a product only when the product "will be used almost exclusively to infringe copyrights." Post, at 9–10. But cf. Sony, 464 U.S., at 442 (recognizing "copyright holder’s legitimate demand for effective—not merely symbolic—protection"). Sony, as I read it, contains no clear, near-exclusivity test. Nor have Courts of Appeals unanimously recognized Justice Breyer’s clear rule. Compare A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004, 1021 (CA9 2001) ("Evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement.") with In re Aimster Copyright Litigation, 334 F. 3d 643, 648–650 (CA7 2003) ("When a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement. . . . But the balancing of costs and benefits is necessary only in a case in which substantial noninfringing uses, present or prospective, are demonstrated."). See also Matthew Bender & Co., Inc. v. West Pub. Co., 158 F. 3d 693, 707 (CA2 1998) ("The Supreme Court applied [the Sony] test to prevent copyright holders from leveraging the copyrights in their original work to control distribution of . . . products that might be used incidentally for infringement, but that had substantial noninfringing uses. . . . The same rationale applies here [to products] that have substantial, predominant and noninfringing uses as tools for research and citation."). All Members of the Court agree, moreover, that "the Court of Appeals misapplied Sony," at least to the extent it read that decision to limit "secondary liability" to a hardly-ever cate-
and cases.

The Ninth Circuit went astray, I will endeavor to explain, when that court granted summary judgment to Grokster and StreamCast on the charge of contributory liability based on distribution of their software products. Relying on its earlier opinion in A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004 (CA9 2001), the Court of Appeals held that “if substantial noninfringing use was shown, the copyright owner would be required to show that the defendant had reasonable knowledge of specific infringing files.” 380 F. 3d 1154, 1161 (CA9 2004). “A careful examination of the record,” the court concluded, “indicates that there is no genuine issue of material fact as to noninfringing use.” Ibid. The appeals court pointed to the band Wilco, which made one of its albums available for free downloading, to other recording artists who may have authorized free distribution of their music through the Internet, and to public domain literary works and films available through Grokster’s and StreamCast’s software. Ibid. Although it acknowledged MGM’s assertion that “the vast majority of the software use is for copyright infringement,” the court concluded that Grokster’s and StreamCast’s proffered evidence met Sony’s requirement that “a product need only be capable of substantial noninfringing uses.” 380 F. 3d, at 1162.2

This case differs markedly from Sony. Cf. Peters, Brace Memorial Lecture: Copyright Enters the Public Domain, 51 J. Copyright Soc. 701, 724 (2004) (“The Grokster panel’s reading of Sony is the broadest that any court has given it

---

1 Grokster and StreamCast, in the Court of Appeals’ view, would be entitled to summary judgment unless MGM could show that that the software companies had knowledge of specific acts of infringement and failed to act on that knowledge—a standard the court held MGM could not meet. 380 F. 3d, at 1162–1163.
Here, there has been no finding of any fair use and little beyond anecdotal evidence of noninfringing uses. In finding the Grokster and StreamCast software products capable of substantial noninfringing uses, the District Court and the Court of Appeals appear to have relied largely on declarations submitted by the defendants. These declarations include assertions (some of them hearsay) that a number of copyright owners authorize distribution of their works on the Internet and that some public domain material is available through peer-to-peer networks including those accessed through Grokster's and StreamCast's software. 380 F.3d, at 1161; 259 F. Supp. 2d 1029, 1035–1036 (CD Cal. 2003); App. 125–171.

The District Court declared it "undisputed that there are substantial noninfringing uses for Defendants' software," thus obviating the need for further proceedings. 259 F. Supp. 2d, at 1035. This conclusion appears to rest almost entirely on the collection of declarations submitted by Grokster and StreamCast. Ibid. Review of these declarations reveals mostly anecdotal evidence, sometimes obtained second-hand, of authorized copyrighted works or public domain works available online and shared through peer-to-peer networks, and general statements about the benefits of peer-to-peer technology. See, e.g., Decl. of Janis Ian ¶13, App. 128 ("P2P technologies offer musicians an alternative channel for promotion and distribution."); Decl. of Gregory Newby ¶12, id., at 136 ("Numerous authorized and public domain Project Gutenberg eBooks are made available on Morpheus, Kazaa, Gnutella, Grokster, and similar software products."); Decl. of Aram Sinnreich ¶6, id., at 151 ("file sharing seems to have a net positive impact on music sales"); Decl. of John Busher ¶8, id., at 166 ("I estimate that Acoustica generates sales of between $1,000 and $10,000 per month as a result of the distribution of its trialware software through the Gnutella and FastTrack Networks."); Decl. of Patricia D. Hoekman ¶¶3–
4, id., at 169–170 (search on Morpheus for “President Bush speeches” found several video recordings, searches for “Declaration of Independence” and “Bible” found various documents and declarant was able to download a copy of the Declaration); Decl. of Sean L. Mayers ¶11, id., at 67 (“Existing open, decentralized peer-to-peer file-sharing networks . . . offer content owners distinct business advantages over alternate online distribution technologies.”). Compare Decl. of Brewster Kahle ¶20, id., at 142 (“Those who download the Prelinger films . . . are entitled to redistribute those files, and the Archive welcomes their redistribution by the Morpheus-Grokster-KaZaa community of users.”), with Deposition of Brewster Kahle, id., at 396–403 (Sept. 18, 2002) (testifying that he has no knowledge of any person downloading a Prelinger film using Morpheus, Grokster, or KaZaA). Compare also Decl. of Richard Prelinger ¶17, id., at 147 (“[W]e welcome further redistribution of the Prelinger films . . . by individuals using peer-to-peer software products like Morpheus, KaZaA and Grokster.”), with Deposition of Richard Prelinger, id., at 410–411 (Oct. 1, 2002) (“Q. What is your understanding of Grokster? A. I have no understanding of Grokster. . . . Q. Do you know whether any user of the Grokster software has made available to share any Prelinger film? A. No.”). See also Deposition of Aram Sinnreich, id., at 390 (Sept. 25, 2002) (testimony about the band Wilco based on “[t]he press and industry news groups and scuttlebutt.”). These declarations do not support summary judgment in the face of evidence, proffered by MGM, of overwhelming use of Grokster’s and StreamCast’s software for infringement.³

³Justice Breyer finds support for summary judgment in this motley collection of declarations and in a survey conducted by an expert retained by MGM. Post, at 4–8. That survey identified 76% of the files available through Grokster as copyrighted works owned or controlled by the plaintiffs, and 15% of the files as works likely copyrighted. App.
GINSBURG, J., concurring

Even if the absolute number of noninfringing files copied using the Grokster and StreamCast software is large, it does not follow that the products are therefore put to substantial noninfringing uses and are thus immune from liability. The number of noninfringing copies may be reflective of, and dwarfed by, the huge total volume of files shared. Further, the District Court and the Court of Appeals did not sharply distinguish between uses of Grokster's and StreamCast's software products (which this case is about) and uses of peer-to-peer technology generally (which this case is not about).

In sum, when the record in this case was developed, there was evidence that Grokster's and StreamCast's products were, and had been for some time, overwhelmingly used to infringe, ante, at 4–6; App. 434–439, 476–481, and that this infringement was the overwhelming source of revenue from the products, ante, at 8–9; 259 F. Supp. 2d, at 1043–1044. Fairly appraised, the evidence was insufficient to demonstrate, beyond genuine debate, a reasonable prospect that substantial or commercially significant noninfringing uses were likely to develop over

439. As to the remaining 10% of the files, "there was not enough information to form reasonable conclusions either as to what those files even consisted of, and/or whether they were infringing or noninfringing." App. 479. Even assuming, as JUSTICE BREYER does, that the Sony Court would have absolved Sony of contributory liability solely on the basis of the use of the Betamax for authorized time-shifting, post, at 3–4, summary judgment is not inevitably appropriate here. Sony stressed that the plaintiffs there owned "well below 10%" of copyrighted television programming, 464 U.S., at 443, and found, based on trial testimony from representatives of the four major sports leagues and other individuals authorized to consent to home-recording of their copyrighted broadcasts, that a similar percentage of program copying was authorized, id., at 424. Here, the plaintiffs allegedly control copyrights for 70% or 75% of the material exchanged through the Grokster and StreamCast software, 380 F. 3d, at 1158; App. 439, and the District Court does not appear to have relied on comparable testimony about authorized copying from copyright holders.
time. On this record, the District Court should not have ruled dispositively on the contributory infringement charge by granting summary judgment to Grokster and StreamCast.4

If, on remand, the case is not resolved on summary judgment in favor of MGM based on Grokster and StreamCast actively inducing infringement, the Court of Appeals, I would emphasize, should reconsider, on a fuller record, its interpretation of Sony's product distribution holding.

4The District Court's conclusion that "[p]laintiffs do not dispute that Defendants' software is being used, and could be used, for substantial noninfringing purposes," 259 F. Supp. 2d 1029, 1036 (CD Cal. 2003); accord 380 F. 3d, at 1161, is, to say the least, dubious. In the courts below and in this Court, MGM has continuously disputed any such conclusion. Brief for Motion Picture Studio and Recording Company Petitioners 30–38; Brief for MGM Plaintiffs-Appellants in No. 03–55894, etc. (CA9), p. 41; App. 356–357, 361–365.
BREYER, J., concurring

SUPREME COURT OF THE UNITED STATES

No. 04–480

METRO-GOLDWYN-MAYER STUDIOS INC., ET AL., PETITIONERS v. GROKSTER, LTD., ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

[June 27, 2006]

JUSTICE BREYER, with whom JUSTICE STEVENS and JUSTICE O'CONNOR join, concurring.

I agree with the Court that the distributor of a dual-use technology may be liable for the infringing activities of third parties where he or she actively seeks to advance the infringement. Ante, at 1. I further agree that, in light of our holding today, we need not now "revisit" Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984). Ante, at 17. Other Members of the Court, however, take up the Sony question: whether Grokster's product is "capable of 'substantial' or 'commercially significant' noninfringing uses." Ante, at 1 (GINSBURG, J., concurring) (quoting Sony, supra, at 442). And they answer that question by stating that the Court of Appeals was wrong when it granted summary judgment on the issue in Grokster's favor. Ante, at 4. I write to explain why I disagree with them on this matter.

I

The Court's opinion in Sony and the record evidence (as described and analyzed in the many briefs before us) together convince me that the Court of Appeals' conclusion has adequate legal support.

A

I begin with Sony's standard. In Sony, the Court con-
sidered the potential copyright liability of a company that did not itself illegally copy protected material, but rather sold a machine—a Video Cassette Recorder (VCR)—that could be used to do so. A buyer could use that machine for noninfringing purposes, such as recording for later viewing (sometimes called “time-shifting,”) Sony, 464 U.S., at 421) uncopyrighted television programs or copyrighted programs with a copyright holder’s permission. The buyer could use the machine for infringing purposes as well, such as building libraries of taped copyrighted programs. Or, the buyer might use the machine to record copyrighted programs under circumstances in which the legal status of the act of recording was uncertain (i.e., where the copying may, or may not, have constituted a “fair use,” id., at 425–426). Sony knew many customers would use its VCRs to engage in unauthorized copying and “library-building.” Id., at 458–459 (Blackmun, J., dissenting). But that fact, said the Court, was insufficient to make Sony itself an infringer. And the Court ultimately held that Sony was not liable for its customers’ acts of infringement.

In reaching this conclusion, the Court recognized the need for the law, in fixing secondary copyright liability, to “strike a balance between a copyright holder’s legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the interests of others freely to engage in substantially unrelated areas of commerce.” Id., at 442. It pointed to patent law’s “staple article of commerce” doctrine, ibid., under which a distributor of a product is not liable for patent infringement by its customers unless that product is “unsuited for any commercial noninfringing use.” Dawson Chemical Co. v. Rohm & Haas Co., 448 U. S. 176, 198 (1980). The Court wrote that the sale of copying equipment, “like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capa-
ble of substantial noninfringing uses." Sony, 464 U. S., at 442 (emphasis added). The Court ultimately characterized the legal "question" in the particular case as "whether [Sony's VCR] is capable of commercially significant noninfringing uses" (while declining to give "precise content" to these terms). *Ibid.* (emphasis added).

It then applied this standard. The Court had before it a survey (commissioned by the District Court and then prepared by the respondents) showing that roughly 9% of all VCR recordings were of the type—namely, religious, educational, and sports programming—owned by producers and distributors testifying on Sony's behalf who did not object to time-shifting. See Brief for Respondent Universal Studios et al. O. T. 1983, No. 81–1687, pp. 52–53; see also *Sony*, supra, at 424 (7.3% of all Sony VCR use is to record sports programs; representatives of the sports leagues do not object). A much higher percentage of VCR *users* had at one point taped an authorized program, in addition to taping unauthorized programs. And the plaintiffs—not a large class of content providers as in this case—owned only a small percentage of the total available unauthorized programming. See *ante*, at 6–7, and n. 3 (GINSBURG, J., concurring). But of all the taping actually done by Sony's customers, only around 9% was of the sort the Court referred to as authorized.

The Court found that the magnitude of authorized programming was "significant," and it also noted the "significant potential for future authorized copying." 464 U. S., at 444. The Court supported this conclusion by referencing the trial testimony of professional sports league officials and a religious broadcasting representative. *Id.*, at 444, and n. 24. It also discussed (1) a Los Angeles educational station affiliated with the Public Broadcasting Service that made many of its programs available for home taping, and (2) Mr. Rodgers' Neighborhood, a widely watched children's program. *Id.*, at 445.
On the basis of this testimony and other similar evidence, the Court determined that producers of this kind had authorized duplication of their copyrighted programs “in significant enough numbers to create a substantial market for a noninfringing use of the” VCR. *Id.*, at 447, n. 28 (emphasis added).

The Court, in using the key word “substantial,” indicated that these circumstances alone constituted a sufficient basis for rejecting the imposition of secondary liability. See *id.*, at 456 (“Sony demonstrated a significant likelihood that substantial numbers of copyright holders” would not object to time-shifting (emphasis added)). Nonetheless, the Court buttressed its conclusion by finding separately that, in any event, unauthorized time-shifting often constituted not infringement, but “fair use.” *Id.*, at 447–456.

B

When measured against *Sony’s* underlying evidence and analysis, the evidence now before us shows that Grokster passes *Sony’s* test—that is, whether the company’s product is capable of substantial or commercially significant noninfringing uses. *Id.*, at 442. For one thing, petitioners’ (hereinafter MGM) own expert declared that 75% of current files available on Grokster are infringing and 15% are “likely infringing.” See App. 436–439, ¶¶6–17 (Decl. of Dr. Ingram Olkin); cf. *ante*, at 4 (opinion of the Court). That leaves some number of files near 10% that apparently are noninfringing, a figure very similar to the 9% or so of authorized time-shifting uses of the VCR that the Court faced in *Sony*.

As in *Sony*, witnesses here explained the nature of the noninfringing files on Grokster’s network without detailed quantification. Those files include:

—Authorized copies of music by artists such as Wilco,
Janis Ian, Pearl Jam, Dave Matthews, John Mayer, and others. See App. at 152–153, ¶¶9–13 (Decl. of Aram Sinnreich) (Wilco’s “lesson has already been adopted by artists still signed to their major labels”); id., at 170, ¶¶5–7 (Decl. of Patricia D. Hoekman) (locating “numerous audio recordings” that were authorized for swapping); id., at 74, ¶10 (Decl. of Daniel B. Rung) (describing Grokster’s partnership with a company that hosts music from thousands of independent artists)

—Free electronic books and other works from various online publishers, including Project Gutenberg. See id., at 136, ¶12 (Decl. of Gregory B. Newby) (“Numerous authorized and public domain Project Gutenberg eBooks are made available” on Grokster. Project Gutenberg “welcomes this widespread sharing . . . using these software products[,] since they assist us in meeting our objectives”); id., at 159–160, ¶32 (Decl. of Sinnreich)

—Public domain and authorized software, such as WinZip 8.1. Id., at 170, ¶8 (Decl. of Hoekman); id., at 165, ¶¶4–7 (Decl. of John Busher)

—Licensed music videos and television and movie segments distributed via digital video packaging with the permission of the copyright holder. Id., at 70, ¶24 (Decl. of Sean L. Mayers)

The nature of these and other lawfully swapped files is such that it is reasonable to infer quantities of current lawful use roughly approximate to those at issue in Sony. At least, MGM has offered no evidence sufficient to survive summary judgment that could plausibly demonstrate a significant quantitative difference. See ante, at 4 (opinion of the Court); see also Brief for Motion Picture Studio and Recording Company Petitioners i (referring to “at
least 90% of the total use of the services"; but see ante, at 6–7, n. 3 (GINSBURG, J., concurring). To be sure, in quantitative terms these uses account for only a small percentage of the total number of uses of Grokster’s product. But the same was true in Sony, which characterized the relatively limited authorized copying market as “substantial.” (The Court made clear as well in Sony that the amount of material then presently available for lawful copying—if not actually copied—was significant, see 464 U. S., at 444, and the same is certainly true in this case.)

Importantly, Sony also used the word “capable,” asking whether the product is “capable of” substantial noninfringing uses. Its language and analysis suggest that a figure like 10%, if fixed for all time, might well prove insufficient, but that such a figure serves as an adequate foundation where there is a reasonable prospect of expanded legitimate uses over time. See ibid. (noting a “significant potential for future authorized copying”). And its language also indicates the appropriateness of looking to potential future uses of the product to determine its “capability.”

Here the record reveals a significant future market for noninfringing uses of Grokster-type peer-to-peer software. Such software permits the exchange of any sort of digital file—whether that file does, or does not, contain copyrighted material. As more and more uncopyrighted information is stored in swappable form, it seems a likely inference that lawful peer-to-peer sharing will become increasingly prevalent. See, e.g., App. 142, ¶20 (Decl. of Brewster Kahle) (“The [Internet Archive] welcomes [the] redistribution [of authorized films] by the Morpheus-Grokster-KaZaa community of users”); id., at 166, ¶8 (Decl. of Busher) (sales figures of $1,000 to $10,000 per month through peer-to-peer networks “will increase in the future as Acoustica’s trialware is more widely distributed through these networks”); id., at 156–164, ¶¶21–40 (Decl. of Sinnreich).
And that is just what is happening. Such legitimate noninfringing uses are coming to include the swapping of: research information (the initial purpose of many peer-to-peer networks); public domain films (e.g., those owned by the Prelinger Archive); historical recordings and digital educational materials (e.g., those stored on the Internet Archive); digital photos (OurPictures, for example, is starting a P2P photo-swapping service); "shareware" and "freeware" (e.g., Linux and certain Windows software); secure licensed music and movie files (Intent MediaWorks, for example, protects licensed content sent across P2P networks); news broadcasts past and present (the BBC Creative Archive lets users "rip, mix and share the BBC"); user-created audio and video files (including "podcasts" that may be distributed through P2P software); and all manner of free "open content" works collected by Creative Commons (one can search for Creative Commons material on StreamCast). See Brief for Distributed Computing Industry Association as Amicus Curiae 15–26; Merges, A New Dynamism in the Public Domain, 71 U. Chi. L. Rev. 183 (2004). I can find nothing in the record that suggests that this course of events will not continue to flow naturally as a consequence of the character of the software taken together with the foreseeable development of the Internet and of information technology. Cf. ante, at 1–2 (opinion of the Court) (discussing the significant benefits of peer-to-peer technology).

There may be other now-unforeseen noninfringing uses that develop for peer-to-peer software, just as the home-video rental industry (unmentioned in Sony) developed for the VCR. But the foreseeable development of such uses, when taken together with an estimated 10% noninfringing material, is sufficient to meet Sony's standard. And while Sony considered the record following a trial, there are no facts asserted by MGM in its summary judgment filings that lead me to believe the outcome after a trial here could
be any different. The lower courts reached the same conclusion.

Of course, Grokster itself may not want to develop these other noninfringing uses. But Sony's standard seeks to protect not the Groksters of this world (which in any event may well be liable under today's holding), but the development of technology more generally. And Grokster's desires in this respect are beside the point.

II

The real question here, I believe, is not whether the record evidence satisfies Sony. As I have interpreted the standard set forth in that case, it does. And of the Courts of Appeals that have considered the matter, only one has proposed interpreting Sony more strictly than I would do—in a case where the product might have failed under any standard. In re Aimster Copyright Litigation, 334 F. 3d 643, 653 (CA7 2003) (defendant “failed to show that its service is ever used for any purpose other than to infringe” copyrights (emphasis added)); see Matthew Bender & Co., Inc. v. West Pub. Co., 158 F. 3d 693, 706–707 (CA2 1998) (court did not require that noninfringing uses be “predominant,” it merely found that they were predominant, and therefore provided no analysis of Sony's boundaries); but see ante, at 3 n. 1 (GINSBURG, J., concurring); see also A&M Records v. Napster, Inc., 239 F. 3d 1004, 1020 (CA9 2001) (discussing Sony); Cable/Home Communication Corp. v. Network Productions, Inc., 902 F. 2d 829, 842–847 (CA11 1990) (same); Vault Corp. v. Quaid Software, Ltd., 847 F. 2d 255, 262 (CA5 1988) (same); cf. Dynacore Holdings Corp. v. U. S. Philips Corp., 363 F. 3d 1263, 1275 (CA Fed. 2004) (same); see also Doe v. GTE Corp., 347 F. 3d 655, 661 (CA7 2003) (“A person may be liable as a contributory infringer if the product or service it sells has no (or only slight) legal use”).

Instead, the real question is whether we should modify
the *Sony* standard, as MGM requests, or interpret *Sony* more strictly, as I believe JUSTICE GINSBURG's approach would do in practice. Compare ante, at 4–8 (concurring) (insufficient evidence in this case of both present lawful uses and of a reasonable prospect that substantial non-infringing uses would develop over time), with *Sony*, 464 U. S., at 442–447 (basing conclusion as to the likely existence of a substantial market for authorized copying upon general declarations, some survey data, and common sense).

As I have said, *Sony* itself sought to "strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce." Id., at 442. Thus, to determine whether modification, or a strict interpretation, of *Sony* is needed, I would ask whether MGM has shown that *Sony* incorrectly balanced copyright and new-technology interests. In particular: (1) Has *Sony* (as I interpret it) worked to protect new technology? (2) If so, would modification or strict interpretation significantly weaken that protection? (3) If so, would new or necessary copyright-related benefits outweigh any such weakening?

A

The first question is the easiest to answer. *Sony*'s rule, as I interpret it, has provided entrepreneurs with needed assurance that they will be shielded from copyright liability as they bring valuable new technologies to market.

*Sony*'s rule is clear. That clarity allows those who develop new products that are capable of substantial non-infringing uses to know, ex ante, that distribution of their product will not yield massive monetary liability. At the same time, it helps deter them from distributing products that have no other real function than—or that are specifically intended for—copyright infringement, deterrence
that the Court's holding today reinforces (by adding a weapon to the copyright holder's legal arsenal).

Sony's rule is strongly technology protecting. The rule deliberately makes it difficult for courts to find secondary liability where new technology is at issue. It establishes that the law will not impose copyright liability upon the distributors of dual-use technologies (who do not themselves engage in unauthorized copying) unless the product in question will be used almost exclusively to infringe copyrights (or unless they actively induce infringements as we today describe). Sony thereby recognizes that the copyright laws are not intended to discourage or to control the emergence of new technologies, including (perhaps especially) those that help disseminate information and ideas more broadly or more efficiently. Thus Sony's rule shelters VCRs, typewriters, tape recorders, photocopiers, computers, cassette players, compact disc burners, digital video recorders, MP3 players, Internet search engines, and peer-to-peer software. But Sony's rule does not shelter descramblers, even if one could theoretically use a descrambler in a noninfringing way. 464 U. S., at 441–442; Compare Cable/Home Communication Corp., supra, at 837–850 (developer liable for advertising television signal descrambler), with Vault Corp., supra, at 262 (primary use infringing but a substantial noninfringing use).

Sony's rule is forward looking. It does not confine its scope to a static snapshot of a product's current uses (thereby threatening technologies that have undeveloped future markets). Rather, as the VCR example makes clear, a product's market can evolve dramatically over time. And Sony—by referring to a capacity for substantial noninfringing uses—recognizes that fact. Sony's word "capable" refers to a plausible, not simply a theoretical, likelihood that such uses will come to pass, and that fact anchors Sony in practical reality. Cf. Aimster, supra, at 651.
BREYER, J., concurring

Sony's rule is mindful of the limitations facing judges where matters of technology are concerned. Judges have no specialized technical ability to answer questions about present or future technological feasibility or commercial viability where technology professionals, engineers, and venture capitalists themselves may radically disagree and where answers may differ depending upon whether one focuses upon the time of product development or the time of distribution. Consider, for example, the question whether devices can be added to Grokster's software that will filter out infringing files. MGM tells us this is easy enough to do, as do several amici that produce and sell the filtering technology. See, e.g., Brief for Motion Picture Studio Petitioners 11; Brief for Audible Magic Corp. et al. as Amicus Curiae 3–10. Grokster says it is not at all easy to do, and not an efficient solution in any event, and several apparently disinterested computer science professors agree. See Brief for Respondents 31; Brief for Computer Science Professors as Amicus Curiae 6–10, 14–18. Which account should a judge credit? Sony says that the judge will not necessarily have to decide.

Given the nature of the Sony rule, it is not surprising that in the last 20 years, there have been relatively few contributory infringement suits—based on a product distribution theory—brought against technology providers (a small handful of federal appellate court cases and perhaps fewer than two dozen District Court cases in the last 20 years). I have found nothing in the briefs or the record that shows that Sony has failed to achieve its innovation-protecting objective.

B

The second, more difficult, question is whether a modified Sony rule (or a strict interpretation) would significantly weaken the law's ability to protect new technology. JUSTICE GINSBURG's approach would require defendants
to produce considerably more concrete evidence—more than was presented here—to earn Sony's shelter. That heavier evidentiary demand, and especially the more dramatic (case-by-case balancing) modifications that MGM and the Government seek, would, I believe, undercut the protection that Sony now offers.

To require defendants to provide, for example, detailed evidence—say business plans, profitability estimates, projected technological modifications, and so forth—would doubtless make life easier for copyright holder plaintiffs. But it would simultaneously increase the legal uncertainty that surrounds the creation or development of a new technology capable of being put to infringing uses. Inventors and entrepreneurs (in the garage, the dorm room, the corporate lab, or the boardroom) would have to fear (and in many cases endure) costly and extensive trials when they create, produce, or distribute the sort of information technology that can be used for copyright infringement. They would often be left guessing as to how a court, upon later review of the product and its uses, would decide when necessarily rough estimates amounted to sufficient evidence. They would have no way to predict how courts would weigh the respective values of infringing and noninfringing uses; determine the efficiency and advisability of technological changes; or assess a product's potential future markets. The price of a wrong guess—even if it involves a good-faith effort to assess technical and commercial viability—could be large statutory damages (not less than $750 and up to $30,000 per infringed work). 17 U.S.C. §504(c)(1). The additional risk and uncertainty would mean a consequent additional chill of technological development.

C

The third question—whether a positive copyright impact would outweigh any technology-related loss—I find the
most difficult of the three. I do not doubt that a more intrusive Sony test would generally provide greater revenue security for copyright holders. But it is harder to conclude that the gains on the copyright swings would exceed the losses on the technology roundabouts.

For one thing, the law disfavors equating the two different kinds of gain and loss; rather, it leans in favor of protecting technology. As Sony itself makes clear, the producer of a technology which permits unlawful copying does not himself engage in unlawful copying—a fact that makes the attachment of copyright liability to the creation, production, or distribution of the technology an exceptional thing. See 464 U.S., at 431 (courts “must be circumspect” in construing the copyright laws to preclude distribution of new technologies). Moreover, Sony has been the law for some time. And that fact imposes a serious burden upon copyright holders like MGM to show a need for change in the current rules of the game, including a more strict interpretation of the test. See, e.g., Brief for Motion Picture Studio Petitioners 31 (Sony should not protect products when the “primary or principal” use is infringing).

In any event, the evidence now available does not, in my view, make out a sufficiently strong case for change. To say this is not to doubt the basic need to protect copyrighted material from infringement. The Constitution itself stresses the vital role that copyright plays in advancing the “useful Arts.” Art. I, §8, cl. 8. No one disputes that “reward to the author or artist serves to induce release to the public of the products of his creative genius.” United States v. Paramount Pictures, Inc., 334 U.S. 131, 158 (1948). And deliberate unlawful copying is no less an unlawful taking of property than garden-variety theft. See, e.g., 18 U.S.C. §2319 (criminal copyright infringement); §1961(1)(B) (copyright infringement can be a predicate act under the Racketeer Influenced and Corrupt
Organizations Act; §1956(c)(7)(D) (money laundering includes the receipt of proceeds from copyright infringement). But these highly general principles cannot by themselves tell us how to balance the interests at issue in Sony or whether Sony’s standard needs modification. And at certain key points, information is lacking.

Will an unmodified Sony lead to a significant diminution in the amount or quality of creative work produced? Since copyright’s basic objective is creation and its revenue objectives but a means to that end, this is the underlying copyright question. See Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) (“Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts”). And its answer is far from clear.

Mar29?language=printer (discussing mixed evidence).

The extent to which related production has actually and resultingly declined remains uncertain, though there is good reason to believe that the decline, if any, is not substantial. See, e.g., M. Madden, Pew Internet & American Life Project, Artists, Musicians, and the Internet, p. 21, http://www.pewinternet.org/pdfs/PIP_Artists.Musicians_Report.pdf (nearly 70% of musicians believe that file sharing is a minor threat or no threat at all to creative industries); Benkler, Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production, 114 Yale L. J. 273, 351–352 (2004) ("Much of the actual flow of revenue to artists—from performances and other sources—is stable even assuming a complete displacement of the CD market by peer-to-peer distribution . . . . [I]t would be silly to think that music, a cultural form without which no human society has existed, will cease to be in our world [because of illegal file swapping]").

More importantly, copyright holders at least potentially have other tools available to reduce piracy and to abate whatever threat it poses to creative production. As today's opinion makes clear, a copyright holder may proceed against a technology provider where a provable specific intent to infringe (of the kind the Court describes) is present. Ante, at 24 (opinion of the Court). Services like Grokster may well be liable under an inducement theory.

In addition, a copyright holder has always had the legal authority to bring a traditional infringement suit against one who wrongfully copies. Indeed, since September 2003, the Recording Industry Association of America (RIAA) has filed "thousands of suits against people for sharing copyrighted material." Walker, New Movement Hits Universities: Get Legal Music, Washington Post, Mar. 17, 2005, p. E1. These suits have provided copyright holders with damages; have served as a teaching tool, making clear that much file sharing, if done without permission, is
unlawful; and apparently have had a real and significant deterrent effect. See, e.g., L. Rainie, M. Madden, D. Hess, & G. Mudd, Pew Internet Project and comScore Media Metrix Data Memo: The state of music downloading and file-sharing online, pp. 2, 4, 6, 10 (Apr. 2004), www.pewinternet.org/pdfs/PIP_Filesharing_April_04.pdf (number of people downloading files fell from a peak of roughly 35 million to roughly 23 million in the year following the first suits; 38% of current downloaders report downloading fewer files because of the suits); M. Madden & L. Rainie, Pew Internet Project Data Memo: Music and video downloading moves beyond P2P, p. 7 (March 2005), www.pewinternet.org/pdfs/PIP_Filesharing_March05.pdf (number of downloaders has “inched up” but “continues to rest well below the peak level”); Groenings, Note, Costs and Benefits of the Recording Industry’s Litigation Against Individuals, 20 Berkeley Technology L. J. 571 (2005); but see Evangelista, Downloading Music and Movie Files is as Popular as Ever, San Francisco Chronicle, Mar. 28, 2005, p. E1 (referring to the continuing “tide of rampant copyright infringement,” while noting that the RIAA says it believes the “campaign of lawsuits and public education has at least contained the problem”).

Further, copyright holders may develop new technological devices that will help curb unlawful infringement. Some new technology, called “digital ‘watermarking’” and “digital fingerprint[ing],” can encode within the file information about the author and the copyright scope and date, which “fingerprints” can help to expose infringers. RIAA Reveals Method to Madness, Wired News, Aug. 28, 2003, http://www.wired.com/news/digiwood/0,1412,60222,00.html; Besek, Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts, 27 Colum. J. L. & Arts 385, 391, 451 (2004). Other technology can, through encryption, potentially restrict users’ ability to make a digital copy. See J. Borland,
Tripping the Rippers, C/net News.com (Sept. 28, 2001), http://news.com.com/Tripping+the+rippers/2009=1023_3= 273619.html; but see Brief for Bridgemar Services Ltd. as Amicus Curiae 5–8 (arguing that peer-to-peer service providers can more easily block unlawful swapping).

At the same time, advances in technology have discouraged unlawful copying by making lawful copying (e.g., downloading music with the copyright holder’s permission) cheaper and easier to achieve. Several services now sell music for less than $1 per song. (Walmart.com, for example, charges $0.88 each). Consequently, many consumers initially attracted to the convenience and flexibility of services like Grokster are now migrating to lawful paid services (services with copying permission) where they can enjoy at little cost even greater convenience and flexibility without engaging in unlawful swapping. See Wu, When Code Isn’t Law, 89 Va. L. Rev. 679, 731–735 (2003) (noting the prevalence of technological problems on unpaid swapping sites); K. Dean, P2P Tilts Toward Legitimacy, wired.com, Wired News (Nov. 24, 2004), http:// www.wired.com/news/digiwood/0,1412,65836,00.html; M. Madden & L. Rainie, March 2005 Data Memo, supra, at 6–7 (percentage of current downloaders who have used paid services rose from 24% to 43% in a year; number using free services fell from 58% to 41%).

Thus, lawful music downloading services—those that charge the customer for downloading music and pay royalties to the copyright holder—have continued to grow and to produce substantial revenue. See Brief for Internet Law Faculty as Amici Curiae 5–20; Bruno, Digital Entertainment: Piracy Fight Shows Encouraging Signs (Mar. 5, 2005), available at LEXIS, News Library, Billboard File (in 2004, consumers worldwide purchased more than 10 times the number of digital tracks purchased in 2003; global digital music market of $330 million in 2004 ex-
pected to double in 2005); Press Release, Informa Media Report, supra (global digital revenues will likely exceed $3 billion in 2010); Ashton, [International Federation of the Phonographic Industry] Predicts Downloads Will Hit the Mainstream, Music Week, Jan. 29, 2005, p. 6 (legal music sites and portable MP3 players “are helping transform the digital music market” into “an everyday consumer experience”). And more advanced types of non-music-oriented P2P networks have also started to develop, drawing in part on the lessons of Grokster.

Finally, as Sony recognized, the legislative option remains available. Courts are less well suited than Congress to the task of “accommodat[ing] fully the varied permutations of competing interests that are inevitably implicated by such new technology.” Sony, 464 U. S., at 431; see, e.g., Audio Home Recording Act of 1992, 106 Stat. 4237 (adding 17 U. S. C., ch. 10); Protecting Innovation and Art While Preventing Piracy: Hearing Before the Senate Comm. on the Judiciary, 108th Cong., 2d Sess. (July 22, 2004).

I do not know whether these developments and similar alternatives will prove sufficient, but I am reasonably certain that, given their existence, a strong demonstrated need for modifying Sony (or for interpreting Sony’s standard more strictly) has not yet been shown. That fact, along with the added risks that modification (or strict interpretation) would impose upon technological innovation, leads me to the conclusion that we should maintain Sony, reading its standard as I have read it. As so read, it requires affirmance of the Ninth Circuit’s determination of the relevant aspects of the Sony question.

* * *

For these reasons, I disagree with JUSTICE GINSBURG, but I agree with the Court and join its opinion.
§ 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching.—

(1) Limitation on liability.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person;
and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions.— The conditions referred to in paragraph (1) are that—

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology—

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its
system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if—

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information Residing on Systems or Networks At Direction of Users.—

(1) In general.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent.— The limitations on liability
established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification.—

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)

(i) Subject to clause (ii), a notification from a
copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information Location Tools.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—

(1) 
(A) does not have actual knowledge that the material or activity is infringing;
(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on Liability of Nonprofit Educational Institutions.—
(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if—

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations.— Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.—

(1) No liability for taking down generally.— Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.
(2) Exception.— Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider—

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider’s system or network.

(3) Contents of counter notification.— To be effective under this subsection, a counter notification must be a written communication provided to the service provider’s designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber’s name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber’s address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability.— A service provider’s compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection
(h) Subpoena To Identify Infringer.—

(1) Request.— A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request.— The request may be made by filing with the clerk—

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena.— The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena.— If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena.— Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena.— Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for Eligibility.—

(1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider—

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition.— As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and—

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions.— The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief.—

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following
forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider’s system or network who is using the provider’s service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.— The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider’s system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders.— Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider’s communications network.

(k) Definitions.—

(1) Service provider.—

(A) As used in subsection (a), the term “service provider” means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term “service provider” means a provider of online
services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary relief.— As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(1) Other Defenses Not Affected.— The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of Privacy.— Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction.— Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.
I. INTRODUCTION

This matter comes before the Court on cross motions for summary judgment and partial summary judgment filed by plaintiff, Corbis Corporation ("Corbis") and defendant, Amazon.com, Inc. ("Amazon"). For the reasons set forth in this Order, the Court finds that Amazon is protected from liability for copyright infringement occurring on its third party vendor platform, zShops.com. In addition, the Court finds that it lacks subject matter jurisdiction over infringement claims regarding photographs for which Corbis has not obtained copyright registration. Finally, the Court finds that Corbis's federal antitrust and state law claims fail as a matter of law.

In accord with these findings, the Court:

Grants Amazon's Motion for Summary Judgment Under the Digital Millennium Copyright Act (Dkt. # 132) ("Def.'s DMCA Mot.");
II. BACKGROUND

A. Procedural Background.

On June 30, 2003, Corbis filed suit against Amazon and 15 other defendants (the "vendor defendants"). Corbis alleges it holds copyright interests in two photographs that Amazon placed on the website IMDb.com and in hundreds of photographs that were being sold by the vendor defendants on Amazon's website. Because Corbis did not grant permission to use the photos, it claims that Amazon directly and vicariously infringed Corbis's copyright interests in violation of 17 U.S.C. §§ 106 & 501 (the "Copyright Act"), engaged in unfair competition in violation of 15 U.S.C. § 1125(a) (the "Lanham Act") and R.C.W. 19.86.020 et seq. (the "Consumer Protection Act"), diluted Corbis's trademarks in violation of 15 U.S.C. § 1125(c) (the "Trademark Act"), and tortiously interfered with Corbis's business relations.

As of September, 2004, Corbis had reached a resolution with each of the vendor defendants, leaving Amazon as the sole remaining defendant. Amazon, for its part, denies the allegations and asserts, as an affirmative defense, that it is immune from liability for copyright infringement under Title II of the Digital Millennium Copyright Act ("DMCA"), 15 U.S.C. § 512, et seq. In addition, Amazon has filed a counterclaim for declaratory relief.

B. Factual Background.

1. Amazon's zShops Platform.

Amazon is a company specializing in electronic commerce. It is most widely known for selling books over the Internet at its website, Amazon.com. The Amazon.com website also hosts several third party vendor platforms, including a platform entitled "zShops." Amazon launched

\[1\]

Amazon hosts two other third party vendor platforms at the Amazon.com website. The "Marketplace" platform allows vendors to sell new, used, or collectible versions of items already sold by Amazon. The "Auctions" platform allows vendors to sell items through an online bidding process. Corbis's allegations focus on the zShops platform. Corbis does not allege that its copyrights have been violated by the selling of items on Auctions or Marketplace.
the zShops platform in the fall of 1995. The zShops platform allows individuals and retailers (referred to as "vendors") to showcase their products and sell them directly to online consumers. Amazon, however, does not sell any of its own inventory on the zShops platform.

To sell on zShops, a vendor creates a web page on the zShops platform that includes information regarding the product being sold. These web pages are referred to as "listings," and are created by using tools and forms provided by Amazon. The forms allow the vendor to describe the product, list the price, and provide an image of the product. A vendor can include a product image in the listing in one of two ways. The vendor either creates a link to an image stored on the vendor’s computer or server, or uploads an image to one of Amazon.com’s servers for display in the listing. Amazon does not actively participate or supervise the uploading or linking of images, nor does Amazon preview the images before the link is created or the upload completed.

Although vendors may accept any variety of payment for their products, if buyers pay by credit, Amazon requires vendors to use its services for processing credit card transactions. Amazon describes its credit card processing service as merely facilitating the monetary exchange between the online buyer and vendor and asserts that it does not conduct the sale of the products offered by the vendors. If the product is paid for by other means, Amazon has no involvement in the transaction.

Vendors must register with Amazon before they list items on zShops. Amazon charges a fee of $39.99 to all vendors, which allows a vendor to use the zShops platform and Amazon’s credit card processing services. Vendors also pay Amazon a percentage of the price of any products sold. The percentage ranges from 2.5% to 5%, depending on the price of the item.

As part of the registration, vendors must also enter into a Participation Agreement, which states that all vendors are bound by its terms as well as the terms set forth in all policies and guidelines for the zShops site. The Participation Agreement prohibits vendors from listing or
linking to any item that

(a) infringes any third-party intellectual property rights (including copyrights, trademark, patent, and trade secrets) or other proprietary rights (including rights of publicity or privacy); ...; or (c) is counterfeited, illegal, stolen, or fraudulent.


In addition, vendors are required to abide by the “Community Rules” set forth in the “Help Section” of the Amazon.com site. The Community Rules state that:

Copies, dubs, duplicates, or transfers of books, music, videos, television programs, radio programs, concerts, DVDs, software, etc., are prohibited. Recopied media infringe upon copyrights and trademarks and are illegal to sell. Just as you cannot sell a photocopied book without the author’s permission, you cannot sell copies or duplicates of videos, music, video games, software, photos, or any copyrighted material without permission of the copyright holder.

Id. at 39a. The Community Rules also make reference to, and state that they are incorporated in, the Participation Agreement. See id. at 38.

In more than one section of the Participation Agreement, Amazon asserts the right to remove listings and terminate services for violations of either the Participation Agreement or Amazon’s policies. For example, the Participation Agreement states that:

Amazon.com has the right, but not the obligation, to monitor any activity and content associated with this site. Amazon.com may investigate any reported violation of its policies or complaints and take any action that it deems appropriate. Such action may include, but is not limited to, issuing warnings, suspension or termination of service, denying access, and/or removal of any materials on the [Amazon.com site], including listings and bids. Amazon.com reserves the right and has absolute discretion to remove, screen, or edit any content that violates these provisions or is otherwise objectionable.

Id. at ¶¶ 20-21, p. 34. The Participation Agreement contains a blanket reservation of Amazon’s right, “in its sole discretion . . . to terminate this Participation Agreement, access to the [Amazon.com site] or the [auction or selling services], or any current auctions or fixed price sales immediately without notice for any reason.” Id. at ¶ 22, p. 36.

Amazon has established a designated agent responsible for receiving claims of infringement of intellectual property rights. See id. at ¶ 24. Contact information for the agent
has been provided to the Copyright Office and is available on Amazon’s website, including on
the zShops platform.

When Amazon receives information that a vendor may be infringing another’s copyrights,
Amazon’s practice is to cancel the allegedly infringing listing and send an e-mail to the vendor.
The e-mail notifies the vendor of the cancellation, identifies a contact e-mail address for the
complaining party, and reminds the vendor that “repeated violations of our Community Rules
could result in permanent suspension from our Auction, zShops, and Amazon Marketplace
sites.” Id. at ¶ 25; Dkt. # 148, Decl. of Claire L. Keeley in Supp. of Pl.’s Mots. for Summ. J.
(“Keeley Decl.”), at 173.

The zShops platform contains approximately 40 million listings of items for sale. From
October 2003 to March 2004, Amazon cancelled over one million listings on its zShops and
Auctions platforms for violations of the Participation Agreement. See Orpet Decl. at ¶ 26.
During that same period, Amazon terminated almost 1,000 vendors for repeat or egregious
violations of the Participation Agreement or Community Rules. See id. at ¶ 26.

When Amazon first launched zShops in 1999, it contacted some vendors to invite them to
list products on the platform. Two of these vendors, Ricks Movie Graphics and Pix Posters,
Inc., were invited to sell their collections of movie posters on zShops. Amazon did not ask
whether these companies also sold celebrity portraits. A representative from Ricks Movie
Graphics stated that during one of these conversations he told Amazon that Ricks Movie
Graphics did not own the copyrights to any of the movie posters it sold but that he believed
Ricks Movie Graphics had the right to sell everything in its inventory. See Keeley Decl. at 46-
47. Ricks Movie Graphics and Pix Posters, Inc. were named as vendor defendants in this suit.
Other vendor defendants assert that they were never contacted by Amazon regarding opening a
zShops site.
2. The IMDb.com Website.

Amazon also owns and operates the Internet Movie Database (IMDb), a website located at www.IMDb.com. IMDb is an information database regarding movies, actors, and entertainment in general. Amazon acquired IMDb in the late 1990s. Although the IMDb site is independent from the Amazon.com site and its third party selling platforms, IMDb contains links to items available on the Amazon.com site. For instance, IMDb contained a banner advertisement with celebrity photos including two photos in which Corbis claims a copyright interest. IMDb users who clicked on the banner were linked to zShops and provided with information regarding vendors selling celebrity images.


Corbis is in the business of licensing art images and photographs, including photographs of celebrities. As part of its business, Corbis enters into contracts with photographers who take celebrity photos. Under these contracts, Corbis represents and distributes a photographer’s work and, in exchange, is paid a royalty based on the fees charged for licensing the photos. Corbis also owns exclusive rights to a number of individual photographs and photographic collections.

Corbis maintains a copyright registration program for itself and the photographers it represents. Corbis receives approximately 100,000 images a year from photographers for review and syndication. If the photographs are not already in digital format, Corbis converts each of them into a digital image. For some of the images, Corbis employees will add “metadata” to the digital image, such as key words describing the image, photographer, and subject. Corbis employees will also add visual enhancements to the image. Every week, Corbis places the images it has received on a computer generated CD-ROM. At regular intervals, Corbis will prepare a copyright application for the group of images on the CD-ROM. It submits the CD-
CORBIS has identified a total of 232 images (the "Corbis Images") in which it claims a copyright interest. Two of the images appeared on the IMDb website. The remaining 230 images have been copied, displayed, and sold by vendor defendants through their zShops sites.

When, in February 2003, Corbis first learned that its images were appearing on zShops, it did not tell Amazon or any of the zShops vendors that displaying and selling the Corbis Images infringed Corbis's copyright interests. Corbis first provided Amazon and the zShops vendors with notice of infringement when Corbis filed and served the Complaint in June, 2003.

Upon receiving the Complaint, Amazon terminated the identified accounts of all of the vendor defendants listed in the Complaint and removed the allegedly infringing images on IMDb. Since its account was terminated, one of the vendor defendants, Posternow, GmbH (also d/b/a Faust Multimedia) ("Posternow"), has opened at least two different vendor accounts with zShops under slightly different names. These accounts were terminated by Amazon once Amazon was made aware of the their existence.

2 At times, Corbis will register an image or a group of images on behalf of a photographer. This process will occur in much the same fashion as the bulk registration described above. In addition, some of the photographers represented by Corbis file their own copyright registrations. In those instances, it is Corbis's practice to obtain a copy of the registration from the photographer.

3 There are three types of copyright interests at issue. First, Corbis asserts the copyright interests of the photographers who took the photos. See Def.'s Mot. for Partial Summ. J. on Copyrights and Copyright Misuse, at 4-5. Second, Corbis asserts a derivative copyright interest in all images to which it has added digital enhancements, metadata, or keywords. See id. Third, Corbis contends that the bulk CD-ROM filings submitted to the Copyright Office contain a unique compilation of the photographs, and asserts a copyright interest in those compilations. See id. Of the 232 images, 49 are subject only to Corbis's derivative and compilation copyright interests. See id. at 2. 102 images are subject only to the photographers' copyright interests that are being pursued by Corbis. See id. The remaining 81 images are subject to both Corbis's and the photographers' copyright interests. See id.
III. DISCUSSION

This Section is broken into four subsections. Subsection A addresses whether the DMCA protects Amazon from copyright liability for the 230 Corbis Images displayed by the vendor defendants. Subsection B addresses whether this Court has subject matter jurisdiction over copyright infringement claims if the photograph in question has not been registered by the Register of Copyrights. Subsection C addresses Corbis’s motion for summary judgment with regard to direct copyright infringement of photographs on IMDb. Subsection D addresses Corbis’s Lanham Act and state law claims.

In reaching its conclusions, the Court has been mindful that summary judgment is proper only if “the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(e). When, as here, parties submit cross-motions for summary judgment, this Court must review the evidence submitted in support of each cross-motion and consider each party’s motions on their own merits. See Fair Housing Council of Riverside County, Inc. v. Riverside Two, 249 F.3d 1132, 1136 (9th Cir. 2001). This Court must examine each set of evidence in the light most favorable to the non-moving party. See U.S. v. Diebold, Inc., 369 U.S. 654, 655, 82 S.Ct. 993, 8 L.Ed.2d 476 (1962).

A. Amazon’s Protection from Copyright Liability Under the DMCA.

Corbis alleges that Amazon infringed its copyrights in 230 Corbis Images that were displayed by the zShops vendors. Amazon has asserted that the DMCA protects it from liability for these alleged copyright violations. Although it may seem premature to address Amazon’s DMCA defense before first determining whether Amazon has violated Corbis’s copyrights in the 230 zShops images, such an approach makes sense under the circumstances. The DMCA gives an Internet service provider (“ISP”) extensive protection against liability, and leaves copyright owners with only limited injunctive relief. As discussed more fully below, the Court finds that

ORDER REGARDING
SUMMARY JUDGMENT MOTIONS

-9-
Amazon is protected from damages sought by Corbis for the alleged infringement of its copyrights in the images displayed by zShops vendors. The relief sought by Corbis for the alleged infringements is prohibited under the DMCA. As a result, even if Corbis’s copyright infringement claims can bare fruit, Amazon’s liability protection ensures that the claims will whither on the vine.

1. Overview of the DMCA

In 1998, Congress enacted the DMCA in an effort to resolve the unique copyright enforcement problems caused by the widespread use of the Internet. See Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004); In re Aimster Copyright Litigation, 334 F.3d 643, 655 (7th Cir. 2003); DMCA, Pub. L. No. 105-304, 112 Stat. 2860 (1998). Tackling copyright infringement on the Internet required balancing the competing interests of several groups. The first set of competing interests includes those of copyright holders and end users. The DMCA “intended to ‘balance the need for rapid response to potential infringement with the end-users’ [sic] legitimate interests in not having material removed without recourse.” Rossi v. Motion Picture Assoc. of America, No. 03-16034, slip op. 16421, 16427 (9th Cir. Dec. 1, 2004) (quoting S. Rep. No. 105-190, at 21 (1998) (alterations in original)). The second set of competing interests were those of copyright holders and ISPs whose services may be used to infringe copyrights. The DMCA intended to balance the interests of these parties by creating a mechanism for rights holders to inform ISPs of potentially infringing conduct while, at the same time, providing “greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.” Ellison, 357 F.3d at 1076 (quoting S. Rep. No. 105-190, at 20 (1998); H.R. Rep. No. 105-551, pt. 2, at 49 (1998)).

This balancing effort resulted in a statute that creates “strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital network environment.” Rossi, No. 03-16034 at slip op. 16427 (quoting H.R. Rep. No. 105-551, pt. 2, at 49 (1998)). For instance, a copyright owner who suspects that
her copyright is being infringed "must follow the notice and take down provisions set forth in § 512(c)(3) of the DMCA." Id. at slip op. 16427–28. Once properly notified, a service provider must "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing." Recording Industry Ass'n of America v. Verizon Internet Servs., 351 F.3d 1229, 1234 (D.C. Cir. 2003). If a service provider fails to take down the potentially infringing material, it exposes itself to copyright liability.

In addition to these notice and take down provisions, the DMCA also establishes several "safe harbors" that protect certain common activities of ISPs. See S. Rep. No. 105-190, at 19; H.R. Rep. No. 105-551, pt. 2, at 41-42. The DMCA safe harbors do not render a service provider immune from copyright infringement. See Ellison, 357 F.3d at 1077. They do, however, protect eligible service providers from all monetary and most equitable relief that may arise from copyright liability. See id.; 17 U.S.C. § 512(a)-(d), (j). Thus, even if a plaintiff can show that a safe harbor-eligible service provider has violated her copyright, the plaintiff will only be entitled to the limited injunctive relief set forth in 17 U.S.C. § 512(j). See 17 U.S.C. §§ 512(a)-(d), (j); Verizon Internet Servs., 351 F.3d at 1234.

The DMCA "safe harbors provide protection from liability for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools." Ellison, 357 F.3d at 1076-1077 (citing 17 U.S.C. §§ 512(a)-(d)).

To be eligible for any of the safe harbors, a service provider must meet a series of threshold conditions. At the outset, a party seeking safe harbor must, in fact, be a "service provider" as that term is defined under the DMCA. See 17 U.S.C. § 512(k)(1)(B). If it fits within that definition, the service provider must then show that it

(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

ORDER REGARDING SUMMARY JUDGMENT MOTIONS
(B) accommodates and does not interfere with standard technical measures.\textsuperscript{4}

17 U.S.C. § 512(i); accord Ellison, 357 F.3d at 1080. A service provider that does not meet
these threshold conditions may not invoke the DMCA’s safe harbor limitations on liability. See
Ellison, 357 F.3d at 1080.

Once the threshold conditions have been met, a service provider must then satisfy the
specific requirements for the particular safe harbor. Amazon asserts that it is entitled to
protection for information residing on systems or networks at the direction of users. See 17
U.S.C. § 512(c). The § 512(c) safe harbor protects a service provider from liability 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." To qualify
for the § 512(c) safe harbor, a service provider must show that:

(1) it has neither actual knowledge that its system contains infringing materials nor
an awareness of facts or circumstances from which infringement is apparent, or it
has expeditiously removed or disabled access to infringing material upon obtaining
actual knowledge of infringement;

(2) it receives no financial benefit directly attributable to infringing activity; and

(3) it responded expeditiously to remove or disable access to material claimed to
be infringing after receiving from the copyright holder a notification conforming
with requirements of § 512(c)(3).

ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 623 (4th Cir. 2001) (citing 17
U.S.C. § 512(c)(1)). Corbis, for its part, asserts that Amazon does not qualify for liability
protection both because it does not satisfy the threshold conditions and because it does not meet
the § 512(c) requirements.

\textsuperscript{4}The term “standard technical measures” refers to technical means by which copyright
owners may identify or protect copyrighted works. See Ellison, 357 F.3d at 1080.
2. Threshold Conditions for DMCA Liability Protection.

a. Is Amazon a "Service Provider" Under the DMCA?

Protection from copyright liability under the DMCA is only available to entities that meet the statute's definition of a "service provider." See 17 U.S.C. § 512(k)(1). For purposes of the § 512(c) safe harbor, a "service provider" is defined as "a provider of online services or network access, or the operator of facilities therefor." See 17 U.S.C. § 512(k)(1)(B). This definition encompasses a broad variety of Internet activities, see e.g., Aimster, 334 F.3d at 655; ALS Scan, 239 F.3d at 623, and there is no doubt that Amazon fits within the definition. See Hendrickson v. Amazon.Com, 298 F.Supp.2d 914, 915 (C.D. Cal. 2003) (holding that Amazon meets the DMCA's definition of a service provider). Amazon operates web sites, provides retail and third party selling services to Internet users, and maintains computers to govern access to its web sites. These activities fall squarely within the broad scope of the § 512(k)(1)(B) definition of "service provider." See e.g., Hendrickson v. eBay, Inc., 165 F.Supp.2d 1082, 1088 (C.D. Cal. 2001) (eBay, an operator of an Internet website for purchase and sale of consumer goods, qualifies as a service provider).

b. Has Amazon Adopted and Reasonably Implemented a User Policy?

The Ninth Circuit has held that the DMCA's infringement policy requirement has three

---

5The DMCA also provides a different, more restrictive, definition of "service provider." See 17 U.S.C. § 512(k)(1)(A). This definition only applies to entities seeking protection from liability under the "transitory digital network communications" safe harbor. See 17 U.S.C. § 512(a). The more restrictive definition does not apply to an entity, such as Amazon, that seeks protection under the "information residing on systems or networks at the direction of users" safe harbor. See 17 U.S.C. § 512(k)(1)(B).

6Corbis argues that Amazon is not a service provider because Amazon does not "serve to route or connect online digital communications." Dkt. # 175, Pl.'s Opp. to Def.'s DMCA Mot. at 7. This argument is unavailing. The relevant definition of service provider does not require Amazon to engage in such activity. See 17 U.S.C. § 512(k)(1)(B).
prongs. See Ellison, 357 F.3d at 1080. A service provider must: 1) adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances; 2) inform users of the service policy; and 3) implement the policy in a reasonable manner. See id. As discussed below, Amazon has satisfied each of the three Ellison prongs.

i. **Amazon Has Adopted a User Policy.**

It is undisputed that Amazon requires each zShops vendor to accept a Participation Agreement that sets forth guidelines for the use of the zShops platform. See Pl.’s § 512(i) Mot. at 3. Nevertheless, Corbis argues that Amazon has not adopted an infringement policy under § 512(i). Corbis’s primary complaint is that the Participation Agreement and related policies are too vague with regard to issues of copyright infringement. For example, Corbis points out that Amazon’s user policies do not include the term “repeat infringer” and do not describe the methodology employed in determining which users will be terminated for repeated copyright violations. Corbis asserts that without such information, Amazon has not sufficiently informed its users of the type of conduct that will cause them to be denied access to Amazon’s services.

The language of § 512(i) and the overall structure of the DMCA indicate that the user policy need not be as specific as Corbis suggests. The language of § 512(i) is telling in this regard. The key term, “repeat infringer,” is not defined and the subsection never elaborates on what circumstances merit terminating a repeat infringer’s access. This open-ended language contrasts markedly with the specific requirements for infringement notices and take-down procedures set forth in § 512(c). See Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003), cert. denied, ___ U.S. ___, 124 S.Ct. 2812, 159 L.Ed.2d 246 (2004). The notice and take-down provisions demonstrate that Congress infused the statute with specific detail when it so chose.

The fact that Congress chose not to adopt such specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.

The open-ended language makes sense given the overall structure of the DMCA. In its
recent discussion of the DMCA, the Ninth Circuit reminded that "the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." Rossi, No. 03-16034 at slip op. 16431 (quoting The Wilderness Soc. v. U.S. Fish & Wildlife Servs., 353 F.3d 1051, 1060 (9th Cir. 2003) (en banc), amended by 360 F.3d 1374 (9th Cir. 2004)). The DMCA's balancing efforts reflect an understanding that "there are different degrees of online copyright infringement, from the inadvertent to the noncommercial, to the willful and commercial." S. Rep. No. 105-190, at 32; H.R. Rep. No. 105-551, pt. 2, at 44. Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, ex ante, the specific types of conduct that will merit restricting access to its services. As Congress made clear, the DMCA was drafted with the understanding that service providers need not "make difficult judgments as to whether conduct is or is not infringing." See id.

This does not mean that the first prong of the Ellison test is a paper tiger. To the contrary, it is clear that a properly adopted infringement policy must convey to users that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others . . . know that there is a realistic threat of losing that access." Id. Amazon's policies convey this message. Each vendor must agree to the terms of the Participation Agreement before selling on the zShops platform. See Pl.'s 512(i) Mot. at 3. The Participation Agreement prohibits the listing, linking, or posting of any material that violates copyright laws, see Orpet Decl. at ¶ 9, p. 30, and makes it clear that those who violate Amazon's policies may face a variety of penalties, including restricting access to Amazon's sites and suspension or termination of service, see id. at ¶¶ 20-21, pp. 32-34. Finally, and perhaps most importantly, those accused of copyright infringement are informed that repeated violations could result in "permanent suspension" from Amazon sites. See Keeley Decl. at 173. Although Amazon does not use the term "repeat infringer" or precisely track the language of the DMCA, the evidence shows that Amazon has adopted a termination policy as required under § 512(i).
ii. Amazon Has Communicated Its Termination Policy to Its Users.

Although the evidence indicates that Amazon required users to enter into the Purchase Agreement and accept the Community Rules, Corbis asserts that Amazon has not communicated its infringement policy to its users. See Dkt. # 205, Reply in Supp. of Pl.’s 512(i) Mot. ("512(i) Reply") at 8. Corbis argues that Amazon had two policies, one it presented to users in the form of the Participation Agreement and Community Rules and a second, internal policy that was not described in the agreements and rules presented to vendors. See id. at 8. The internal policy Corbis refers to is a set of criteria used by Amazon when determining whether to terminate a user’s access to the site. Corbis argues that these internal criteria make up Amazon’s actual policy on infringement. Since the internal criteria were never communicated to users, Corbis argues, Amazon has failed to satisfy this prong of the Ellison test.

Section 512(i), however, is not so exacting. Amazon need only inform users that, in appropriate circumstances, it may terminate the user’s accounts for repeated copyright infringement. See, e.g., In re Aimster Copyright Liability, 252 F.Supp.2d 634, 659 (N.D. Ill. 2002), aff’d, 334 F.3d 643 (8th Cir. 2004) (policy communicated when users informed they “may have their access to all services terminated” for repeated copyright violations) (emphasis added); Perfect 10, Inc. v. CCBill, LLC, 340 F.Supp.2d 1077, 1088-89 (C.D. Cal. 2004) (policy stating user’s access may be terminated deemed sufficient communication). The statute does not suggest what criteria should be considered by a service provider, much less require the service provider to reveal its decision-making criteria to the user. Amazon need only put users on notice that they face exclusion from the service if they repeatedly violate copyright laws. Amazon has done so, and has satisfied this prong of the Ellison test.

iii. Amazon Has Reasonably Implemented Its Infringement Policy.

The final Ellison prong requires Amazon to reasonably implement its infringement policy. See Ellison, 357 F.3d at 1080; 17 U.S.C. § 512(i)(A). Section 512(i) provides little guidance on what constitutes reasonable implementation of an infringement policy. Cases that have
addressed this issue generally raise two questions. The first is whether the service provider
adopted a procedure for receiving complaints and conveying those complaints to users. See id.
If such a procedure has been adopted, then the second question is whether the service provider
nonetheless still tolerates flagrant or blatant copyright infringement by its users. See Perfect 10,

(a) Procedure for Receiving and Conveying Complaints.

In Ellison, the Ninth Circuit addressed the first question, regarding procedural
implementation of an infringement policy. See Ellison, 357 F.3d at 1080. The Court analyzed
America Online Inc.'s ("AOL's") infringement policy and identified flaws in how the policy had
been implemented. At the time of the allegedly infringing activity, AOL had changed the e-mail
address to which infringement notifications were to be sent but did not forward messages sent to
the old address or notify senders that the old e-mail address was inactive. Instead, "AOL
allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded."
Id. Because of this flawed notification procedure, the Court found that it was "difficult to
conclude as a matter of law . . . that AOL had "reasonably implemented" a policy against repeat
infringers." Id.

The Northern District of Illinois reached a similar conclusion in Aimster, 252 F.Supp.2d
at 659. When determining whether a repeat infringer policy had been reasonably implemented,
the court focused on whether the policy allowed the service provider to communicate
infringement notices to the service users. In Aimster, defendant had adopted a repeat infringer
policy but, because of defendant's own encryption system, could not identify infringing users.
The court held that defendant's repeat infringer policy had not been properly implemented. As
the court noted, "adopting a repeat infringer policy and then . . . eviscerating any hope that such
a policy could ever be carried out is not an 'implementation' as required by § 512(i)." Id.

Here, the evidence indicates that Amazon developed a sufficient procedure for
implementing its infringement policy. It is undisputed that Amazon's 2Shops platform includes
over 40 million listings. See Orpet Decl. at ¶ 27. Amazon has cancelled millions of listing for violations of its user policies. See id. at ¶ 26. Amazon notifies the vendor of the cancellation through e-mail and warns that repeated violations of the rules may result in “permanent suspension” from Amazon sites. See Keeley Decl. at 173. In addition, Amazon has terminated access to zShops for hundreds of vendors for egregious or repeated violations of its user policies. See Orpet Decl. at ¶ 26.

Corbis points out that these figures do not differentiate between action taken for copyright infringement and action taken for other policy violations. The evidence, however, indicates that Amazon does respond to allegations of copyright infringement. See Keeley Decl. at ¶ 15, pp. 123-131. Amazon’s practice is to promptly cancel a listing once it receives adequate notice that the listing violates another’s copyrights. See Keeley Decl. at 105-106. Amazon informs the listing vendor via e-mail that “your listing may have violated the intellectual property rights of others and the Community Rules that govern our Auction, zShops, and Amazon Marketplace sites.” Orpet Decl. at ¶ 25. The e-mail also provides the vendor with the complaining party’s contact information. See id. Finally, as with other cancellations, Amazon warns vendors that repeated violations may result in permanent suspension from the Amazon site. See Orpet Decl. at ¶ 25. This evidence indicates that Amazon has properly implemented a procedure for addressing copyright complaints and enforcing violations of its policies.

As Corbis points out, however, Amazon’s infringement policy has not been able to prevent certain vendors from reappearing on the zShops platform under pseudonyms. Even though Amazon’s policies prohibit vendors from opening new accounts once the original account has been terminated, see Keeley Decl. at 95, Posternow has been able to open at least two new accounts under slightly different names since it was initially terminated in June 2003. See Dkt. # 191, Decl. of Claire Keeley in Supp. of Opps. to Summ. J. Mot. (“Keeley Opp. Decl.”), at 651-655.

Although this type of behavior is understandably vexing for a copyright holder like
Corbis, it is not clear how Posternow's efforts to sidestep Amazon's policies amount to a failure of implementation. Corbis has not alleged that Amazon intentionally allowed Posternow to open a zShops account or suggested that a more effective means of denying Posternow's access could have been implemented by Amazon. Compare A&M Records, Inc. v. Napster, Inc., 2000 U.S. Dist. LEXIS 6243, *28-29; 2000 WL 573136, *9 (N. D. Cal. 2000) (expert evidence that additional measure to thwart repeat violations could have been taken).

Instead, Corbis merely asserts that Posternow's reappearance shows that the infringement policy is a failure. This argument, however, fails to pass summary judgment muster. Corbis is required to present "specific facts showing that there is a genuine issue for trial." Celotex Corp. v. Catrett, 477 U.S. 317, 323, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986). An infringement policy need not be perfect; it need only be reasonably implemented. See CCBill 340 F.Supp.2d at 1089. Here, Corbis has not brought forth any facts to suggest that Amazon could have used another, more effective and reasonable, method for preventing disingenuous users from re-accessing zShops. In Napster, by comparison, the copyright holder plaintiffs avoided summary judgment on § 512(i) by providing expert testimony that Napster could have kept terminated users from re-accessing the service by blocking the user's Internet protocol address. See Napster, 2000 U.S. Dist. LEXIS 6243, *28-29; 2000 WL 573136, *9. Corbis's silence in this regard is telling. The mere fact that Posternow appeared on zShops under a different user name and identity does not, by itself, create a legitimate question of fact regarding the procedural implementation of Amazon's termination policy.

(b). Tolerating Flagrant or Blatant Copyright Infringement.

Even with proper enforcement procedures, a copyright holder may still demonstrate that

In some respects, the evidence regarding Posternow's efforts to continue to sell on zShops suggests that Amazon's procedures for dealing with repeat infringers are properly implemented. Each time that Amazon has been made aware of Posternow's pseudonymous zShop sites, Amazon has immediately cancelled the listings and terminated the account.
the service provider has not satisfied § 512(i) if there are specific instances demonstrating that
the service provider tolerates repeat copyright infringement by its users. As § 512(i) makes
clear, however, termination of a user because of repeated copyright infringement is required only
in “appropriate circumstances.” See 17 U.S.C. § 512(i). Amazon need not conduct active
investigation of possible infringement or make a decision regarding difficult infringement issues.
See Cybernet, 213 F.Supp.2d at 1176-77. Because it does not have an affirmative duty to police
its users, failure to properly implement an infringement policy requires a showing of instances
where a service provider fails to terminate a user even though it has sufficient evidence to create
actual knowledge of that user’s blatant, repeat infringement of a willful and commercial nature.
See Cybernet, 213 F.Supp.2d at 1177; see also, Costar Group Inc. v. Loopnet, Inc., 164
F.3d 544 (4th Cir. 2004).

Corbis identifies two specific vendors that it believes typify Amazon’s failed
implementation – Famed & Framed and Posternow. Corbis provides evidence that, between
October, 2002 and February, 2003, Amazon received three e-mails in which the sender claimed
that zShops listings posted by Famed & Framed violated the sender’s copyrights. See Pl.’s
512(i) Mot. at 6-7. Similarly, between June, 2002 and February, 2003, Amazon received seven
e-mails in which the sender claimed that zShops listings posted by Posternow violated the
sender’s copyrights. See id. at 7. Both Famed & Framed and Posternow were vendor
defendants in this lawsuit.8 Amazon did not terminate either party’s access to zShops until after
this suit was filed. See Orpet Decl. at ¶ 30.

The Famed & Framed and Posternow examples do not provide evidence that Amazon had
knowledge of blatant, repeat infringement that would have required Amazon to terminate access

8None of the e-mails to Amazon in which the senders complained that Famed & Framed
or Posternow were infringing copyrights were sent by Corbis or its representatives.
to the vendors’ zShops sites. Although efforts to pin down exactly what amounts to knowledge
of blatant copyright infringement may be difficult, it requires, at a minimum, that a service
provider who receives notice of a copyright violation be able to tell merely from looking at the
user’s activities, statements, or conduct that copyright infringement is occurring. See Cybernet,
213 F.Supp.2d at 1177. Examples of such blatant infringement may include statements from the
vendor that a product is bootlegged or pirated, see eBay, 165 F.Supp.2d at 1093 n.14, chat rooms
hosted by the service provider in which users discuss how the service can be used to circumvent
copyright laws, see Aimers, 252 F.Supp.2d at 652, or the offering of hundreds of audio files in a
single day for peer to peer copying, see Verizon Internet Servs., 351 F.3d at 1233. Corbis has
presented no such examples of blatant infringing activity on the vendor defendants’ zShops sites.

Corbis argues, however, that the notices regarding infringing items on Famed & Framed
and Posternow were sufficient to show blatant copyright infringement. Even assuming that the
notices complied with the DMCA’s notice requirements, see 17 U.S.C. § 512(c)(3), such notices
are not the sine qua non of copyright liability. See Ellison, 357 F.3d at 1077 (claims for on-line
copyright infringement are evaluated just as they would be in the non-online world). A
copyright owner may have a good faith belief that her work is being infringed, but may still be
wrong. The notification requirement does not take into account that a vendor may have “a
legitimate fair use defense, or can otherwise invoke any of the myriad other factors that go into
evaluating a copyright infringement claim.” 3 Melville B. Nimmer & David Nimmer, NIMMER
ON COPYRIGHT, § 12B.02[B][2], at 12B-36. Although the notices have brought the listings to

—

7 In this regard, this Court respectfully disagrees with CCBill, in which the district court
for the Central District of California held that receipt by the service provider of two or more
DMCA compliant notices about one of its users required termination under § 512(i). See 340
F.Supp.2d at 1088. Although there may be instances in which two or more DMCA compliant
notices make a service provider aware of a user’s blatant, repeat infringement, the notices alone
do not make the user’s activity blatant, or even conclusively determine that the user is an
infringer.

ORDER REGARDING
SUMMARY JUDGMENT MOTIONS -21-
Amazon’s attention, they did not, in themselves, provide evidence of blatant copyright infringement.

Corbis cites testimony from Eric Orpet, Amazon’s quality compliance manager, as evidence that Amazon knew a portion of Posternow’s inventory was infringing based on the notices of infringement. When confronted with the notices of infringement, Mr. Orpet stated that, “based on what has been communicated to us, a small portion of [Posternow’s] inventory would be construed as infringing.” See Keeley Decl. at 118. This statement was made after a discussion in which Mr. Orpet repeatedly asserted that the term “repeat infringer” had not been defined. See id. at 115, 119. In addition, Mr. Orpet asserted that Posternow was not a repeat infringer, but that Amazon had “received repeat violation notification emails” about Posternow. See id. at 122.

In evaluating Mr. Orpet’s statements, the recent Rossi decision is instructive. In Rossi, the Ninth Circuit held that the term “knowing misrepresentation,” as it is used in the DMCA, requires “actual knowledge of misrepresentation.” See Rossi, No. 03-16034 at slip op. 16431. A party does not make a knowing misrepresentation “simply because an unknowing mistake is made, even if [the party] acted unreasonably in making the mistake.” Id. Here, even if Amazon acted unreasonably when it failed to terminate Posternow, that unreasonable act is not the equivalent of having actual knowledge that Posternow was engaged in blatant, repeat infringement. Actual knowledge of blatant, repeat infringement cannot be imputed merely from the receipt of notices of infringement. Instead, there must be additional evidence available to the service provider to buttress the claim of infringement supplied by the notices. Here, Corbis provides no additional evidence that was available to Amazon that would have led Amazon to conclude that Posternow was a blatant, repeat infringer.

In fact, outside of the third party notices, Corbis lacks other evidence that Amazon ignored blatant copyright infringement by Posternow and Famed & Framed. For instance, there is no evidence suggesting that Amazon would have been able to tell, merely by looking at the
Famed & Framed and Posternow listings, that the posters and photos being sold infringed another's copyrights. Without some evidence from the site raising a red flag, Amazon would not know enough about the photograph, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement. See S. Rep. No. 105-190, p. 30 (merely being aware of "one or more well known photographs of a celebrity at a site" does not provide a service provider with knowledge of possible infringement).

With respect to Famed & Framed, Corbis makes much of evidence that Amazon knew that Famed & Framed did not own the copyrights to the posters and images it sold. See Pl.'s 512(c) Mot. at 8. Corbis, however, presents this evidence in a somewhat selective fashion. Corbis neglects to mention that the Famed & Framed representative unequivocally stated that he informed Amazon that Famed & Framed had the right to sell all of the posters in its inventory. See Keeley Decl. at ¶ 10, p. 48. As Corbis is aware, owning a copyright and having the legal right to sell the copyrighted image are two very different things.

In fact, there is at least some evidence to suggest that Posternow and Famed & Framed were not the kind of "repeat infringers" envisioned under § 512(i). As late as July, 2003, Posternow indicated to Amazon that all of its products were officially licensed. See id. at ¶ 25, pp. 170, 171. In addition, there is evidence that Famed & Framed attempted to work with Amazon to ensure that allegedly infringing items did not get re-listed on zShops. See id. at ¶ 26, p. 174. Such assertions by the two users militate against a finding that Amazon turned a blind eye to blatant, repeat infringement. Indeed, for Amazon to determine that these two users were infringers, it would have had to conduct the type of investigation that the courts and the legislature has found unnecessary. See Cybernet, 213 F.Supp.2d at 1176-77.

C. **Does Amazon Accommodate and Not Interfere with Standard Technical Measures?**

Corbis has not challenged Amazon's assertion that it accommodates and does not interfere with standard technical measures used to identify and protect copyrighted works.
Accordingly, this Court finds that this threshold condition has been met.

3. **The Safe Harbor Conditions Under § 512(c).**

Having satisfied the threshold conditions, Amazon must still meet the three conditions for liability protection set forth in § 512(c)(1)(A)-(C). First, Amazon must show that it does not have actual or apparent knowledge that material on its network is infringing. See 17 U.S.C. § 512(c)(1)(A)(i) & (ii). If Amazon does have actual or apparent knowledge, it must show that it acted “expeditiously to remove, or disable access to, the [infringing] material.” 17 U.S.C. § 512(c)(1)(A)(iii). Second, Amazon must show that it does not receive a financial benefit directly attributable to any infringing activity that it maintains the right and ability to control. Third, Amazon must show that it has expeditiously removed or disabled access to allegedly infringing material for which it has received appropriate notice under § 512(c)(3).

Amazon asserts that it has met all the elements necessary to invoke liability protection under § 512(c). Corbis does not challenge Amazon’s claim that it acts expeditiously to remove or disable access to allegedly infringing material in accord with the third safe harbor element. Corbis argues, however, that Amazon does not fulfill the requirements of § 512(c)(1) because (a) it knew or should have known of infringements of Corbis Images by zShops vendors, and (b) it receives a financial benefit directly attributable to the infringing activity and has the right and ability to control such activity.

a. **Knowledge of Infringement.**

To enjoy the § 512(c) safe harbor Amazon must show that it (1) does not have actual knowledge that the material or an activity using the material on the system or network is infringing, and (2) is not aware of facts or circumstances from which infringing activity is apparent. If a service provider does obtain either actual or apparent knowledge, it may still invoke the § 512(c) safe harbor if it acts expeditiously to remove or disable access to the infringing material.

In all of the published cases addressing the knowledge component of § 512(c), the
The copyright holder has provided evidence that it notified the service provider of the infringing material. See, e.g., Ellison, 357 F.3d at 1075 (DMCA compliant notice sent to service provider); ALS Scan, 239 F.3d at 620-21 (pre-suit letter substantially complying with DMCA sent to service provider); Amazon, 298 F.Supp.2d at 915 (plaintiff attempted to notify service provider); eBay, 165 F.Supp.2d at 1084-85 (non-DMCA-compliant cease and desist letters sent); CoStar, 164 F.Supp.2d at 703 (plaintiff sent DMCA notification of claimed infringement). The notice of infringement constitutes evidence of the service provider’s knowledge. Under the DMCA, the service provider may attempt to refute this knowledge by showing that the notice failed to substantially comply with the DMCA’s notice requirements. See 17 U.S.C. § 512(c)(3)(B).

This case differs from other cases addressing the § 512(c) knowledge component. Here, Corbis acknowledges that it never attempted to notify Amazon that zShops vendors were selling images that violated Corbis copyrights. Corbis chose not to address the copyright infringement issues through the DMCA’s notice provisions, but instead decided to file this infringement suit.

Corbis, of course, was under no obligation to give notice of claimed infringement before filing this suit. See H.R. Rep. No. 105-551, pt. 2, at 54. Its decision to forego the DMCA notice provisions, however, stripped it of the most powerful evidence of a service provider’s knowledge – actual notice of infringement from the copyright holder. See 3 NIMMER ON COPYRIGHT, § 12B.04[A][3], at 12B-53.

Corbis asserts that its decision to forego notice is of no import. It proffers evidence of notices provided by other copyright holders addressing non-Corbis photos. In addition, Corbis provides evidence suggesting that Amazon was aware that Corbis licensed celebrity photos. Based on this evidence, Corbis argues that Amazon should have known that zShops vendors sold infringing Corbis Images.

This evidence does not create a material issue of fact regarding either Amazon’s actual knowledge or its apparent knowledge of infringing material on the zShops platform. With regard to actual knowledge, this evidence is wholly insufficient. Taken in the light most

ORDER REGARDING SUMMARY JUDGMENT MOTIONS -25-
favorable to Corbis, the evidence shows that Amazon knew Corbis licensed celebrity photos and that celebrity photos were vulnerable to copyright infringement. The issue is not whether Amazon had a general awareness that a particular type of item may be easily infringed. The issue is whether Amazon actually knew that specific zShops vendors were selling items that infringed Corbis copyrights. Corbis provides no evidence from which such actual knowledge could be gleaned.

Corbis fares little better with regard to demonstrating Amazon's apparent knowledge. Corbis contends that it has provided sufficient evidence to show that Amazon "knew or should have known" that zShops vendors were selling infringing Corbis Images. Corbis, however, misstates the standard of knowledge necessary under § 512(c). In determining whether a service provider is "aware of facts or circumstances from which infringing activity was apparent," 17 U.S.C. § 512(C)(1)(A)(ii), the question is not "what a reasonable person would have deduced given all the circumstances." 3 NIMMER ON COPYRIGHT, § 12B.04[A][1], at 12B-49. Instead, the question is "whether the service provider deliberately proceeded in the face of blatant factors of which it was aware." Id. As articulated by Congress, apparent knowledge requires evidence that a service provider "turned a blind eye to 'red flags' of obvious infringement." H.R. Rep. No. 105-551, pt. 2, at 42.

Congress's discussion of apparent knowledge, and what evidence demonstrates such knowledge, is instructive. Absent evidence of its own efforts to notify a service provider, a copyright owner could establish apparent knowledge if she could show that an online location at which her copyrighted material was available was clearly a "pirate site." Id. Pirate sites are ones that are "obviously infringing because they typically use words such as 'pirate,' 'bootleg' or slang terms in their URL and header information to make their illegal purpose obvious." Id. Congress described the advertisement of illegal copyright activity through such slang words as a "red flag' of obvious infringement," and indicated that the infringing nature of sites containing such red flags would be apparent from even a "brief and casual viewing." Id. Thus, once a
service provider is aware of a site containing such "red flags," the service provider would have apparent knowledge of the infringing activity.

Corbis argues that its strongest evidence regarding apparent knowledge is that Amazon received notices that zShops vendors were infringing the copyrights of unrelated parties by selling celebrity photographs. There are a number of problems with this evidence. First, it is not clear which, if any, of the vendors that were the subject of the third party notices are also vendor defendants in this litigation. Second, notices of infringement must substantially comply with the DMCA's notice requirements to be considered evidence of a service provider's knowledge. See ALS Scan, 239 F.3d at 625; 17 U.S.C. § 512(c)(3)(B)(i). Corbis, however, makes no attempt to suggest that these third party notices were DMCA compliant. Assuming that they did comply, Corbis runs into yet another problem; the notices would still not be considered as evidence of knowledge if Amazon acted expeditiously to cancel the complained of listings. See 17 U.S.C. § 512(c)(1)(C). Amazon has asserted that it promptly cancels a listing after receiving a notice of infringement, and Corbis never directly challenges that assertion.

Sweeping aside these difficulties, the third party notices do not, in themselves, constitute red flags. As Congress suggested, evidence of blatant copyright infringement will often derive from information on the offending site. See, e.g., H.R. Rep. No. 105-551, pt. 2, at 42. Outside of the fact that the zShop vendors sold pictures of celebrities, Corbis is silent regarding the content of the complained of listings. There is simply nothing to suggest that the vendor listings contained evidence of blatant copyright infringement. As a result, even if the notices of infringement would have caused Amazon to examine the content of the zShops sites, Corbis has failed to close the link by showing that those sites contained the type of blatant infringing activity that would have sent up a red flag for Amazon.

Corbis's other evidence of "red flags" is similarly unavailing. Corbis points out that IMDb representatives met with Corbis representatives in 2001 and that Amazon's corporate counsel was employed at Corbis between 1993 and 1998. See Pl.'s 512(c) Mot. at 8-10. Corbis
indicates that these events provide a link between Amazon and Corbis from which apparent knowledge can be inferred. Even ignoring the tentuonsness of these links, it would only suggest that Amazon had general knowledge that photos may be the subject of online copyright infringement. It provides no evidence from which to infer that Amazon was aware of, but chose to ignore, red flags of blatant copyright infringement on specific zShops sites.

b. Amazon Does Not Have the Right and Ability to Control the Infringing Activity.

A service provider will be excluded from the § 512(c) safe harbor if it (1) "has the right and ability to control" the infringing activity, and (2) receives "a financial benefit directly attributable to the infringing activity." 17 U.S.C. § 512(c)(1)(B). Both elements must be met for the safe harbor to be denied. See 3 NIMMER ON COPYRIGHT, § 12.12B.04[A][1], at 12B-50.

One court has already ruled on Amazon's right and ability to control infringing activity on its third party vendor platforms. In Hendrickson v. Amazon.Com, the Central District of California held that Amazon had satisfied this component of § 512(c), finding that Amazon merely provided the forum for an independent third party seller to list and sell his merchandise. Amazon was not actively involved in the listing, bidding, sale or delivery of [the infringing item]. The fact that Amazon generated automatic email responses when the [infringing item] was listed and again when it was sold, does not mean that Amazon was actively involved in the sale. Once a third party seller decides to list an item, the responsibility is on the seller to consummate the sale. While Amazon does provide

10 Representatives from IMDb and Corbis had one meeting in 2000. Although this meeting would have made IMDb aware that Corbis licensed images of celebrities, Corbis does not assert that it made Amazon aware that Corbis faced an infringement threat from any of the zShops vendors. Furthermore, the employee who left Corbis to join Amazon was not involved in acquiring the group of images that are involved in this litigation. See Def.'s Opp. to Pl.'s § 512(c) Mot. at 11. Given that Corbis, itself, had to first conduct an investigation before determining whether zShops vendors were selling unauthorized images, see Dkt. # 188, Decl. of Charles C. Sipos in Supp. of Def.'s Reply to DMCA Mot. ("Sipos Reply Decl."), at ¶ 2, p. 7, it is difficult to imagine that Amazon would have gleaned such knowledge based on these connections.
transaction processing for credit card purchases, that additional
service does not give Amazon control over the sale. In sum,
Amazon's evidence shows that it did not have control of the sale of
the infringing item.

Amazon, 298 F.Supp.2d at 918.

Corbis attempts to distinguish Amazon in two ways. First, Corbis notes that, unlike the
plaintiff in Amazon, Corbis has presented evidence that Amazon was able to identify vendors
and the items sold on the zShops platform. As an example, Corbis notes that Amazon
terminated the zShops defendants on the same day Corbis filed and served its complaint. This
evidence, however, does not suggest a right and ability to control under the DMCA. Courts have
routinely held that "the right and ability to control infringing activity, as the concept is used in
the DMCA, cannot simply mean the ability of a service provider to remove or block access to
materials posted on its website or stored in its system." CCBill, 340 F.Supp.2d at 1098 (citing
Costar, 164 F.Supp.2d at 704). This Court agrees. Merely because Amazon could identify the
zShops defendants and terminate their accounts does not mean they exercised the type of right
and ability to control that would disqualify them from § 512(c) safe harbor.

Second, Corbis notes that Amazon met with several vendors of movie posters when the
zShops site was launched in 1999. Amazon encouraged these vendors to list their items on
zShops. Implicit in this argument is that Amazon knew, or should have known, that movie
poster vendors were solely in the copyright infringement business. As discussed above, there is
no evidence to warrant such a conclusion, much less to impute that knowledge to Amazon.
Without any indication that Amazon intended to pick infringing material for its site, the fact
that it advertised the zShops platform does not amount to a right and ability to control the items
sold there.

Outside of providing the zShops platform, Amazon did not have the right or ability to
control vendor sales. Amazon is never in possession of the products sold by zShops vendors.
See Orpet Decl. at ¶ 9; compare eBay, 165 F.Supp.2d at 1094. Furthermore, Amazon does not
preview the products prior to their listing, does not edit the product descriptions, does not
suggest prices, or otherwise involve itself in the sale. See id.; compare Cybertel, 213 F.Supp. 2d
at 1181-82 (service provider maintains right and ability to control where it prescreens sites, gives
extensive advice regarding content, and prohibits the proliferation of identical sites). The
evidence provided by Corbis does not sufficiently distinguish the previous finding in Amazon.
See 298 F.Supp. 2d at 918.

Because Amazon does not have the right and ability to control the infringing material, it
is not necessary for this Court to inquire as to whether Amazon receives a direct financial benefit
from the allegedly infringing conduct. See CC Bill, 340 F.Supp. at 1098.


Amazon has satisfied all of the threshold conditions for DMCA protection and all of the
requirements for protection under the § 512(c) safe harbor. As a result, Amazon is immune from
all monetary relief and, save the limited relief in 17 U.S.C. § 512(j), all forms of injunctive relief
for any copyright infringement committed by zShops vendors on the Amazon site.11 There is no
genuine issue of material fact that Amazon is entitled to safe harbor protection under § 512(c).

Since the DMCA protects Amazon from liability for the 230 images displayed on the
zShops listings, this Court grants Amazon’s motion for partial summary judgment regarding
Corbis’s claims of direct copyright infringement relating to those 230 images (Dkt. # 153). In
practical terms, the damages and injunctive relief sought by Corbis are no longer available and
the direct infringement claims related to the 230 images on zShops have become moot. See
Seven Words LLC v. Network Solutions, 260 F.3d 1089, 1095 (9th Cir. 2001) (where relief no
longer available, plaintiff’s claim is moot). The only relief Corbis could seek is the limited
injunctive relief set forth in § 512(j) of the DMCA. Corbis has never requested such relief and,

11Amazon has not asserted that DMCA protection applies to Corbis Images that appeared
on IMDb. Accordingly, Corbis’s Motion for Partial Summary Judgment Against Amazon as to
DMCA Eligibility for its IMDb Platform (Dkt. # 144) is granted.

ORDER REGARDING
SUMMARY JUDGMENT MOTIONS

253
considering that Amazon has asserted that it has terminated the accounts of the defendant vendors, it is not certain how the limited injunctive relief would apply in the context of this litigation. See Friends of the Payette v. Horseshoe Bend Hydroelec., 988 F.2d 989, 996 (9th Cir. 1993) (an issue is moot where the court can no longer provide a cognizable remedy). At this point, any opinion rendered on the direct copyright infringement claims related to the 230 zShops images would be merely advisory.

B. Subject Matter Jurisdiction and Registration of Copyrights.

17 U.S.C. § 411(a) prohibits a party from suing for copyright infringement in any district court “until registration of the copyright claim has been made in accordance with this title.”\(^\text{12}\)

The parties agree that some of the Corbis Images that Corbis claims have been infringed have been submitted to the Copyright Office, but have yet to be registered by the Register of Copyrights.\(^\text{13}\) Amazon argues that under § 411(a), this court has subject matter jurisdiction with

\(^{12}\)17 U.S.C. § 411(a) states in full:
Except for an action brought for a violation of the rights of the author under section 106A(a), and subject to the provisions of subsection (b), no action for infringement of the copyright in any United States work shall be instituted until registration of the copyright claim has been made in accordance with this title. In any case, however, where the deposit, application, and fee required for registration have been delivered to the Copyright Office in proper form and registration has been refused, the applicant is entitled to institute an action for infringement if notice thereof, with a copy of the complaint, is served on the Register of Copyrights. The Register may, at his or her option, become a party to the action with respect to the issue of registrability of the copyright claim by entering an appearance within sixty days after such service, but the Register’s failure to become a party shall not deprive the court of jurisdiction to determine that issue.

\(^{13}\)The number of Corbis Images that have not been registered by the Register of Copyrights is in dispute. Amazon indicates that 86 of the Corbis Images were not registered at the time this case was filed. See Dkt. # 215, Reply in Supp. of Def.’s Copyright Reg. Mot. at 8-9 n.10. Corbis contends that only 19 of the Corbis Images have not been registered by the Register of Copyrights. See Dkt. # 195, Opp. to Def.’s Copyright Reg. Mot. at 2.

ORDER REGARDING
SUMMARY JUDGMENT MOTIONS
party empowered to take it is surely among the least appropriate in which to presume nonexclusivity. ‘Where a statute . . . names the parties granted [the] right to invoke its provisions . . . such parties only may act.’” Hartford Underwriters Ins. v. Union Planters Bank, N.A., 530 U.S. 1, 6-7, 120 S.Ct. 1942, 147 L.Ed.2d 1 (2000) (quoting 2A N. Singer, SUTHERLAND ON STATUTORY CONSTRUCTION § 47.23, p. 217 (5th ed. 1992)).

Here, § 411(a) gives those who have applied and obtained registration and those who have applied and failed to obtain registration the right to file suit in federal court. This Court will not expand the meaning of the statute to include those whose applications are pending but undecided. As a result, the copyright claims relating to Corbis Images for which Corbis does not have a certificate of registration are dismissed for lack of subject matter jurisdiction.

C. Direct and Vicarious Copyright Infringement.

Corbis has filed a motion for partial summary judgment on its claims of direct and vicarious copyright infringement (Dkt. # 147), and Amazon has filed a motion for partial summary judgment challenging Corbis’s copyrights and alleging copyright misuse (Dkt. # 151). Once the claims arising from DMCA-protected activity and the claims relating to unregistered images have been culled, only two direct copyright infringement claims, both regarding a photograph that appeared on the IMDb website, remain.

To prove direct copyright infringement against Amazon, Corbis must demonstrate that (1) it owns a valid copyright, and (2) Amazon itself violated one or more of Corbis’s exclusive rights under the Copyright Act. See Ellison, 357 F.3d at 1076; see also A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001). The exclusive rights conveyed by copyright ownership include the right to reproduce the work, the right to prepare derivative works based on the work, the right to distribute copies of the work to the public and the right to display the work publicly. See 17 U.S.C. § 106(1)-(3) & (5).

Corbis claims that it owns the copyright to a photograph of actor Erika Christensen taken by photographer David Ash (the “Christensen Photo”). The Christensen Photo appeared among
a montage of celebrity photographs in an advertisement banner on IMDb that provided a link to
Amazon's zShops platform. Corbis has moved for summary judgment regarding whether
Amazon directly violated its copyright interests in the Christensen Photo by displaying it on
IMDb.\(^\text{14}\) Amazon argues that it should be entitled to summary judgment because Corbis has
failed to provide evidence that the Christensen Photo has been registered by the Copyright
Office.

Existence of a certificate of registration from the United States Copyright Office
("registration certificate") is prima facie evidence of a valid copyright. \textit{See} 17 U.S.C. § 410(c);
\textit{Apple Computer, Inc. v. Formula Intern. Inc.}, 725 F.2d 521, 523 (9th Cir. 1984). Corbis has
provided a registration certificate numbered VA 1-181-996 ("Registration No. '996"), which it
claims covers its derivative and compilation copyright interests in the Christensen Photo. \textit{See}
Keeley Decl. at 162. Registration No. '966 is entitled "Corbis Digital Online October 2002 &
Automated Database." \textit{See} Dkt. # 217, Supp. Decl. of Beth A. Colgan in Supp. of Mot. for
Corbis is listed as an author along with photographers "Fabian Cevallos, John Springer,
Micheline Pelletier & Others." \textit{Id.} The work is listed as a derivative or compilation and is
described as "[m]onthly updates of new unpublished photographs and digitally enhanced images,
along with a compilation of digitally enhanced, unpublished, previously published and public
domain images." \textit{Id.} at 372. A deposit of the work was filed with the Copyright Office. \textit{See} \textit{id.}
at 371.

Corbis has also provided a second registration certificate numbered VA 1-207-124

\(^{14}\)Corbis also claimed that Amazon directly infringed its copyrights in an image of Vin
Diesel displayed on IMDb. Corbis, however, has acknowledged that it has applied for
registration of the Vin Diesel image but that the image has yet to be registered. As a result, this
Court does not have subject matter jurisdiction with respect to that image. \textit{See} Section III. B,
infra.

ORDER REGARDING
SUMMARY JUDGMENT MOTIONS

-35-
("Registration No. '124"), which it claims covers the photographer's copyright interests in the Christensen Photo. See Dkt. # 209, Decl. of Claire L. Keeley in Supp. of Corbis's Mots. for Summ. J. ("Keeley S.J. Decl."), at 622-623. Registration No. '124 is entitled "Erika Christensen" and indicates that the photograph was published in Detour magazine in November, 2000. Id. David Ash submitted the photograph and is listed as its author. A copy of the photograph was deposited with the Copyright Office.

Corbis has provided the Court with a spreadsheet listing the 232 images it claims have been infringed. See Keeley Opp. Decl., at ¶ 10, pp. 030-087. The spreadsheet indicates that the Christensen Photo is copyrighted under Registration Nos. '966 and '124. See id. at 047. Corbis argues that Registration Nos. '966 and '124, combined with its spreadsheet, demonstrate prima facie evidence of valid copyrights in the Christensen Photo. Amazon, in turn, has spent much time and energy pointing out inconsistencies in the Corbis spreadsheet. Amazon argues that it should be granted summary judgment because Corbis has failed to prove that it owns the copyrights to the Christensen Photo.

There exists a legitimate question of fact regarding whether Registration Nos. '966 and

Amazon also argues that Corbis should be denied summary judgment because it does not have standing to assert an infringement of Mr. Ash's copyright interest in the Christensen Photo. Although not a model of clarity, Corbis’s contract with Mr. Ash states that Mr. Ash transfers to Corbis "the right to use, reproduce, publish, exhibit, perform, publicly display, distribute, broadcast and transmit [the photographs]." Dkt. # 149, Decl. of David N. Weiskopf in Supp. of Pl.'s Mots. for Part. Sum. J., ¶ 3, at 32. Corbis has "full and complete authority to make and settle claims or to institute proceedings in Corbis’s or [Mr. Ash’s] name but at Corbis’s expense to recover damages for [the photographs] . . . and for the unauthorized use of [the photographs]." Id. at 34. The rights transferred by the contract are among those exclusive rights enumerated in § 106 of the Copyright Act. See 17 U.S.C. § 106. It is well-settled that the recipient of such transferred rights may sue for infringement of those rights. See Campbell v. Board of Trustees of Leland Stanford Junior University, 817 F.2d 499, 504 (9th Cir. 1987) (citing 17 U.S.C. § 501(d)).

ORDER REGARDING SUMMARY JUDGMENT MOTIONS
'124 cover the Christensen Photo. Although Corbis does have copyright certificates, those certificates are only prima facie evidence of "the validity of the copyright and of the facts stated in the certificate." Seiler v. Lucasfilm, Ltd., 808 F.2d 1316, 1321 (9th Cir. 1986) (quoting 17 U.S.C. § 401(c)), cert. denied, 484 U.S. 826 (1987). The facts stated in the '966 certificate make no mention of Mr. Ash, Ms. Christensen, or the photograph. The '124 certificate fares little better, merely indicating that it covers a photograph of Erika Christensen taken by David Ash. Although the Corbis spreadsheet links the registrations with the Christensen Photo, there is no way to corroborate this link. There is nothing on the face of the certificates for Registration Nos. '966 and '124 to confirm that the Christensen Photo is included among the deposited photos. The only way to determine with any certainty whether Registration Nos. '966 and '124 cover the Christensen Photo is to review a copy of the deposits included with the registration applications.

Although the deposits are equally available to both parties from the Copyright Office, see Copyright Office Circular 6 (2002), neither party bothered to obtain a copy of the deposits and provide them to the Court. Without the deposit, Corbis cannot show that the Christensen Photo is among the photographs covered by Registration Nos. '966 and '124. Because Amazon has equal access to the deposit, it cannot simply rest on Corbis's failure to provide the evidence. To prove that Registration Nos. '966 and '124 do not protect the Christensen Photo, Amazon has an obligation to obtain and provide the evidence available to it. Without the deposit, there remains a legitimate question of fact regarding whether the Christensen Photo is protected by Registration Nos. '966 and '124.

For the same reasons, Amazon's challenge to Registration No. '966 as a derivative copyright (Dkt. # 151) must also be denied. Amazon's motion is premised on the theory that Registration No. '966 is invalid because the enhanced image lacks sufficient originality and would negatively impact the original copyrighted image. Determining whether Amazon is correct requires a comparison of the images deposited with the Copyright Office for Registration.
No. '966 with the image deposited for Registration No. '124. As noted, neither party has provided that information, and this Court is simply unable to tell whether the '966 Copyright is valid without viewing the deposits.¹⁶

Finally, Amazon has also filed a motion for partial summary judgment on Corbis's measure of actual damages (Dkt. # 154). Amazon contends that Corbis's measure of actual damages is too speculative and should be rejected by this Court. In accord with this Order, at most Corbis is entitled to damages only for violations of its copyright interests in Registration Nos. '966 and '124 by the unauthorized display of the Christensen Photo on IMDb. The motion on actual damages addressed Corbis's calculation of damages with regard to all 232 photos that Corbis alleged were infringed. Because this Order changes the scope and extent of the damages available to Corbis, the Court denies Amazon's motion regarding damages. Either party may revisit this issue if, after consultation, they determine that the issue of actual damages with respect to the Christensen Photo is ripe for summary judgment.

D. Lanham Act and State Law Claim.

1. Lanham Act Claims.

In its complaint, Corbis alleges claims of trademark dilution under § 43(c) of the Lanham Act, 15 U.S.C. § 1125(c), et seq., and false designation of origin under § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a). See Compl. ¶¶ 120-144. Amazon has moved for summary judgment with regard to these claims. See Def.'s Trademark and State Law Mot. at 2. In its opposition, Corbis failed to proffer any argument in support of its trademark dilution claim. See generally, Opp. to Def.'s Trademark and State Law Mot. As a result, this Court grants Amazon's motion.

¹⁶Amazon's defense of copyright misuse (Dkt. # 151) is also denied. Corbis has not overstepped its bounds in pursuing its copyright interests. The areas of copyright litigation touched on by this suit are relatively new, often conflicting and certainly open to the interpretation adopted by Corbis. The evidence does not support a conclusion that Corbis is using its copyright interests "in a manner violative of the public policy embodied in the grant of a copyright." Lasercomb America, Inc. v. Reynolds, 911 F.2d 970, 978 (4th Cir. 1990).
§ 1125. False designations of origin, false descriptions, and dilution forbidden

(a) Civil action

(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—

(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person’s goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

(2) As used in this subsection, the term “any person” includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.

(3) In a civil action for trade dress infringement under this chapter for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that the matter sought to be protected is not functional.

(b) Importation

Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States. The owner, importer, or consignee of goods refused entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this chapter in cases involving goods refused entry or seized.

(c) Remedies for dilution of famous marks
(1) The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection. In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to—

(A) the degree of inherent or acquired distinctiveness of the mark;

(B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;

(C) the duration and extent of advertising and publicity of the mark;

(D) the geographical extent of the trading area in which the mark is used;

(E) the channels of trade for the goods 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 marks' owner and the person against whom the injunction is sought;

(G) the nature and extent of use of the same or similar marks by third parties; and

(H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

(2) In an action brought under this subsection, the owner of the famous mark shall be entitled only to injunctive relief as set forth in section 1116 of this title unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. If such willful intent is proven, the owner of the famous mark shall also be entitled to the remedies set forth in sections 1117 (a) and 1118 of this title, subject to the discretion of the court and the principles of equity.

(3) The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register shall be a complete bar to an action against that person, with respect to that mark, that is brought by another person under the common law or a statute of a State and that seeks to prevent dilution of the distinctiveness of a mark, label, or form of advertisement.

(4) The following shall not be actionable under this section:

(A) Fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark.
(B) Noncommercial use of a mark.

(C) All forms of news reporting and news commentary.

(d) Cyberpiracy prevention

(1) 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 or section 220506 of title 36.

(B) 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 person'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 others 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 incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

(iii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines 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 paragraph, 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 licensee.

(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 currency, 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 assigned the
domain name is located if—

(i) the domain name violates any right of the
owner of a mark registered in the Patent and
Trademark Office, or protected under subsection (a)
or (c) of this section; 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) 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.
§ 1129. Cyberpiracy protections for individuals

Release date: 2005-08-01

(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, including a work made for hire as defined in section 101 of title 17, 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 section, 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 section shall apply to domain names registered on or after November 29, 1999.
TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1114

§ 1114. Remedies; infringement; innocent infringement by printers and publishers

Release date: 2005-08-01

(1) Any person who shall, without the consent of the registrant—
   (a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or
   (b) reproduce, counterfeit, copy, or colorably imitate a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive,

shall be liable in a civil action by the registrant for the remedies hereinafter provided. Under subsection (b) hereof, the registrant shall not be entitled to recover profits or damages unless the acts have been committed with knowledge that such imitation is intended to be used to cause confusion, or to cause mistake, or to deceive.

As used in this paragraph, the term “any person” includes the United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, or other persons acting for the United States and with the authorization and consent of the United States, and any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. The United States, all agencies and instrumentalities thereof, and all individuals, firms, corporations, other persons acting for the United States and with the authorization and consent of the United States, and any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this chapter in the same manner and to the same extent as any nongovernmental entity.

(2) Notwithstanding any other provision of this chapter, the remedies given to the owner of a right infringed under this chapter or to a person bringing an action under section 1125 (a) or (d) 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 owner of the right infringed or person bringing the...
action under section 1125 (a) of this title 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 or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510 (12) of title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125 (a) of this title as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.

(C) Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 1125 (a) of this title with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.

(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 liable for monetary relief or, except as provided in subclause (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 authority described in subclause (I) may be subject to injunctive 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 1125 (d) of this title; 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 chapter. 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.

(E) As used in this paragraph—

(i) the term "violator" means a person who violates section 1125 (a) of this title; and

(ii) the term "violating matter" means matter that is the subject of a violation under section 1125 (a) of this title.
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

http://www.icann.org/udrp/udrp-policy-24oct99.htm

8/8/2005
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

http://www.icann.org/udrp/udrp-policy-24oct99.htm
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 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 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.

Comments concerning the layout, construction and functionality of this site should be sent to webmaster@icann.org.

Page Updated 05-Feb-2002

©2000, 2002 The Internet Corporation for Assigned Names and Numbers. All rights reserved.
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 telecopy or facsimile transmission, with a confirmation of transmission; or

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

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

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

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

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

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

(i) if delivered by telecopy 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.

Comments concerning the layout, construction and functionality of this site should be sent to webmaster@icann.org.

Page Updated 05-Feb-2002
©2000, 2002 The Internet Corporation for Assigned Names and Numbers. All rights reserved.

CONTENTS
Definitions

- What is a trademark?
- What is a service mark?
- What is a certification mark?
- What is a collective mark?

Basic Questions

- Do I have to register my trademark?
- What are the benefits of federal trademark registration?
- Do I have to be a U.S. citizen to obtain a federal registration?
- Where can I find trademark forms?
- Where can I get basic trademark information?
- Where can I ask a question about trademarks?
- Are there federal regulations governing the use of the designations "TM" or "SM" with trademarks?
- When can I use the federal registration symbol © with the mark?
- Do I need an attorney to file a trademark application?
- What constitutes "interstate commerce"?
- How do I find out whether a mark is already registered?
- Is a federal registration valid outside the United States?

Searching

- Is it advisable to conduct a search of the Office records before filing an application?
- Can the Office conduct a search for an applicant?
- Can trademarks be searched online?
- In searching the trademark data base on the Web there are records that appear to be registrations but the registration numbers are shown as 0000000. Is this an error?
- Where can I conduct a trademark search?
- What are "common law" rights?
- What is a "common law" search? How can I do one? Is doing a common law search necessary?

Trademarks, Patents and Copyrights

- How do I find out if I need patent, trademark and/or copyright protection?
- How do I register a copyright?

Application Process

- How do I obtain a federal trademark registration?
- Who may file an application?
- Do I have to use the application form provided by the Office?
- Can a fax copy or photocopy of an application be filed?
- Can I fax in my application?
- What is a specimen?
- What is a drawing?
- If I submit a specimen, is a drawing still required?
- Do I need an attorney to file my application?
Trademark FAQ

On what bases can a foreign applicant file an application for registration?
Can the Office refuse to register a mark?
Can I get a refund of monies paid to the Office?
How can I check on the status of a pending U.S. Trademark application?
How long does it take for a mark to be registered?
How long does a trademark registration last?
When did the renewal period change from twenty to ten years?
How long does an Intent-to-Use applicant have to allege actual use of the mark in commerce?
What are the different classes of goods and services?

Other

What is the Trademark Electronic Application System (TEAS)?
How do I contest someone else using a trademark similar to mine?
What official publications and information are available concerning trademarks?
What is a PTDL (Patent and Trademark Depository Library)?
How do I register to practice before the Patent and Trademark Office?
Is the name of a band a trademark?
Can a minor file a trademark application?
Can the ownership of a trademark be assigned or transferred from one person to another?
My spouse owned a trademark registration and has since died. Do I own it now?
What are some suggestions to facilitate filing a trademark application and/or contacting the Office?

Madrid Protocol - Frequently Asked Questions

Definitions

What is a trademark?

A trademark includes any word, name, symbol, or device, or any combination, used, or intended to be used, in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. In short, a trademark is a brand name.

^ Back to the Contents

What is a service mark?

A service mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce, to identify and distinguish the services of one provider from services provided by others, and to indicate the source of the services.

^ Back to the Contents

What is a certification mark?

A certification mark is any word, name, symbol, device, or any combination, used, or intended to be used, in commerce with the owner's permission by someone other than its owner, to certify regional or other geographic origin, material, mode of manufacture, quality, accuracy, or other characteristics of someone's goods or services, or that the work or labor on the goods or services was performed by members of a union or other organization.

^ Back to the Contents
What is a collective mark?

A collective mark is a trademark or service mark used, or intended to be used, in commerce, by the members of a cooperative, an association, or other collective group or organization, including a mark which indicates membership in a union, an association, or other organization.

^ Back to the Contents

Basic Questions

Do I have to register my trademark?

No, but federal registration has several advantages, including notice to the public of the registrant's claim of ownership of the mark, a legal presumption of ownership nationwide, and the exclusive right to use the mark on or in connection with the goods or services set forth in the registration.

^ Back to the Contents

What are the benefits of federal trademark registration?

1. Constructive notice nationwide of the trademark owner's claim.
2. Evidence of ownership of the trademark.
3. Jurisdiction of federal courts may be invoked.
4. Registration can be used as a basis for obtaining registration in foreign countries.
5. Registration may be filed with U.S. Customs Service to prevent importation of infringing foreign goods.

^ Back to the Contents

Do I have to be a U.S. Citizen to obtain a federal registration?

No. However, an applicant's citizenship must be set forth in the record. If an applicant is not a citizen of any country, then a statement to that effect is sufficient. If an applicant has dual citizenship, then the applicant must choose which citizenship will be printed in the Official Gazette and on the certificate of registration.

^ Back to the Contents

Where can I find trademark forms?


^ Back to the Contents

Where can I get basic trademark information?

The USPTO website at http://www.uspto.gov/main/trademarks.htm provides a wide variety of information about trademarks and offers electronic filing of trademark applications and other trademark documents. The Trademark Electronic Business Center contains all the information needed for the entire registration process. You can search the trademark database for conflicting marks using the Trademark

For information about applying for a trademark, click Basic Facts About Trademarks. If you need answers to specific trademark questions, please contact the Trademark Assistance Center at 1-800-786-9199 (or 571-272-9250).

For patent information, please contact the Inventors Assistance Center at 1-800-786-9199. If you live in Northern Virginia, the number is (703) 308-4357.

Back to the Contents

Where can I ask a question about trademarks?

If you need answers to specific trademark questions or want to know more about trademarks in general, please contact the Trademark Assistance Center at 1-800-786-9199 (or 571-272-9250).

Back to the Contents

Are there federal regulations governing the use of the designations "TM" or "SM" with trademarks?

No. Use of the symbols "TM" or "SM" (for trademark and service mark, respectively) may, however, be governed by local, state, or foreign laws and the laws of the pertinent jurisdiction must be consulted. These designations usually indicate that a party claims rights in the mark and are often used before a federal registration is issued.

Back to the Contents

When is it proper to use the federal registration symbol (the letter R enclosed within a circle -- ® --) with the mark.

The federal registration symbol may be used once the mark is actually registered in the U.S. Patent and Trademark Office. Even though an application is pending, the registration symbol may not be used before the mark has actually become registered. The federal registration symbol should only be used on goods or services that are the subject of the federal trademark registration. [Note: Several foreign countries use the letter R enclosed within a circle to indicate that a mark is registered in that country. Use of the symbol by the holder of a foreign registration may be proper.]

Back to the Contents

Do I need an attorney to file a trademark application?

No, although it may be desirable to employ an attorney who is familiar with trademark matters. An applicant must comply with all substantive and procedural requirements of the Trademark Act and Trademark Rules of Practice even if he or she is not represented by an attorney. The names of attorneys who specialize in trademark law may be found in the telephone yellow pages, or by contacting a local bar association. Trademark search firms are often listed in the yellow pages under the heading "Trademark Search Services" or "Patent and Trademark Search Services." The USPTO cannot aid in the selection of a search firm or an attorney.

Back to the Contents

What constitutes interstate commerce?

For goods, "Interstate commerce" involves sending the goods across state lines with the mark displayed
on the goods or the packaging for the goods. With services, "interstate commerce" involves offering a service to those in another state or rendering a service which affects interstate commerce (e.g. restaurants, gas stations, hotels, etc.). See TMEP section 901.03.

^ Back to the Contents

How do I find out whether a mark is already registered?

You may conduct a search free of charge on the USPTO website using the Trademark Electronic Search System (TESS) at http://tess2.uspto.gov/bin/gate.exe?f=login&i=login&i_login=English&i_lang=English&p_d=trmk. If your mark includes a design element, you will have to search it by using a design code. To locate the proper design code(s), please consult the Design Search Code Manual.

You may also conduct a trademark search by visiting the Trademark Public Search Library, between 8:00 a.m. and 5:00 p.m. at Public Search Facility - Madison East, 1st Floor; 600 Dulany St.; Alexandria, VA 22313. Use of the Public Search Library is free to the public. You can also conduct a search at a Patent and Trademark Depository Library near you. For locations, click PTDL.

Private trademark search firms will conduct searches for a fee. The USPTO cannot aid in the selection of a search firm. Search firms are often listed in the yellow page section of telephone directories under the heading "Trademark Search Services" or "Patent and Trademark Search Services."

^ Back to the Contents

Is a federal registration valid outside the United States?

No. However, if you are a qualified owner of a trademark application pending before the USPTO, or of a registration issued by the USPTO, you may seek registration in any of the countries that have joined the Madrid Protocol by filing a single application, called an "international application," with the International Bureau of the World Property Intellectual Organization, through the USPTO. For more information about the Madrid Protocol, click here.

Also, certain countries recognize a United States registration as a basis for filing an application to register a mark in those countries under international treaties. See TMEP Chapter 1000 for further information. The laws of each country regarding registration must be consulted.

^ Back to the Contents

Is It advisable to conduct a search of the Office records before filing an application?

Yes. You may conduct a search free of charge on the USPTO website using the Trademark Electronic Search System (TESS) at http://tess2.uspto.gov/bin/gate.exe?f=login&i=login&i_login=English&i_lang=English&p_d=trmk. You may also conduct a trademark search by visiting the Trademark Public Search Library, between 8:00 a.m. and 5:00 p.m. at Public Search Facility - Madison East, 1st Floor; 600 Dulany St.; Alexandria, VA 22313. Use of the Public Search Library is free to the public. You can also conduct a search at a Patent and Trademark Depository Library near you. For locations, click PTDL.

^ Back to the Contents

Can the Office conduct a search for an applicant?

No. After a trademark application is filed, the U.S. Patent and Trademark Office (USPTO) will conduct a search of the records as part of the official examination process. The official search is not done for the
Trademark Handout

TM Basics

- Trademarks identify and distinguish the source and origin of goods and services in the marketplace
- Hierarchy of TMs:
  - Fanciful—Kodak, Verizon, Oreo
  - Arbitrary—Apple Computers
  - Suggestive—Greyhound Bus
  - Descriptive—Computerland
  - Generic—Toothpaste for toothpaste
- Categories are not static—Aspirin, Escalator
- "Inherently Distinctive" = arbitrary, fanciful, suggestive

TM Basics

- Infringement occurs when a use creates a likelihood of consumer confusion about product source
  - Trademarks can co-exist if they are used in different geographical areas or are used in connection with unrelated products
  - Registration not required
- Multi-factor tests for confusion
  - 9th Circuit "Steelcase" factors: mark strength, proximity of goods, mark similarity, evidence of actual confusion, marketing channels used, purchase care, intent, and likelihood of product line expansion

TM Basics

- Initial Interest Confusion can be alternative to multi-factor likelihood of confusion test
- Promatek definition: "when a customer is lured to a product by the similarity of the mark, even if the customer realizes the true source of the goods before the sale is consummated":
  - Ex: Search engine placement
  - Plaintiff-friendly doctrine
  - Some courts limit doctrine to competitors

TM Dilution

- Dilution is "lessening of the capacity of a famous mark to identify and distinguish goods or services"
- Elements
  - Famous mark
  - Distinctive (?)
  - Commercial use in commerce
  - Defendant's use began after mark became famous
  - Actual dilution
  - Consumer confusion is not a factor!

TM Dilution

- "Famous" trademark:
  - degree of distinctiveness
  - duration/extent of mark use
  - duration/extent of advertising and publicity
  - geography of mark's trading area
  - trade channels for goods and services associated with mark
  - degree of mark recognition
  - nature and extent of similar marks
  - mark registered?

TM Dilution

- Actual Dilution
  - Tarnishment
    - Pillsbury Doughboy having raunchy sex
  - Blurring
    - Rolex-Royce Coca, Buck Aspirin
  - Other lessening of capacity?
- Defenses
  - Fair use in comparative commercial advertising to identify the TM owner's competing goods
  - Noncommercial use
  - News reporting and news commentary
**ACPA**

- **15 USC 1125(d):** Civil cause of action against a domain name registrant who
  - registers, traffics in or uses a domain name that
    - is identical or confusingly similar to a distinctive TM,
    - dilutes a famous TM, or
    - is a Red Cross or Olympic TM,
  - has bad faith intent to profit from domain name

**ACPA**

- Factors bearing on bad faith intent to profit
  - registrant's IP rights in domain name
  - if domain name contains registrant's name
  - bona fide use to offer goods/services
  - bona fide noncommercial or fair use
  - intent to divert consumers for commercial gain or to hurt TM owner
  - offer to sell domain name without legitimate use
  - failed contact info
  - multiple bogus registrations
  - degree of distinctiveness/famousness
- No bad faith where person reasonably believed that use was fair or lawful

**ACPA**

- Remedies:
  - cancellation of registration
  - transfer to TM owner
  - damages
    - actual damages or
    - statutory damages of $1,000 to $100,000
- Paradigmatic application: typosquatting

**ACPA**

- Special protections for personal names (15 USC 1129)
  - Civil cause of action for registering a domain name containing another living person's name (or confusingly similar version) with intent to profit by selling the domain name
    - Unless registration is associated with biography or other copyrighted work
    - Remedies include cancellation, transfer and maybe costs/attorneys fees

**UDRP**

- Complainant needs to show:
  - domain name identical/confusingly similar to TM;
  - registrant has no legitimate interests in domain name, and
  - domain name registered and used in bad faith, which can be evidenced by
    - registered for profit/business;
    - registered to block legitimate TM owner (if pattern can be shown);
    - registered to disrupt competition, or
    - name used to attract attention to site by creating likelihood of confusion

**UDRP**

- Registrant can show legitimate rights in the domain name by showing
  - actual or planned bona fide offering of goods/services,
  - commonly known by domain name, or
  - legitimate noncommercial or fair use without profit-seeking intent to divert traffic or tarnish TM
- Also, "reverse domain name hijacking"
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BOSLEY MEDICAL INSTITUTE, INC., a
Delaware corporation,
Plaintiff-Appellant,

and

BOSLEY MEDICAL GROUP, S.C., an
Illinois corporation,

v.

MICHAEL STEVEN KREMER,
Defendant-Appellee.

No. 04-55962
D.C. No.
CV-01-01752-WQH
OPINION

Appeal from the United States District Court
for the Southern District of California
William Q. Hayes, District Judge, Presiding

Argued and Submitted
March 8, 2005—Pasadena, California

Filed April 4, 2005

Before: Thomas G. Nelson, Barry G. Silverman, and
Richard C. Tallman, Circuit Judges.

Opinion by Judge Silverman
COUNSEL

Diana M. Torres, O’Melveny & Myers, Los Angeles, California, for the plaintiff-appellant.

Paul Alan Levy, Public Citizen Litigation Group, Washington, D.C., for the defendant-appellee.

OPINION

SILVERMAN, Circuit Judge:

Defendant Michael Kremer was dissatisfied with the hair restoration services provided to him by the Bosley Medical
Institute, Inc. In a bald-faced effort to get even, Kremer started a website at www.BosleyMedical.com, which, to put it mildly, was uncomplimentary of the Bosley Medical Institute. The problem is that “Bosley Medical” is the registered trademark of the Bosley Medical Institute, Inc., which brought suit against Kremer for trademark infringement and like claims. Kremer argues that noncommercial use of the mark is not actionable as infringement under the Lanham Act. Bosley responds that Kremer is splitting hairs.

Like the district court, we agree with Kremer. We hold today that the noncommercial use of a trademark as the domain name of a website — the subject of which is consumer commentary about the products and services represented by the mark — does not constitute infringement under the Lanham Act.

Bosley Medical’s cybersquatting claim is another matter. The issue under the Anticybersquatting Consumer Protection Act was whether Kremer had a “bad faith intent to profit” from the use of the trademark in his domain name, such as by making an extortionate offer to sell the BosleyMedical.com site to Bosley. Because discovery regarding that claim had not been completed, and the issue itself was not within the scope of the summary judgment motions, the district court erred in granting summary judgment to Kremer as to cybersquatting.

Finally, we hold that the district court should not have granted Kremer’s motion to strike Bosley Medical’s state-law claims pursuant to the California anti-SLAPP statute. Bosley Medical’s complaint about the unauthorized use of its trademark as Kremer’s domain name was not so lacking in merit as to be susceptible to an anti-SLAPP motion to strike at an early stage of the case.
I. Background

Bosley Medical provides surgical hair transplantation, restoration, and replacement services to the public. Bosley Medical owns the registered trademark “BOSLEY MEDICAL,”† has used the mark “BOSLEY MEDICAL” since 1992, and registered the mark with the United States Patent and Trademark Office in January 2001. Bosley has spent millions of dollars on advertising and promotion throughout the United States and the rest of the world.

Michael Kremer is a dissatisfied former patient of Bosley. Unhappy with the results of a hair replacement procedure performed by a Bosley physician in Seattle, Washington, he filed a medical malpractice lawsuit against Bosley Medical in 1994. That suit was eventually dismissed.

In January 2000, Kremer purchased the domain name www.BosleyMedical.com, the subject of this appeal, as well as the domain name www.BosleyMedicalViolations.com, which is not challenged by Bosley. Five days after registering the domain name, Kremer went to Bosley Medical’s office in Beverly Hills, California and delivered a two-page letter to Dr. Bosley, Founder and President of Bosley Medical. The first page read:

Let me know if you want to discuss this. Once it is spread over the internet it will have a snowball effect and be too late to stop. M. Kremer [phone number].
P.S. I always follow through on my promises.

The second page was entitled “Courses of action against BMG” and listed eleven items. The first item stated: “1. Net web sites disclosing true operating nature of BMG. Letter 3/

†Bosley also owns the following trademarks: BOSLEY, BOSLEY HEALTHY HAIR, BOSLEY HEALTHY HAIR FORMULA, and BOSLEY HEALTHY HAIR COMPLEX.
14/96 from LAC D.A. Negative testimonials from former clients. Links. Provide BMG competitors with this information.” The letter contains no mention of domain names or any other reference to the Internet.

Kremer began to use www.BosleyMedical.com in 2001. His site summarizes the Los Angeles County District Attorney’s 1996 investigative findings about Bosley, and allows visitors to view the entire document. It also contains other information that is highly critical of Bosley. Kremer earns no revenue from the website and no goods or services are sold on the website. There are no links to any of Bosley’s competitors’ websites. BosleyMedical.com does link to Kremer’s sister site, BosleyMedicalViolations.com, which links to a newsgroup entitled alt.baldspot, which in turn contains advertisements for companies that compete with Bosley. BosleyMedical.com also contained a link to the Public Citizen website. Public Citizen is the organization that represents Kremer in this case.

Bosley brought this suit alleging trademark infringement, dilution, unfair competition, various state law claims, and a libel claim that was eventually settled. Bosley sought to take discovery aimed at the trademark and libel claims. The magistrate judge granted limited discovery on the libel claims. Following discovery, Bosley dismissed the libel claims and amended the complaint.

Kremer moved to dismiss the First Amended Complaint and in addition moved for partial summary judgment on the issues of commercial use and likelihood of confusion. Bosley filed a cross-motion for partial summary judgment on the infringement and dilution claims. Kremer agreed that the facts were undisputed with regard to the issues of commercial use and likelihood of confusion, and that these issues were ripe for summary judgment.

Ruling that Kremer’s use of “Bosley Medical” in the domain name was noncommercial and unlikely to cause con-
fusion, the district court entered summary judgment for Kremer on the federal claims and dismissed the state law claims under California’s anti-SLAPP statute. Bosley now appeals.

II. Jurisdiction and Standard of Review


III. Analysis

A. Trademark Infringement and Dilution Claims


[2] Infringement claims are subject to a commercial use requirement. The infringement section of the Lanham Act, 15 U.S.C. § 1114, states that any person who "use[s] in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive . . ." can be held liable for such use. 15 U.S.C. § 1114(1)(a).

[3] In 1996, Congress expanded the scope of federal trademark law when it enacted the Federal Trademark Dilution Act
("FTDA"). The FTDA allows the "owner of a famous mark" to obtain "an injunction against another person's commercial use in commerce of a mark or trade name . . . ." 15 U.S.C. § 1125(c)(1) (emphasis added). While the meaning of the term "commercial use in commerce" is not entirely clear, we have interpreted the language to be roughly analogous to the "in connection with" sale of goods and services requirement of the infringement statute. See Mattel, Inc. v. MCA Records, Inc., 296 F.3d 894, 903 (9th Cir. 2002) ("Although this statutory language is ungainly, its meaning seems clear: It refers to a use of a famous and distinctive mark to sell goods other than those produced or authorized by the mark's owner."); see also Huthwaite, Inc. v. Sunrise Assisted Living, Inc., 261 F. Supp. 2d 502, 517 (E.D. Va. 2003) (holding that the commercial use requirement of the FTDA is "virtually synonymous with the 'in connection with the sale, offering for sale, distribution, or advertising of goods and services' requirement" of the Lanham Act).

The inclusion of these requirements in the Lanham Act serves the Act's purpose: "to secure to the owner of the mark the goodwill of his business and to protect the ability of consumers to distinguish among competing producers." Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 774 (1992) (internal quotation marks and citations omitted). In other words, the Act is designed to protect consumers who have formed particular associations with a mark from buying a competing product using the same or substantially similar mark and to allow the mark holder to distinguish his product from that of his rivals. See Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 873 (9th Cir. 1999).

The Supreme Court has made it clear that trademark infringement law prevents only unauthorized uses of a trademark in connection with a commercial transaction in which the trademark is being used to confuse potential consumers. See Prestonettes, Inc. v. Coty, 264 U.S. 359, 368 (1924) ("A trade-mark only gives the right to prohibit the use of it so far
as to protect the owner’s good will against the sale of another’s product as his.” [emphasis added]); see also Mishawaka Rubber & Woolen Mfg. Co. v. S.S. Kresge Co., 316 U.S. 203, 205 (1942) (explaining that the main purpose of the Lanham Act is to prevent the use of identical or similar marks in a way that confuses the public about the actual source of goods and services).

As the Second Circuit held, “[t]he Lanham Act seeks to prevent consumer confusion that enables a seller to pass off his goods as the goods of another . . . . [T]rademark infringement protects only against mistaken purchasing decisions and not against confusion generally.” Lang v. Ret. Living Publ’g Co., Inc., 949 F.2d 576, 582-83 (2d Cir. 1991) (internal quotation marks and citation omitted) (emphasis added).

As a matter of First Amendment law, commercial speech may be regulated in ways that would be impermissible if the same regulation were applied to noncommercial expressions. Florida Bar v. Went For It, Inc., 515 U.S. 618, 623 (1995). “The First Amendment may offer little protection for a competitor who labels its commercial good with a confusingly similar mark, but trademark rights do not entitle the owner to quash an unauthorized use of the mark by another who is communicating ideas or expressing points of view.” Mattel, 296 F.3d at 900 (internal quotation marks and citations omitted).

The district court ruled that Kremer’s use of Bosley’s mark was noncommercial. To reach that conclusion, the court focused on the “use in commerce” language rather than the “use in connection with the sale of goods” clause. This approach is erroneous. “Use in commerce” is simply a jurisdictional predicate to any law passed by Congress under the Commerce Clause. See Steele v. Bulova Watch Co., 344 U.S. 280, 283 (1952); OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176, 185 (W.D.N.Y. 2000). 15 U.S.C. § 1127 states that “unless the contrary is plainly apparent from the context
. . . [t]he word ‘commerce’ means all commerce which may lawfully be regulated by Congress.” Therefore, the district court should have determined instead whether Kremer’s use was “in connection with a sale of goods or services” rather than a “use in commerce.” However, we can affirm the district court’s grant of summary judgment on any ground supported by the record. *Lamps Plus, Inc. v. Seattle Lighting Fixture Co.*, 345 F.3d 1140, 1143 (9th Cir. 2003). The question before us, then, boils down to whether Kremer’s use of Bosley Medical as his domain name was “in connection with a sale of goods or services.” If it was not, then Kremer’s use was “noncommercial” and did not violate the Lanham Act.

Bosley argues that it has met the commercial use requirement in three ways. First, it argues that a mark used in an otherwise noncommercial website or as a domain name for an otherwise noncommercial website is nonetheless used in connection with goods and services where a user can click on a link available on that website to reach a commercial site. *Nissan Motor Co. v. Nissan Computer Corp.*, 378 F.3d 1002 (9th Cir. 2004). However, Bosley’s reliance on *Nissan* is unfounded.

[4] In *Nissan*, Nissan Motor Company sued Nissan Computer Corporation for using the Internet websites www.Nissan.com and www.Nissan.net. *Id.* at 1006. In *Nissan*, however, commercial use was undisputed, as the core function of the defendant’s website was to advertise his computer business. *Id.* Additionally, the defendant in *Nissan*, like the defendant in *Taubman Co. v. Webfeats*, 319 F.3d 770 (6th Cir. 2003), placed links to other commercial businesses directly on their website. 319 F.3d at 772-73. Kremer’s website contains no commercial links, but rather contains links to a discussion group, which in turn contains advertising. This roundabout path to the advertising of others is too attenuated to render Kremer’s site commercial. At no time did Kremer’s BosleyMedical.com site offer for sale any product or service or contain paid advertisements from any other commercial
entity. See *TMI, Inc. v. Maxwell*, 368 F.3d 433, 435, 438 (5th Cir. 2004) (holding that the commercial use requirement is not satisfied where defendant’s site had no outside links).

[5] Bosley also points out that Kremer’s site contained a link to Public Citizen, the public interest group representing Kremer throughout this litigation. We hold that Kremer’s identification of his lawyers and his provision of a link to same did not transform his noncommercial site into a commercial one.

[6] Bosley’s second argument that Kremer’s website satisfies the “in connection with the sale of goods or services” requirement of the Lanham Act is that Kremer created his website to enable an extortion scheme in an attempt to profit from registering BosleyMedical.com. In *Panavision International, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998), this court held that a defendant’s “commercial use was his attempt to sell the trademarks themselves.” *Id.* at 1325. Similarly, in *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996), the court found that “Toeppen’s intention to arbitrage the ‘intermatic.com’ domain name constitute[d] a commercial use.” *Id.* at 1239; see also *Boston Prof’l Hockey Ass’n, Inc. v. Dallas Cap & Emblem Mfg., Inc.*, 510 F.2d 1004, 1010 (5th Cir. 1975) (holding that trademark law protects the trademark itself, despite the fact that only “a reproduction of the trademark itself is being sold, unattached to any other goods or services”).

[7] However, in this case, there is no evidence that Kremer was trying to sell the domain name itself. The letter delivered by Kremer to Bosley’s headquarters is a threat to expose negative information about Bosley on the Internet, but it makes no reference whatsoever to ransoming Bosley’s trademark or to Kremer’s use of the mark as a domain name.

Bosley argues that it was denied an opportunity to pursue discovery on commercial use, and had it been allowed to pro-
ceed with discovery, it could further establish that Kremer has attempted to sell the domain name. However, in opposing Kremer’s motion for summary judgment, Bosley did not make any such objections. Bosley failed to request further discovery under Federal Rule of Civil Procedure 56(f), but instead moved for summary judgment itself. Although Bosley’s reply brief supporting its own motion for summary judgment complained about limited discovery in a footnote, Bosley did not move for leave to take discovery. The district court did not abuse its discretion in granting the summary judgment without permitting further discovery.

Bosley’s third and final argument that it satisfied the commercial use requirement of the Lanham Act is that Kremer’s use of Bosley’s trademark was in connection with Bosley’s goods and services. In other words, Kremer used the mark “in connection with goods and services” because he prevented users from obtaining the plaintiff’s goods and services. See People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359 (4th Cir. 2001) (“PETA”). In PETA, defendants created a site that promoted ideas antithetical to those of the PETA group. Id. at 362-63. The Fourth Circuit held that the defendant’s parody site, though not having a commercial purpose and not selling any goods or services, violated the Lanham Act because it “prevented users from obtaining or using PETA’s goods or services.” Id. at 365.

[8] However, in PETA, the defendant’s website “provide[d] links to more than 30 commercial operations offering goods and services.” Id. at 366. To the extent that the PETA court held that the Lanham Act’s commercial use requirement is satisfied because the defendant’s use of the plaintiff’s mark as the domain name may deter customers from reaching the plaintiff’s site itself, we respectfully disagree with that rationale. While it is true that www.BosleyMedical.com is not sponsored by Bosley Medical, it is just as true that it is about Bosley Medical. The PETA approach would place most critical, otherwise protected consumer commentary under the

The PETA court’s reading of the Lanham Act would encompass almost all uses of a registered trademark, even when the mark is merely being used to identify the object of consumer criticism. This broad view of the Lanham Act is supported by neither the text of the statute nor the history of trademark laws in this country. “[T]rademark laws are intended to protect” consumers from purchasing the products of an infringer “under the mistaken assumption that they are buying a product produced or sponsored by [the trademark holder].” Beneficial Corp. v. Beneficial Capital Corp., 529 F. Supp. 445, 450 (S.D.N.Y. 1982). Limiting the Lanham Act to cases where a defendant is trying to profit from a plaintiff’s trademark is consistent with the Supreme Court’s view that “[a trademark’s] function is simply to designate the goods as the product of a particular trader and to protect his good will against the sale of another’s product as his.” United Drug Co. v. Theodore Rectanus Co., 248 U.S. 90, 97 (1918); see also l McCarthy on Trademarks and Unfair Competition § 2:7 (4th ed. 2004).

[9] The Second Circuit held in United We Stand America, Inc. v. United We Stand, America New York, Inc., 128 F.3d 86, 90 (2d Cir. 1997), that the “use in connection with the sale of goods and services” requirement of the Lanham Act does not require any actual sale of goods and services. Thus, the

*In fact, such a holding would suggest that any time a non-holder of a trademark uses the mark as his domain name, he would violate the Lanham Act. However, when Congress amended the Lanham Act to add the Anti-cybersquatting Consumer Protection Act, it limited violations only to situations where a person registers the site with a bad faith intent to profit. To find a Lanham Act violation without finding commercial use may contradict Congress’ intent.*
appropriate inquiry is whether Kremer offers competing services to the public. Kremer is not Bosley’s competitor; he is their critic. His use of the Bosley mark is not in connection with a sale of goods or services — it is in connection with the expression of his opinion about Bosley’s goods and services.

[10] The dangers that the Lanham Act was designed to address are simply not at issue in this case. The Lanham Act, expressly enacted to be applied in commercial contexts, does not prohibit all unauthorized uses of a trademark. Kremer’s use of the Bosley Medical mark simply cannot mislead consumers into buying a competing product — no customer will mistakenly purchase a hair replacement service from Kremer under the belief that the service is being offered by Bosley. Neither is Kremer capitalizing on the good will Bosley has created in its mark. Any harm to Bosley arises not from a competitor’s sale of a similar product under Bosley’s mark, but from Kremer’s criticism of their services. Bosley cannot use the Lanham Act either as a shield from Kremer’s criticism, or as a sword to shut Kremer up.3

B. Anticybersquatting Consumer Protection Act

In 1999, Congress passed the Anticybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C. § 1125(d), as an amendment to the Lanham Act to prohibit cybersquatting.

Cybersquatting occurs when a person other than the trademark holder registers the domain name of a well known trademark and then attempts to profit from this by either ransomming the domain name back to the trademark holder or by using the domain name to divert business from the trademark holder to the domain name holder.

3Because we hold that Kremer’s use of Bosley’s mark was noncommercial, we do not reach the issue of initial interest confusion which was addressed in Interstellar Starship Services, Ltd. v. Epix, Inc., 304 F.3d 936 (9th Cir. 2002).
DaimlerChrysler v. The Net Inc., 388 F.3d 201, 204 (6th Cir. 2004) (internal quotation marks omitted).

The ACPA states:

A person shall be liable in a civil action by the owner of a mark . . . if, without regard to the goods or services of the parties, that person (i) has a bad faith intent to profit from that mark . . . ; and (ii) registers, traffics in, or uses a domain name [that is confusingly similar to another’s mark or dilutes another’s famous mark].


The district court dismissed Bosley’s ACPA claim for the same reasons that it dismissed the infringement and dilution claims — namely, because Kremer did not make commercial use of Bosley’s mark. However, the ACPA does not contain a commercial use requirement, and we therefore reverse.

Kremer argues that the “noncommercial use” proviso that appears in the dilution portion of § 1125 applies to cybersquatting claims with equal force. Admittedly, the language in § 1125 is confusing. 15 U.S.C. § 1125(c)(4) reads: “The following shall not be actionable under this section: . . . (B) Noncommercial use of a mark.” 15 U.S.C. § 1125(c)(4)(B). Kremer asserts that by using the word “section,” rather than the more precise term “subsection,” Congress meant for the proviso to apply to all of § 1125, as opposed to subsection (c).

[11] This argument fails for two reasons. The noncommercial use exception, which appears in a different part of the Lanham Act, is in direct conflict with the language of the ACPA. The ACPA makes it clear that “use” is only one possible way to violate the Act (“registers, traffics in, or uses”). Allowing a cybersquatter to register the domain name with a bad faith intent to profit but get around the law by making
noncommercial use of the mark would run counter to the purpose of the Act. “[T]he use of a domain name in connection with a site that makes a noncommercial or fair use of the mark does not necessarily mean that the domain name registrant lacked bad faith.” Coca-Cola Co. v. Purdy, 382 F.3d 774, 778 (8th Cir. 2004) (internal quotation marks and citation omitted); see also H.R. Rep. No. 106-412 at 11 (1999) (“This factor is not intended to create a loophole that otherwise might swallow the bill, however, by allowing a domain name registrant to evade application of the Act by merely putting up a noninfringing site under an infringing domain name.”). “It is a well-established canon of statutory construction that a court should go beyond the literal language of a statute if reliance on that language would defeat the plain purpose of the statute.” Bob Jones Univ. v. United States, 461 U.S. 574, 586 (1983); see also Albertson’s, Inc. v. Commissioner, 42 F.3d 537, 546 (9th Cir. 1994).

Additionally, one of the nine factors listed in the statute that courts must consider is the registrant’s “bona fide non-commercial or fair use of the mark in a site accessible under the domain name.” 15 U.S.C. § 1125(d)(1)(B)(iv). This factor would be meaningless if the statute exempted all non-commercial uses of a trademark within a domain name. We try to avoid, where possible, an interpretation of a statute “that renders any part of it superfluous and does not give effect to all of the words used by Congress.” Nevada v. Watkins, 939 F.2d 710, 715 (9th Cir. 1991) (internal quotation marks and citation omitted).

[12] Finally, other courts that have construed the ACPA have not required commercial use. In DaimlerChrysler, the Sixth Circuit held that a

trademark owner asserting a claim under the ACPA must establish the following: (1) it has a valid trademark entitled to protection; (2) its mark is distinctive or famous; (3) the defendant’s domain name is iden-
tical or confusingly similar to, or in the case of famous marks, dilutive of, the owner’s mark; and (4) the defendant used, registered, or trafficked in the domain name (5) with a bad faith intent to profit.

388 F.3d at 204. See also Ford Motor Co. v. Catalanotte, 342 F.3d 543, 546 (6th Cir. 2003); E. & J. Gallo Winery v. Spider Webs Ltd., 129 F. Supp. 2d 1033, 1047-48 (S. D. Tex. 2001), aff’d, 286 F.3d 270 (5th Cir. 2002) (“As reflected by the language of the ACPA and the case law interpreting it, there is no requirement . . . that the ‘use’ be a commercial use to run afoul of the ACPA”).

[13] The district court erred in applying the commercial use requirement to Bosley’s ACPA claim. Rather, the court should confine its inquiry to the elements of the ACPA claim listed in the statute, particularly to whether Kremer had a bad faith intent to profit from his use of Bosley’s mark in his site’s domain name. Bosley has met the first prong of the ACPA (that the domain name is identical to the mark) because Kremer used an unmodified version of Bosley’s mark as his domain name.

Concluding that all of Bosley’s claims, including the ACPA claim, were subject to a commercial use requirement, the district judge granted summary judgment in Kremer’s favor. But the ACPA claim was not in front of the district court in the motions for summary judgment. The court did not provide notice to Bosley that it would rule on this claim, and did not give Bosley an opportunity to conduct discovery on the issue. See Celotex Corp. v. Catrett, 477 U.S. 317, 326 (1986). For this reason, the district court erred in granting summary judgment for Kremer on the ACPA claim. It remains to be seen whether Bosley can establish that Kremer registered the domain name in bad faith or can authenticate other letters that Bosley alleges were written and sent by Kremer.
C. California's Anti-SLAPP Law

[14] In 1993, responding to the "disturbing increase in lawsuits brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances," the California Legislature enacted the Anti-Strategic Lawsuit Against Public Participation ("anti-SLAPP") statute. Cal. Civ. Proc. Code § 425.16(a). "The hallmark of a SLAPP suit is that it lacks merit, and is brought with the goals of obtaining an economic advantage over a citizen party by increasing the cost of litigation to the point that the citizen party's case will be weakened or abandoned, and of deterring future litigation." United States ex rel. Newsham v. Lockheed Missiles & Space Co., 190 F.3d 963, 970-71 (9th Cir. 1999) (citing Wilcox v. Superior Court, 33 Cal. Rptr. 2d 446, 449-50 (Cal. Ct. App. 1994)). The anti-SLAPP statute was designed to curtail these lawsuits by establishing a procedure to promptly expose and dismiss meritless and harassing claims seeking to chill protected expression. The statute provides that a defendant may move to strike a plaintiff's complaint if it "aris[es] from any act of that person in furtherance of the person's right of petition or free speech under the United States or California Constitution in connection with a public issue." Cal. Civ. Proc. Code § 425.16(b)(1).

A defendant filing an anti-SLAPP motion to strike "must make an initial prima facie showing that the plaintiff's suit arises from an act in furtherance of defendant's right of petition or free speech." Braun v. Chronicle Publ'g Co., 61 Cal. Rptr. 2d 58, 61 (Cal. Ct. App. 1997). The defendant need not show that plaintiff's suit was brought with the intention to chill defendant's speech; the plaintiff's "intentions are ultimately beside the point." Equilon Enters., LLC v. Consumer Cause, Inc., 124 Cal. Rptr. 2d 507, 519 (Cal. 2002).

[15] The district court ruled that Bosley was seeking to limit Kremer's free speech and granted Kremer's anti-SLAPP motion to strike Bosley's state law trademark claims. We now
reverse. An infringement lawsuit by a trademark owner over a defendant’s unauthorized use of the mark as his domain name does not necessarily impair the defendant’s free speech rights. As noted by the Second Circuit, “[d]omain names . . . per se are neither automatically entitled to nor excluded from the protections of the First Amendment, and the appropriate inquiry is one that fully addresses particular circumstances presented with respect to each domain name.” Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 585 (2d Cir. 2000). In Panavision, we stated that “[a] significant purpose of a domain name is to identify the entity that owns the web site,” 141 F.3d at 1327, and we explained in Mattel that a source identifier is not entitled to full First Amendment protection. 296 F.3d at 900. While a summary judgment motion might have been well-taken, an anti-SLAPP motion to strike was not. We reverse the grant of the anti-SLAPP motion to strike and remand to the district court for further proceedings on the state law claims.

IV. Conclusion

We affirm the district court’s entry of summary judgment in favor of Kremer with respect to the infringement and dilution claims. We remand the ACPA claim for further proceedings. The district court’s grant of the anti-SLAPP motion to strike the state law claims is reversed.

AFFIRMED in part, REVERSED in part, and REMANDED. No costs allowed.
In the
United States Court of Appeals
For the Seventh Circuit

No. 00-4276
PROMATEK INDUSTRIES, LTD.,

Plaintiff-Appellee,

v.

EQUITRAC CORPORATION,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division.
No. 00 C 4999—Milton I. Shadur, Judge.

ARGUED MAY 22, 2002—DECIDED AUGUST 13, 2002

Before POSNER, KANNE, and WILLIAMS, Circuit Judges.

WILLIAMS, Circuit Judge. This appeal concerns the propriety of a preliminary injunction in which one competitor, Promatek, prevailed against another, Equitrac. The preliminary injunction was issued without a hearing and Equitrac had to place language on its web page to remedy violations of the Lanham Act. Equitrac now appeals that order and because the district court did not abuse its discretion, we affirm.

I. BACKGROUND

Promatek and Equitrac are competitors in selling cost-recovery equipment. Equitrac's marketing department ad-
vised its web designer that certain words and phrases should be used as metatags for Equitrac’s website.¹ In response, the web designer placed the term “Copitrack” in the contents of Equitrac’s website as a metatag. Equitrac used the term as a metatag because it provides maintenance and service on Copitrak equipment, a product used in the cost-recovery business.² Promatek holds the trademark for Copitrak, and once it learned of Equitrac’s use of the term Copitrack in the metatag, it brought suit. After learning of Promatek’s suit, Equitrac contacted all of the search engines known to it and requested that they remove any link between the term Copitrack and Equitrac’s website. Equitrac also removed the Copitrack metatag from its website.

Not satisfied with Equitrac’s remedial measures, Promatek sought a preliminary injunction preventing Equitrac from using the term Copitrack in its website. After receiving materials submitted by both parties, the district

¹ Metatags are HTML [HyperText Markup Language] code intended to describe the contents of the web site. There are different types of metatags, but those of principal concern to us are the “description” and “keyword” metatags. The description metatags are intended to describe the web site; the keyword metatags, at least in theory, contain keywords relating to the contents of the web site. The more often a term appears in the metatags and in the text of the web page, the more likely it is that the web page will be “hit” in a search for that keyword and the higher on the list of “hits” the web page will appear.

² The parties agree that Equitrac meant to use the term “Copitrak” as its metatag rather than “Copitrack.”

Brookfield Communications, Inc. v. West Coast Entm’t Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).
court granted Promatek's motion for preliminary injunction. Under the terms of the injunction, Equitrac was directed to place language on its web page informing consumers that any link between its website and Copitrack was in error:

If you were directed to this site through the term "Copitrack," that is in error as there is no affiliation between Equitrac and that term. The mark "Copitrack" is a registered trademark of Promatek Industries, Ltd., which can be found at www.promatek.com or www.copitrack.com.

(Equitrac Ex. 1, Prelim. Inj. Order at 5).

Equitrac appeals the issuance of the injunction, arguing that the ordered language will not only inform consumers of its competitor, Promatek, but will encourage people to go to Promatek's website. Promatek counters that without this language, Equitrac will continue to benefit to Promatek's detriment, from consumer internet searches containing the word Copitrack. We conclude that the district court was correct in finding Promatek would suffer a greater harm than Equitrac if corrective measures were not taken, and we affirm the grant of the preliminary injunction.

II. ANALYSIS

A party seeking a preliminary injunction is required to demonstrate a likelihood of success on the merits, that it has no adequate remedy at law, and that it will suffer irreparable harm if the relief is not granted. Ty, Inc. v. Jones Group, 237 F.3d 391, 895 (7th Cir. 2001) (citing Abbott Labs v. Mead Johnson & Co., 971 F.2d 6, 11 (7th Cir. 1992)). If the moving party can satisfy these conditions, the court must then consider any irreparable harm an injunction would cause the nonmoving party.
In assessing the likelihood of consumer confusion, we consider: (i) the similarity between the marks in appearance and suggestion, (ii) the similarity of the products, (iii) the degree of care likely to be exercised by consumers, and (iv) any misuse of the term by the defendant.

1. Likelihood of success on the merits

Equitrac argues that because there was no likelihood of success on the merits of Promatek's Lanham Act claim, the district court erred in granting the preliminary injunction. However, we turn to the issue of whether consumer confusion would be confused by Equitrac's use of Copitrak as a trademark for computer input devices.

See 15 U.S.C. § 1125(a), Promatek is a protectable trademark and that Equitrac use of the term is likely to cause confusion among consumers. See Lenticular Systems, Inc. v. Adorne, Inc., 164 F.3d 337, 340 (2d Cir. 1999), which Equitrac does not disprove. Therefore, the district court erred in granting the preliminary injunction. In order to prevail under the Lanham Act, Promatek must establish that the district court committed clear error of fact or law.
(5) the strength of the plaintiff's marks, (6) any evidence of actual confusion, and (7) the defendant's intent to palm off its goods as those of the plaintiff's. *Ty*, 237 F.3d at 897-98. None of these factors are dispositive and the proper weight given to each will vary in each case. *Id.* However, the similarity of the marks, the defendant's intent, and evidence of actual confusion are of particular importance. *Id.*

Given these factors, it is clear that Promatek has a fair likelihood of succeeding on the merits of its Lanham Act claim. Although Promatek has not provided us with evidence regarding the strength of its Copitrak mark or evidence of any actual consumer confusion, the other factors weigh in its favor. First, not only are the marks Copitrack and Copitrak similar, Equitrac admits that it meant to use the correct spelling of Copitrak in its metatag. Second, Equitrac's use of Copitrack refers to Promatek's registered trademark, Copitrak. Additionally, Equitrac and Promatek are direct competitors in the cost-recovery and cost-control equipment and services market. Most importantly, for purposes of this case, however, is the degree of care to be exercised by consumers.

Although Equitrac claims that it did not intend to mislead consumers with respect to Copitrak, the fact remains that there is a strong likelihood of consumer confusion as a result of its use of the Copitrack metatag. The degree of care exercised by consumers could lead to initial interest confusion. Initial interest confusion, which is actionable under the Lanham Act, occurs when a customer is lured to a product by the similarity of the mark, even if the customer realizes the true source of the goods before the sale is consummated. *Dorr-Oliver, Inc. v. Fluid-Quip, Inc.*, 94 F.3d 376, 382 (7th Cir. 1996).

The Ninth Circuit has dealt with initial interest confusion for websites and metatags and held that placing
a competitor's trademark in a metatag creates a likelihood of confusion. In *Brookfield Communications*, the court found that although consumers are not confused when they reach a competitor's website, there is nevertheless initial interest confusion. 174 F.3d at 1062. This is true in this case, because by Equitrac's placing the term Copitrack in its metatag, consumers are diverted to its website and Equitrac reaps the goodwill Promatek developed in the Copitrak mark. *Id.* That consumers who are misled to Equitrac's website are only briefly confused is of little or no consequence. In fact, "that confusion as to the source of a product or service is eventually dispelled does not eliminate the trademark infringement which has already occurred." *Forum Corp. of N. Am. v. Forum, Ltd.*, 903 F.2d 434, 442 n.2 (7th Cir. 1990).

What is important is not the duration of the confusion, it is the misappropriation of Promatek's goodwill. Equitrac cannot unring the bell. As the court in *Brookfield* explained, "[u]sing another's trademark in one's metatags is much like posting a sign with another's trademark in front of one's store." *Brookfield*, 174 F.3d at 1064. Customers believing they are entering the first store rather than the second are still likely to mill around before they leave. The same theory is true for websites. Consumers who are directed to Equitrac's webpage are likely to learn more about Equitrac and its products before beginning a new search for Promatek and Copitrak. Therefore, given the likelihood of initial consumer confusion, the district court was correct in finding Promatek could succeed on the merits.

2. No adequate remedy at law

A plaintiff seeking a preliminary injunction must also prove that it has no adequate remedy at law and as a result, will suffer irreparable harm if the injunction is not
issued. Roland Mach. Co. v. Dresser Indus., Inc., 749 F.2d 380, 386 (7th Cir. 1984). Furthermore, it is well settled that injuries arising from Lanham Act violations are presumed to be irreparable, even if the plaintiff fails to demonstrate a business loss. Abbott Labs, 971 F.2d at 16.

As has been discussed, Promatek has suffered injury to its consumer goodwill through Equitrac’s use of Copitrack as a metatag and would have continued to suffer in the absence of an injunction. This damage would have constituted irreparable harm for which Promatek had no adequate remedy. See Meridian Mut. Ins. Co. v. Meridian Ins. Group, Inc., 128 F.3d 1111, 1120 (7th Cir. 1997). Because of the difficulty in assessing the damages associated with a loss of goodwill, the district court was correct in finding that Promatek lacked an adequate remedy at law.

3. Balancing of the harms

The final factor we must consider is the balance of harms—the irreparable harm Equitrac will suffer if the injunction is enforced weighed against the irreparable harm Promatek will suffer if it is not. See Meridian, 128 F.3d at 1121-22. We must also consider the effect the injunction will have on the public. Roland, 749 F.2d at 388. We review a district court’s balancing of the harms for an abuse of discretion. Ty, 237 F.3d at 902.

In finding that the harm to Promatek as a result of denying the injunction outweighed the harm to Equitrac in granting it, the district court found, and we agree, that without the injunction, Equitrac would continue to attract consumers browsing the web by using Promatek’s trademark, thereby acquiring goodwill that belongs to Promatek. In response, Equitrac points out that even though it offers products for sale on its website, it has yet to consummate a sale by this means. (Equitrac Ex. 2 ¶8). Furthermore, Equitrac claims that “consumers of products and
services provided by Equitrac and Promatek are sophisticated business people who are not likely to be confused between Equitrac and Copitrak and are not likely to buy based on a visit to a website." (Id. at ¶6).

Although Equitrac claims that the language on its website is harmful because it alerts consumers to Promatek’s website, it has not provided any evidence of customers it has lost as a result of the remedial language. Indeed the remedial language on the website is more informative than it is harmful. Equitrac’s speculative argument that Promatek may gain a competitive advantage by inclusion of the remedial language is rejected. As to the public interest, because the injunction prevents consumer confusion in the marketplace, the public interest will be served as well. Accordingly, the strong likelihood of consumer confusion weighs strongly in favor of issuing the injunction, and the district court did not abuse its discretion in finding this to be the case.

B. No evidentiary hearing was needed.

Finally, it was not necessary for the district court to hold a hearing before ruling on the motion for preliminary injunction. An evidentiary hearing is required if the nonmoving party raises genuine issues of material fact in response to a motion for a preliminary injunction. Ty, Inc. v. GMA Accessories, Inc., 132 F.3d 1167, 1171 (7th Cir. 1997). However, the party seeking the evidentiary hearing must demonstrate that it has “and intends to introduce evidence that if believed will so weaken the moving party’s case as to affect the judge’s decision on whether to issue the injunction.” Id.

Equitrac claims that the court should not have issued the preliminary injunction without a hearing. Specifically, Equitrac argues that because the court failed to find, and did not receive evidence to contradict, Equitrac’s position
that it was entitled to advertise that it was capable of servicing Copitrak equipment. Promatek's motion for a preliminary injunction should have been denied. Equitrac's argument misses the point. What is relevant to the preliminary injunction is not that Equitrac may advertise that it is capable of servicing Copitrak. Equitrac is free to do so; it is also free to place comparison claims on its website, or include press releases involving the litigation between Equitrac and Promatek. See *Brookfield*, 174 F.3d at 1065-66. It is Equitrac's use of the term Copitrack in its metatag that is a prohibited practice because of its potential for customer confusion. See *Brookfield*, 174 F.3d at 1066. Because Equitrac failed to demonstrate that its evidence would weaken Promatek's case, an evidentiary hearing was not necessary.

III. CONCLUSION

The district court did not abuse its discretion in issuing the preliminary injunction. We therefore AFFIRM.

A true Copy:

Teste:

_Clerk of the United States Court of Appeals for the Seventh Circuit_
ORDER

The slip opinion issued in the above-entitled cause on August 13, 2002 is hereby amended as follows:

On page 9, the second-to-last sentence of the first paragraph (beginning “It is Equitrac’s use of the term...”) should be removed and replaced with the following: “The problem here is not that Equitrac, which repairs Promatek products, used Promatek’s trademark in its metatag, but that it used that trademark in a way calculated to deceive consumers into thinking that Equitrac was Promatek. Id.”

Immediately following the sentence to be inserted above, the following footnote should be inserted: “It is not the case that trademarks can never appear in metatags, but that they may only do so where a legitimate use of the trademark is being made.”
LOCKHEED MARTIN CORPORATION,
Plaintiff-Counter-Defendant-
Appellant,
D.C. No.
v.

NETWORK SOLUTIONS, INC.,
Defendant-Counter-
Claimant-Appellee.

No. 97-56734
CV96-07438-DDP (ANx)

OPINION

Appeal from the United States District Court
for the Central District of California
Dean D. Pregerson, District Judge, Presiding

Argued and Submitted
June 8, 1999--Pasadena, California

Filed October 25, 1999

Before: Dorothy W. Nelson, Stephen Reinhardt, and
Stephen S. Trott, Circuit Judges.

Opinion by Judge Trott

COUNSEL

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

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

OPINION

TROTT, Circuit Judge:

Plaintiff Lockheed Martin Corp. ("Lockheed") appeals
summary judgment in favor of Defendant Network Solutions,
Inc. ("NSI") on Lockheed's action for trademark infringe
ment, unfair competition, dilution, and contributory infringe
ment under the Lanham Trademark Act of 1946, 15 U.S.C. SS 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, No. 98-55810 (9th Cir. August 23, 1999), decision. An interested reader may wish to review the district court's in-depth discussion of the Internet technology that forms the basis of this cause of action. 985 F. Supp. at 951-53.

When a third party seeks to maintain an Internet web site, that party must reserve a location, called an Internet Protocol ("IP") Address, and do the necessary programming. When an Internet user accesses the third party's web site, the user enters the domain-name combination that corresponds to the IP Address and is routed to the host computer. An industry of surrogate hosts has developed, where an Internet Service Provider licenses space on its computers to a third-party web-site operator, permitting the operator to maintain a web site without keeping his or her computer continually connected to the Internet. The Internet Service Providers do not provide the translation service from an entered domain-name combination to the appropriate IP Address. A separate organization has the responsibility to perform the translation function.

A

At all relevant times, NSI was the sole National Science Foundation contractor in charge of registering domain name combinations for the top-level domains <.gov>, <.edu>, <.com>, <.org>, and <.net>. (For clarity, we set off Internet related character strings with the caret symbols ("^>").) After registration, NSI entered the combination and the corresponding IP Address in its database, permitting automatic translation when an Internet user entered a domain-name combination. NSI is no longer the exclusive registrar. Since oral argument on this appeal, a new competitive scheme has been implemented. See Jeri Clausing, 3-Week Delay in Opening Up Internet Name Registration, N.Y. Times, June 28, 1999, at C1.

When registering with NSI to receive a domain-name combination, an applicant submits NSI's "template" electronically over the Internet. On approval, NSI puts the domain-name combination in its database in conjunction with the correct IP
Address. NSI then routes Internet users who enter a certain domain-name combination to the registrant's computer. At the time of argument on this appeal, NSI was receiving approximately 130,000 registrations per month, although evidence indicates that the number of monthly registrations has been increasing steadily and is possibly much larger today. Ninety percent of templates are processed electronically, and the entire registration process for each application requires between a few minutes and a few hours. Ten percent of the time, an employee of NSI reviews the application. Human intervention might occur because of an error in filling out the form or because the applied-for domain name includes a "prohibited" character string—such as specific variations on the words Olympic, Red Cross, or NASA, and certain "obscene" words. NSI also performs a conflict check on all applications, which compares an application to other registered domain-name combinations. However, NSI does not consult third parties during the registration process, check for a registrant's right to use a particular word in a domain-name combination, or monitor the use of a combination once registered. NSI is also not an Internet Service Provider. It performs none of the "hosting" functions for a web site.

NSI does maintain a post-registration dispute-resolution procedure. Anyone who feels that his or her rights are violated by the domain-name combination maintained by a registrant can submit a certified copy of a trademark registration to NSI. NSI then requires the registrant to obtain a declaratory judgment of the right to maintain the domain-name combination. If the registrant fails to do so, its registration is terminated.

B

Lockheed owns and operates "The Skunk Works," an aircraft design and construction laboratory. Since 1943, The Skunk Works has developed prototypes of this country's first jet fighter, the U-2 and SR-71 spy planes, and the F-117 and F-22 fighter planes. The Skunk Works is currently involved in designing a possible replacement for the space shuttle. "Skunk Works" is a registered and incontestable service mark.

II

Third parties, not involved in this litigation, have registered domain-name combinations with NSI which are variations on the phrase "skunk works." These include: <skunkworks.com>, <skunkworks.net>, <skunkwrks.com>, <skunkwerks.com>, <skunkworx.com>, <theskunkworks.com>, <skunkworksl.com>, <skunkworks.org>, <skunkwear.com>, <theskunkwerks.com>, <skunkwrks.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>.

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 cutoff 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. Margolin v. Ryan, 140 F.3d 850, 852 (9th Cir. 1998). Viewing the evidence in the light most favorable to the nonmoving party, summary judgment is appropriate if no genuine issues of material fact remain and the nonmoving 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. Face Am. Group, Inc., 170 F.3d 877, 879 (9th Cir. 1999).

IV

[1] Contributory infringement occurs when the defendant either intentionally induces a third party to infringe the plaintiff's mark or supplies a product to a third party with actual or constructive knowledge that the product is being used to infringe the service mark. Inwood Lab., Inc. v. Ives Lab., Inc., 456 U.S. 844, 853 -54 (1982). Lockheed alleges only the latter basis for contributory infringement liability and therefore must prove that NSI supplies a product to third parties with actual or constructive knowledge that its product is being used to infringe "Skunk Works." Id. at 854.

[2] The district court assumed for purposes of summary judgment that third parties were infringing Lockheed's "Skunk Works" service mark, and NSI does not ask us to
affirm on the alternate ground that no genuine issue of material fact exists as to infringement. We are thus left to consider two issues on Lockheed's contributory infringement cause of action: (1) whether NSI supplied a product to third parties and (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 96062, we affirm summary judgment without reaching the second.

A

Under the plain language of the Inwood Lab. formulation, to be liable for contributory infringement, NSI must supply a "product" to a third party with which the third party infringes Lockheed's service mark.

456 U.S. at 854

In Inwood Lab., the Supreme Court considered an action against a manufacturer of generic pharmaceuticals. Id. at 847. Nonparty pharmacists packaged the defendant's less-expensive generic pills, but labeled them with the plaintiff's brand name. Id. at 850. The plaintiff stated a cause of action for contributory infringement by alleging that the defendant "continued to supply [the product] to pharmacists whom the petitioners knew were mislabeling generic drugs." Id. at 855.

Inwood Lab. has been applied in the broader context of renting booth space at a flea market. See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148-49 (7th Cir. 1992). In Hard Rock, the Seventh Circuit explicitly addressed the distinction between a product and a service, noting that while the pharmaceutical company in Inwood Lab. clearly supplied a product to the third-party pharmacists, a "temporary help service . . . might not be liable if it furnished [to the defendant] the workers he employed to erect his stand." Hard Rock, 955 F.2d at 1148. The court then held that space at a flea market was more comparable to pharmaceuticals than to manpower, in part because of the close comparison between the legal duty owed by a landlord to control illegal activities on his or her premises and by a manufacturer to control illegal use of his or her product. Id. at 1149. We adopted the Hard Rock analysis in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), holding that a flea market could be liable for contributory infringement if it "supplied the necessary marketplace" for the sale of infringing products. Id. at 265 (citing Hard Rock, 955 F.2d at 1149).

[3] Hard Rock and Fonovisa teach us that when measuring and weighing a fact pattern in the contributory infringement context without the convenient "product" mold dealt with in Inwood Lab., we consider the extent of control exercised by the defendant over the third party's means of infringement. Hard Rock, 955 F.2d at 1148-49 (noting the common-law responsibilities of a landlord regarding illegal activity on a rented premises); see Fonovisa, 76 F.3d at 265 (adopting Hard Rock's analysis). Direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark permits the expansion of Inwood Lab.'s "supplies a product" requirement for contributory infringement.
[4] The case at bench involves a fact pattern squarely on the "service" side of the product/service distinction suggested by Inwood Lab and its offspring. All evidence in the record indicates that NSI's role differs little from that of the United States Postal Service: when an Internet user enters a domain name combination, NSI translates the domain name combination to the registrant's IP Address and routes the information or command to the corresponding computer. Although NSI's routing service is only available to a registrant who has paid NSI's fee, NSI does not supply the domain name combination any more than the Postal Service supplies a street address by performing the routine service of routing mail. As the district court correctly observed,

Where domain names are used to infringe, the infringement does not result from NSI's publication of the domain name list, but from the registrant's use of the name on a web site or other Internet form of communication in connection with goods or services. . . . NSI's involvement with the use of domain names does not extend beyond registration.

985 F. Supp. at 958.

[5] The "direct control and monitoring" rule established by Hard Rock and Fonovisa likewise fails to reach the instant situation. The district court correctly recognized that NSI's routine translation service does not entail the kind of direct control and monitoring required to justify an extension of the "supplies a product" requirement. See 985 F. Supp. at 962 ("While the landlord of a flea market might reasonably be expected to monitor the merchandise sold on his premises, NSI cannot reasonably be expected to monitor the Internet."). Such a stretch would reach well beyond the contemplation of Inwood Lab. and its progeny.

In an attempt to fit under Fonovisa's umbrella, Lockheed characterizes NSI's service as a licensing arrangement with alleged third-party infringers. Although we accept Lockheed's argument that NSI licenses its routing service to domain name registrants, the routing service is just that—a service. In Fonovisa and Hard Rock, by contrast, the defendants licensed real estate, with the consequent direct control over the activity that the third-party alleged infringers engaged in on the premises. Hard Rock, 955 F.2d at 1149; see Fonovisa, 96 F.3d at 265.

[6] Lockheed also urges that NSI is liable as a printer or publisher under 15 U.S.C. § 1114(2) (1994), which reads in pertinent part:

[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:

Pornography Defined

- Obscenity defined [Miller]:
  - the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest
  - the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and
  - the work, taken as a whole, lacks serious literary, artistic, political or scientific value

- Child pornography defined [Ferber]: works that visually depict sexual conduct by children below a specified age, where the category of sexual conduct proscribed is suitably limited and described
  - In NY statute's case, "sexual conduct" was "actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masochism, sadomasochistic abuse, or lewd exhibition of the genitals"

- Indecent:
  - "language that describes, in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities and organs, at times of the day when there is a reasonable risk that children may be in the audience" (FCC definition, quoted in Pacifica)
  - "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" [CDA]

- Harmful to Minors [Ginsberg]:
  - "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors
  - appeals to the prurient interests of minors
  - is utterly without redeeming social importance for minors

- Harmful to Minors [COPA]:
  - any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that
  - the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest
  - depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast
  - taken as a whole, lacks serious literary, artistic, political, or scientific value for minors
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." 6 It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought." 7

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

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.
From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. 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." 

Sexually Explicit Material

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest core." These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community." Thus, for example,

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

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

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

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

Age Verification

The problem of age verification differs for different uses of the Internet. The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms." 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). 26 One


8/5/2005
covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications, §223(e)(5)(A). The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code. §223(e)(5)(B).

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

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

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

Judge Dalzell's review of "the special attributes of Internet communication" disclosed by the evidence convinced him that the First Amendment denies Congress the power to regulate the content of protected speech on the Internet. Id., at 867. His opinion explained at length why he believed the Act would abridge significant protected speech, particularly by noncommercial speakers, while "[p]erversely, commercial pornographers would remain relatively unaffected." Id., at 879. He construed our cases as requiring a "medium specific" approach to the analysis of the regulation of mass communication, id., at 873, and concluded that the Internet--as "the most participatory form of mass speech yet developed," id., at 883--is entitled to "the highest protection from governmental intrusion," ibid. 30
The judgment of the District Court enjoins the Government from enforcing the prohibitions in §223(a)(1)(B) insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of §§223(d)(1) and (2) is unqualified because those provisions contain no separate reference to obscenity or child pornography.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Government argues that 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. Each of Miller's additional two prongs--(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lack[s] serious literary, artistic, political, or scientific value"--critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary
community standards. See Pope v. Illinois, 481 U.S. 497, 500 (1987). This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value. The Government's contention that courts will be able to give such legal limitations to the CDA's standards is belied by Miller's own rationale for having juries determine whether material is "patently offensive" according to community standards: that such questions are essentially ones of fact. 39

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

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

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

admonished that "the fact that society may find speech offensive is not a sufficient reason for suppressing it." 438 U.S., at 745.

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

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

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

Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100 person chat group will be minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults. 42

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

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

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and "patently offensive" messages communicated to a 17 year old—no matter how much valuable 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 theproffered 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." 49 The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

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

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

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

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

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

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

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

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

For the foregoing reasons, the judgment of the district court is affirmed.

It is so ordered.

U.S. Supreme Court

No. 96-511

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

on appeal from the united states district court for the eastern district of pennsylvania

[June 26, 1997]

Justice O'Connor, with whom The Chief Justice joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). What the Court classifies as a single "'patently offensive display' " provision, see ante, at 11, is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specificperson" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in any manner available" to minors ("display" provision). §223(d)(1)(B). None of these provisions purports to keep indecent (or patently offensive) material away from adults, who have a First Amendment right to obtain this speech. Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by the First Amendment"). Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access. See S. Conf. Rep. No. 104-230, p. 189 (1996) (CDA imposes "access restrictions . . . to protect minors from exposure to indecent material").

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults. Stateshave also denied minors access to speech deemed to be "harmful to minors." 2 The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is 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 be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone." Thus, the only way for a speaker to avoid liability under the CDA is to refrain completely from using indecent speech. But this forced silence impinges on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." Butler, 352 U.S., at 383. As a result, the "display" provision cannot withstand scrutiny. Accord, Sable Communications, 492 U.S., at 126-131; Bolger v. Young's Drug Products Corp., 463 U.S., at 73-75.

The "indecency transmission" and "specific person" provisions present a closer issue, for they are not unconstitutional in all of their applications. As discussed above, the "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18 years of age. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient of his indecent message is a minor. §223(d)(1)(A). Appellant urges the Court to construe the provision to impose such a knowledge requirement, see Brief for Federal Parties 25-27, and I would do so. See Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress").

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors—e.g., when an adult speaker sends an e-mail knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in Ginsberg. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults. He is not prevented from speaking indecently to other adults in a chat room (because there are no other adults participating in the conversation) and he remains free to send indecent e-mails to other adults. The relevant universe contains only one adult, and the adult in that universe has the power to refrain from using indecent speech and consequently to keep all such speech within the room in an "adult" zone.

The analogy to Ginsberg breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group, since they would be transmitting an indecent message to specific persons, one of whom is a
minor. Accord, ante, at 30. The CDA is therefore akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store. Even assuming such a law might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store, the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. And as discussed below, I do not find that the provisions are overbroad in the sense that they restrict minors' access to a substantial amount of speech that minors have the right to read and view. Accordingly, the CDA can be applied constitutionally in some situations. Normally, this fact would require the Court to reject a direct facial challenge. United States v. Salerno, 481 U.S. 739, 745 (1987) ("A facial challenge to a legislative Act [succeeds only if] the challenger . . . establish[es] that no set of circumstances exists under which the Act would be valid"). Appellees' claim arises under the First Amendment, however, and they argue that the CDA is facially invalid because it is "substantially overbroad"--that is, it "sweeps too broadly . . . [and] penaliz[es] a substantial amount of speech that is constitutionally protected," Forsyth County v. Nationalist Movement, 505 U.S. 123, 130 (1992). See Brief for Appellees American Library Association et al. 48; Brief for Appellees American Civil Liberties Union et al. 39-41. I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication.

This conclusion does not end the matter, however. Where, as here, "the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish . . . [t]he statute may forthwith be declared invalid to the extent that it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 504 (1985). There is no question that Congress intended to prohibit certain communications between one adult and one or more minors. See 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.) (punishing "[w]hoever . . . initiates the transmission of [any indecent communication] knowingly that the recipient of the communication is under 18 years of age"); §223(d)(1)(A) (punishing "[w]hoever . . . send[s] to a specific person or persons under 18 years of age [a patently offensive message]"). There is also no question that Congress would have enacted a narrower version of these provisions had it known a broader version would be declared unconstitutional. 47 U.S.C. § 608 ("If . . . the application of any provision of the CDA to any person or circumstance is held invalid, . . . the application of such provision to other persons or circumstances shall not be affected thereby"). I would therefore sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of Internet communications where the party initiating the communication knows that all of the recipients are minors.

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question. In Ginsberg, the New York law we sustained prohibited the sale to minors of magazines that were "harmful to minors." Under that law, a magazine was "harmful to minors" only if it was obscene as to minors. 390 U.S., at 632-633. Noting that obscene speech is not protected by the First Amendment, Roth v. United States, 354 U.S. 476, 485 (1957), and that New York was constitutionally free to adjust the definition of obscenity for minors, 390 U.S., at 638, the Court concluded that the law did not "inva[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)(1)(B) (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 as 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 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."

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 Conferes' own assertion that the CDA was intended "to establish a uniform national standard of content regulation." S. Conf. Rep., at 191.


[Footnote 41.] The lack of legislative attention to the statute at issue in Sable suggests another parallel with this case. Compare 492 U.S., at 129-130 ("[A]side from conclusory statements during the debates by proponents of the bill, as well as similar assertions in hearings on a substantially identical bill the year before, . . . the congressional record presented to us contains no evidence as to how effective or ineffective the FCC's most recent regulations were or might prove to be. . . . No Congressman or Senator purported to present a considered judgment with respect to how often or to what extent minors could or would circumvent the rules and have access to dial a porn messages") with n. 24, supra.

[Footnote 42.] The Government agrees that these provisions are applicable whenever "a sender transmits a message to more than one recipient, knowing that at least one of the specific persons receiving the message is a minor." Opposition to Motion to Affirm and Reply to Juris. Statement 4-5, n. 1.

[Footnote 43.] The Government asserts that "[t]here is nothing constitutionally suspect about requiring commercial Web site operators . . . to shoulder the modest burdens associated with their use." Brief for Appellants 35. As a matter of fact, however, there is no evidence that a "modest burden" would be effective.

[Footnote 44.] Transmitting obscenity and child pornography, whether via the Internet or other means,
is already illegal under federal law for both adults and juveniles. See 18 U.S.C. §§ 1464-1465 (criminalizing obscenity); §2251 (criminalizing child pornography). In fact, when Congress was considering the CDA, the Government expressed its view that the law was unnecessary because existing laws already authorized its ongoing efforts to prosecute obscenity, child pornography, and child solicitation. See 141 Cong. Rec. S8342 (June 14, 1995) (letter from Kent Markus, Acting Assistant Attorney General, U. S. Department of Justice, to Sen. Leahy).

[ Footnote 45 ] Citing Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993), among other cases, appellees offer an additional reason why, in their view, the CDA fails strict scrutiny. Because so much sexually explicit content originates overseas, they argue, the CDA cannot be "effective." Brief for Appellees American Library Association et al. 33-34. This argument raises difficult issues regarding the intended, as well as the permissible scope of, extraterritorial application of the CDA. We find it unnecessary to address those issues to dispose of this case.

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

[ Footnote 47 ] Thus, ironically, this defense may significantly protect commercial purveyors of obscene postings while providing little (or no) benefit for transmitters of indecent messages that have significant social or artistic value.


[ Footnote 49 ] As this Court long ago explained, "It would certainly be dangerous if the Legislature could set a net large enough to catch all possible offenders and leave it to the courts to step inside and say who could be rightfully 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").


Opinion of the Court

SUPREME COURT OF THE UNITED STATES

No. 03–218

JOHN D. ASHCROFT, ATTORNEY GENERAL,
PETITIONER v. AMERICAN CIVIL
LIBERTIES UNION ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF
APPEALS FOR THE THIRD CIRCUIT

[June 29, 2004]

JUSTICE KENNEDY delivered the opinion of the Court.

This case presents a challenge to a statute enacted by Congress to protect minors from exposure to sexually explicit materials on the Internet, the Child Online Protection Act (COPA). 112 Stat. 2681–736, codified at 47 U. S. C. §231. We must decide whether the Court of Appeals was correct to affirm a ruling by the District Court that enforcement of COPA should be enjoined because the statute likely violates the First Amendment.

In enacting COPA, Congress gave consideration to our earlier decisions on this subject, in particular the decision in Reno v. American Civil Liberties Union, 521 U. S. 844 (1997). For that reason, “the Judiciary must proceed with caution and . . . with care before invalidating the Act.” Ashcroft v. American Civil Liberties Union, 535 U. S. 564, 592 (Ashcroft I) (KENNEDY, J., concurring in judgment). The imperative of according respect to the Congress, however, does not permit us to depart from well-established First Amendment principles. Instead, we must hold the Government to its constitutional burden of proof.

Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard
against that threat the Constitution demands that content-based restrictions on speech be presumed invalid, *R. A. V. v. St. Paul*, 505 U. S. 377, 382 (1992), and that the Government bear the burden of showing their constitutionality. *United States v. Playboy Entertainment Group, Inc.*, 529 U. S. 803, 817 (2000). This is true even when Congress twice has attempted to find a constitutional means to restrict, and punish, the speech in question.

This case comes to the Court on certiorari review of an appeal from the decision of the District Court granting a preliminary injunction. The Court of Appeals reviewed the decision of the District Court for abuse of discretion. Under that standard, the Court of Appeals was correct to conclude that the District Court did not abuse its discretion in granting the preliminary injunction. The Government has failed, at this point, to rebut the plaintiffs' contention that there are plausible less restrictive alternatives to the statute. Substantial practical considerations, furthermore, argue in favor of upholding the injunction and allowing the case to proceed to trial. For those reasons, we affirm the decision of the Court of Appeals upholding the preliminary injunction, and we remand the case so that it may be returned to the District Court for trial on the issues presented.

I

A

COPA is the second attempt by Congress to make the Internet safe for minors by criminalizing certain Internet speech. The first attempt was the Communications Decency Act of 1996, Pub. L. 104–104, §502, 110 Stat. 133, 47 U. S. C. §223 (1994 ed., Supp. II). The Court held the CDA unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available. *Reno, supra.*
In response to the Court's decision in Reno, Congress passed COPA. COPA imposes criminal penalties of a $50,000 fine and six months in prison for the knowing posting, for "commercial purposes," of World Wide Web content that is "harmful to minors." §231(a)(1). Material that is "harmful to minors" is defined as:

"any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that—

"(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

"(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

"(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors." §231(e)(6).

"Minors" are defined as "any person under 17 years of age." §231(e)(7). A person acts for "commercial purposes only if such person is engaged in the business of making such communications." "Engaged in the business," in turn,

"means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the
making or offering to make such communications be
the person’s sole or principal business or source of in-
come.” §231(e)(2).

While the statute labels all speech that falls within
these definitions as criminal speech, it also provides an
affirmative defense to those who employ specified means
to prevent minors from gaining access to the prohibited
materials on their Web site. A person may escape convic-
tion under the statute by demonstrating that he

“has restricted access by minors to material that is
harmful to minors—
“(A) by requiring use of a credit card, debit account,
adult access code, or adult personal identification
number;
“(B) by accepting a digital certificate that verifies age,
or
“(C) by any other reasonable measures that are feasi-
ble under available technology.” §231(c)(1).

Since the passage of COPA, Congress has enacted addi-
tional laws regulating the Internet in an attempt to pro-
tect minors. For example, it has enacted a prohibition on
misleading Internet domain names, 18 U. S. C. A. §2252B
(Supp. 2004), in order to prevent Web site owners from
disguising pornographic Web sites in a way likely to cause
uninterested persons to visit them. See Brief for Peti-
tioner 7 (giving, as an example, the Web site “white-
house.com”). It has also passed a statute creating a “Dot
Kids” second-level Internet domain, the content of which is
restricted to that which is fit for minors under the age of

B

Respondents, Internet content providers and others
concerned with protecting the freedom of speech, filed suit
in the United States District Court for the Eastern Dis-
district of Pennsylvania. They sought a preliminary injunction against enforcement of the statute. After considering testimony from witnesses presented by both respondents and the Government, the District Court issued an order granting the preliminary injunction. The court first noted that the statute would place a burden on some protected speech. *American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473, 495 (1999). The court then concluded that respondents were likely to prevail on their argument that there were less restrictive alternatives to the statute: “On the record to date, it is not apparent . . . that [petitioner] can meet its burden to prove that COPA is the least restrictive means available to achieve the goal of restricting the access of minors” to harmful material. *Id.*, at 497. In particular, it noted that “[t]he record before the Court reveals that blocking or filtering technology may be at least as successful as COPA would be in restricting minors’ access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators.” *Ibid.*

The Government appealed the District Court’s decision to the United States Court of Appeals for the Third Circuit. The Court of Appeals affirmed the preliminary injunction, but on a different ground. 217 F. 3d 162, 166 (2000). The court concluded that the “community standards” language in COPA by itself rendered the statute unconstitutionally overbroad. *Id.*, at 166. We granted certiorari and reversed, holding that the community-standards language did not, standing alone, make the statute unconstitutionally overbroad. *Ashcroft I*, 535 U.S., at 585. We emphasized, however, that our decision was limited to that narrow issue. *Ibid.* We remanded the case to the Court of Appeals to reconsider whether the District Court had been correct to grant the preliminary injunction. On remand, the Court of Appeals again af-
firmed the District Court. 322 F. 3d 240 (2003). The Court of Appeals concluded that the statute was not narrowly tailored to serve a compelling Government interest, was overbroad, and was not the least restrictive means available for the Government to serve the interest of preventing minors from using the Internet to gain access to materials that are harmful to them. Id., at 266–271. The Government once again sought review from this Court, and we again granted certiorari. 540 U.S. 944 (2003).

II

A

“This Court, like other appellate courts, has always applied the abuse of discretion standard on the review of a preliminary injunction.” Walters v. National Assn. of Radiation Survivors, 473 U.S. 305, 336 (1985) (O’CONNOR, J., concurring) (internal quotation marks omitted). “The grant of appellate jurisdiction under [28 U. S. C.] §1252 does not give the Court license to depart from established standards of appellate review.” Ibid. If the underlying constitutional question is close, therefore, we should uphold the injunction and remand for trial on the merits. Applying this mode of inquiry, we agree with the Court of Appeals that the District Court did not abuse its discretion in entering the preliminary injunction. Our reasoning in support of this conclusion, however, is based on a narrower, more specific grounds than the rationale the Court of Appeals adopted. The Court of Appeals, in its opinion affirming the decision of the District Court, construed a number of terms in the statute, and held that COPA, so construed, was unconstitutional. None of those constructions of statutory terminology, however, were relied on by or necessary to the conclusions of the District Court. Instead, the District Court concluded only that the statute was likely to burden some speech that is protected
for adults, 31 F. Supp. 2d, at 495, which petitioner does not dispute. As to the definitional disputes, the District Court concluded only that respondents' interpretation was "not unreasonable," and relied on their interpretation only to conclude that respondents had standing to challenge the statute, id., at 481, which, again, petitioner does not dispute. Because we affirm the District Court's decision to grant the preliminary injunction for the reasons relied on by the District Court, we decline to consider the correctness of the other arguments relied on by the Court of Appeals.

The District Court, in deciding to grant the preliminary injunction, concentrated primarily on the argument that there are plausible, less restrictive alternatives to COPA. A statute that "effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another ... is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve." Reno, 521 U. S., at 874. When plaintiffs challenge a content-based speech restriction, the burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute. Id., at 874.

In considering this question, a court assumes that certain protected speech may be regulated, and then asks what is the least restrictive alternative that can be used to achieve that goal. The purpose of the test is not to consider whether the challenged restriction has some effect in achieving Congress' goal, regardless of the restriction it imposes. The purpose of the test is to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to assure that legitimate speech is not chilled or punished. For that reason, the test does not begin with the status quo of existing regulations, then ask whether the challenged restriction has some additional
ability to achieve Congress' legitimate interest. Any restriction on speech could be justified under that analysis. Instead, the court should ask whether the challenged regulation is the least restrictive means among available, effective alternatives.

In deciding whether to grant a preliminary injunction stage, a district court must consider whether the plaintiffs have demonstrated that they are likely to prevail on the merits. See, e.g., Doran v. Salem Inn, Inc., 422 U. S. 922, 931 (1975). (The court also considers whether the plaintiff has shown irreparable injury, see id., at 931, but the parties in this case do not contest the correctness of the District Court's conclusion that a likelihood of irreparable injury had been established. See 31 F. Supp. 2d, at 497–498). As the Government bears the burden of proof on the ultimate question of COPA's constitutionality, respondents must be deemed likely to prevail unless the Government has shown that respondents' proposed less restrictive alternatives are less effective than COPA. Applying that analysis, the District Court concluded that respondents were likely to prevail. Id., at 496–497. That conclusion was not an abuse of discretion, because on this record there are a number of plausible, less restrictive alternatives to the statute.

The primary alternative considered by the District Court was blocking and filtering software. Blocking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them. The District Court, in granting the preliminary injunction, did so primarily because the plaintiffs had proposed that filters are a less restrictive alternative to COPA and the Government had not shown it would be likely to disprove the plaintiffs' contention at trial. Ibid.

Filters are less restrictive than COPA. They impose selective restrictions on speech at the receiving end, not
universal restrictions at the source. Under a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information. Even adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers. Above all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished. All of these things are true, moreover, regardless of how broadly or narrowly the definitions in COPA are construed.

Filters also may well be more effective than COPA. First, a filter can prevent minors from seeing all pornography, not just pornography posted to the Web from America. The District Court noted in its factfindings that one witness estimated that 40% of harmful-to-minors content comes from overseas. Id., at 484. COPA does not prevent minors from having access to those foreign harmful materials. That alone makes it possible that filtering software might be more effective in serving Congress' goals. Effectiveness is likely to diminish even further if COPA is upheld, because the providers of the materials that would be covered by the statute simply can move their operations overseas. It is not an answer to say that COPA reaches some amount of materials that are harmful to minors; the question is whether it would reach more of them than less restrictive alternatives. In addition, the District Court found that verification systems may be subject to evasion and circumvention, for example by minors who have their own credit cards. See id., at 484, 496–497. Finally, filters also may be more effective because they can be applied to all forms of Internet communication, including e-mail, not just communications available via the World Wide Web.

That filtering software may well be more effective than
COPA is confirmed by the findings of the Commission on Child Online Protection, a blue-ribbon commission created by Congress in COPA itself. Congress directed the Commission to evaluate the relative merits of different means of restricting minors' ability to gain access to harmful materials on the Internet. Note following 47 U. S. C. §231. It unambiguously found that filters are more effective than age-verification requirements. See Commission on Child Online Protection (COPA), Report to Congress, at 19-21, 23-25, 27 (Oct. 20, 2000) (assigning a score for "Effectiveness" of 7.4 for server-based filters and 6.5 for client-based filters, as compared to 5.9 for independent adult-id verification, and 5.5 for credit card verification). Thus, not only has the Government failed to carry its burden of showing the District Court that the proposed alternative is less effective, but also a Government Commission appointed to consider the question has concluded just the opposite. That finding supports our conclusion that the District Court did not abuse its discretion in enjoining the statute.

Filtering software, of course, is not a perfect solution to the problem of children gaining access to harmful-to-minors materials. It may block some materials that are not harmful to minors and fail to catch some that are. See 31 F. Supp. 2d, at 492. Whatever the deficiencies of filters, however, the Government failed to introduce specific evidence proving that existing technologies are less effective than the restrictions in COPA. The District Court made a specific factfinding that "[n]o evidence was presented to the Court as to the percentage of time that blocking and filtering technology is over- or underinclusive." Ibid. In the absence of a showing as to the relative effectiveness of COPA and the alternatives proposed by respondents, it was not an abuse of discretion for the District Court to grant the preliminary injunction. The Government's burden is not merely to show that a pro-
Opinion of the Court

proposed less restrictive alternative has some flaws; its burden is to show that it is less effective. *Reno*, 521 U. S., at 874. It is not enough for the Government to show that COPA has some effect. Nor do respondents bear a burden to introduce, or offer to introduce, evidence that their proposed alternatives are more effective. The Government has the burden to show they are less so. The Government having failed to carry its burden, it was not an abuse of discretion for the District Court to grant the preliminary injunction.

One argument to the contrary is worth mentioning—the argument that filtering software is not an available alternative because Congress may not require it to be used. That argument carries little weight, because Congress undoubtedly may act to encourage the use of filters. We have held that Congress can give strong incentives to schools and libraries to use them. *United States v. American Library Assn., Inc.*, 539 U. S. 194 (2003). It could also take steps to promote their development by industry, and their use by parents. It is incorrect, for that reason, to say that filters are part of the current regulatory status quo. The need for parental cooperation does not automatically disqualify a proposed less restrictive alternative. *Playboy Entertainment Group*, 529 U. S., at 824. (“A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act”). In enacting COPA, Congress said its goal was to prevent the “widespread availability of the Internet” from providing “opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control.” Congressional Findings, note following 47 U. S. C. §231 (quoting Pub. L. 105–277, Tit. XIV, §1402(1), 112 Stat. 2681–736). COPA presumes that parents lack the ability, not the will, to monitor what their children see. By enacting programs to promote use of
filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties.

The closest precedent on the general point is our decision in *Playboy Entertainment Group*. *Playboy Entertainment Group*, like this case, involved a content-based restriction designed to protect minors from viewing harmful materials. The choice was between a blanket speech restriction and a more specific technological solution that was available to parents who chose to implement it. 529 U.S., at 825. Absent a showing that the proposed less restrictive alternative would not be as effective, we concluded, the more restrictive option preferred by Congress could not survive strict scrutiny. *Id.*, at 826 (reversing because “[t]he record is silent as to the comparative effectiveness of the two alternatives”). In the instant case, too, the Government has failed to show, at this point, that the proposed less restrictive alternative will be less effective. The reasoning of *Playboy Entertainment Group*, and the holdings and force of our precedents require us to affirm the preliminary injunction. To do otherwise would be to do less than the First Amendment commands. “The starch in our constitutional standards cannot be sacrificed to accommodate the enforcement choices of the Government.” *Id.*, at 830 (THOMAS, J., concurring).

B

There are also important practical reasons to let the injunction stand pending a full trial on the merits. First, the potential harms from reversing the injunction outweigh those of leaving it in place by mistake. Where a prosecution is a likely possibility, yet only an affirmative defense is available, speakers may self-censor rather than risk the perils of trial. There is a potential for extraordinary harm and a serious chill upon protected speech. Cf. *id.*, at 817 (“Error in marking that line exacts an extraordinary cost”). The harm done from letting the injunction
stand pending a trial on the merits, in contrast, will not be extensive. No prosecutions have yet been undertaken under the law, so none will be disrupted if the injunction stands. Further, if the injunction is upheld, the Government in the interim can enforce obscenity laws already on the books.

Second, there are substantial factual disputes remaining in the case. As mentioned above, there is a serious gap in the evidence as to the effectiveness of filtering software. See supra, at 9. For us to assume, without proof, that filters are less effective than COPA would usurp the District Court's factfinding role. By allowing the preliminary injunction to stand and remanding for trial, we require the Government to shoulder its full constitutional burden of proof respecting the less restrictive alternative argument, rather than excuse it from doing so.

Third, and on a related point, the factual record does not reflect current technological reality—a serious flaw in any case involving the Internet. The technology of the Internet evolves at a rapid pace. Yet the factfindings of the District Court were entered in February 1999, over five years ago. Since then, certain facts about the Internet are known to have changed. Compare, e.g., 31 F. Supp. 2d, at 481 (36.7 million Internet hosts as of July 1998) with Internet Systems Consortium, Internet Domain Survey, Jan. 2004, http://www.isc.org/index.pl?ops/ds (as visited June 22, 2004, and available in the Clerk of Court's case file) (233.1 million hosts as of Jan. 2004). It is reasonable to assume that other technological developments important to the First Amendment analysis have also occurred during that time. More and better filtering alternatives may exist than when the District Court entered its findings. Indeed, we know that after the District Court entered its factfindings, a congressionally appointed commission issued a report that found that filters are more effective than verification screens. See supra, at 8.
Delay between the time that a district court makes factfindings and the time that a case reaches this Court is inevitable, with the necessary consequence that there will be some discrepancy between the facts as found and the facts at the time the appellate court takes up the question. See, e.g., Benjamin, Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process, 78 Texas L. Rev. 269, 290–296 (1999) (noting the problems presented for appellate courts by changing facts in the context of cases involving the Internet, and giving as a specific example the Court's decision in Reno, 521 U.S. 844). We do not mean, therefore, to set up an insuperable obstacle to fair review. Here, however, the usual gap has doubled because the case has been through the Court of Appeals twice. The additional two years might make a difference. By affirming the preliminary injunction and remanding for trial, we allow the parties to update and supplement the factual record to reflect current technological realities.

Remand will also permit the District Court to take account of a changed legal landscape. Since the District Court made its factfindings, Congress has passed at least two further statutes that might qualify as less restrictive alternatives to COPA—a prohibition on misleading domain names, and a statute creating a minors-safe “Dot Kids” domain. See supra, at 4. Remanding for trial will allow the District Court to take into account those additional potential alternatives.

On a final point, it is important to note that this opinion does not hold that Congress is incapable of enacting any regulation of the Internet designed to prevent minors from gaining access to harmful materials. The parties, because of the conclusion of the Court of Appeals that the statute's definitions rendered it unconstitutional, did not devote their attention to the question whether further evidence might be introduced on the relative restrictiveness and
effectiveness of alternatives to the statute. On remand, however, the parties will be able to introduce further evidence on this point. This opinion does not foreclose the District Court from concluding, upon a proper showing by the Government that meets the Government’s constitutional burden as defined in this opinion, that COPA is the least restrictive alternative available to accomplish Congress’ goal.

* * *

On this record, the Government has not shown that the less restrictive alternatives proposed by respondents should be disregarded. Those alternatives, indeed, may be more effective than the provisions of COPA. The District Court did not abuse its discretion when it entered the preliminary injunction. The judgment of the Court of Appeals is affirmed, and the case is remanded for proceedings consistent with this opinion.

It is so ordered.
Breyer, J., dissenting

SUPREME COURT OF THE UNITED STATES

No. 03–218

JOHN D. ASHCROFT, ATTORNEY GENERAL,
PETITIONER v. AMERICAN CIVIL
LIBERTIES UNION ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF
APPEALS FOR THE THIRD CIRCUIT

[June 29, 2004]

Justice Breyer, with whom The Chief Justice and
Justice O'Connor join, dissenting.

The Child Online Protection Act (Act), 47 U. S. C. §231,
seeks to protect children from exposure to commercial
pornography placed on the Internet. It does so by requir-
ing commercial providers to place pornographic material
behind Internet "screens" readily accessible to adults who
produce age verification. The Court recognizes that we
should "proceed . . . with care before invalidating the
Act," while pointing out that the "imperative of according
respect to the Congress . . . does not permit us to depart
from well-established First Amendment principles." Ante,
at 1. I agree with these generalities. Like the Court, I
would subject the Act to "the most exacting scrutiny,"
Turner Broadcasting System, Inc. v. FCC, 512 U. S. 622, 642
(1994), requiring the Government to show that any restric-
tion of nonobscene expression is "narrowly drawn" to
further a "compelling interest" and that the restriction
amounts to the "least restrictive means" available to fur-
ther that interest, Sable Communications of Cal., Inc. v.
Telecommunications Consortium, Inc. v. FCC, 518 U. S.

Nonetheless, my examination of (1) the burdens the Act
imposes on protected expression, (2) the Act’s ability to further a compelling interest, and (3) the proposed “less restrictive alternatives” convinces me that the Court is wrong. I cannot accept its conclusion that Congress could have accomplished its statutory objective—protecting children from commercial pornography on the Internet—in other, less restrictive ways.

I

Although the Court rests its conclusion upon the existence of less restrictive alternatives, I must first examine the burdens that the Act imposes upon protected speech. That is because the term “less restrictive alternative” is a comparative term. An “alternative” is “less restrictive” only if it will work less First Amendment harm than the statute itself, while at the same time similarly furthering the “compelling” interest that prompted Congress to enact the statute. Unlike the majority, I do not see how it is possible to make this comparative determination without examining both the extent to which the Act regulates protected expression and the nature of the burdens it imposes on that expression. That examination suggests that the Act, properly interpreted, imposes a burden on protected speech that is no more than modest.

A

The Act’s definitions limit the material it regulates to material that does not enjoy First Amendment protection, namely legally obscene material, and very little more. A comparison of this Court’s definition of unprotected, “legally obscene,” material with the Act’s definitions makes this clear.

Material is legally obscene if

“(a) . . . ‘the average person, applying contemporary community standards’ would find that the work, taken as a whole, appeals to the prurient interest . . . ; (b) . . . the work depicts or describes, in a patently of-
BREYER, J., dissenting

fensive way, sexual conduct specifically defined by the applicable state law; and (c) ... the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." Miller v. California, 413 U.S. 15, 24 (1973).

The present statute defines the material that it regulates as material that meets all of the following criteria:

"(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, [that the material] is designed to appeal to, or is designed to pander to, the prurient interest;

"(B) [the material] depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

"(C) [the material] taken as a whole, lacks serious literary, artistic, political, or scientific value for minors."


Both definitions define the relevant material through use of the critical terms "prurient interest" and "lacks serious literary, artistic, political, or scientific value." Insofar as material appeals to, or panders to, "the prurient interest," it simply seeks a sexual response. Insofar as "patently offensive" material with "no serious value" simply seeks that response, it does not seek to educate, it does not seek to elucidate views about sex, it is not artistic, and it is not literary. Compare, e.g., Erznoznik v. Jacksonville, 422 U.S. 205, 213 (1975) (invalidating an ordinance regulating nudity in films, where the ban was not confined to "sexually explicit nudity" or otherwise limited), with Ginsburg v. United States, 383 U.S. 463, 471 (1966) (finding unprotected material that was "created, represented, and
sold solely as a claimed instrument of the sexual stimulation it would bring"). That is why this Court, in Miller, held that the First Amendment did not protect material that fits its definition.

The only significant difference between the present statute and Miller’s definition consists of the addition of the words “with respect to minors,” §231(e)(6)(A), and “for minors,” §231(e)(6)(C). But the addition of these words to a definition that would otherwise cover only obscenity expands the statute’s scope only slightly. That is because the material in question (while potentially harmful to young children) must, first, appeal to the “prurient interest” of, i.e., seek a sexual response from, some group of adolescents or postadolescents (since young children normally do not so respond). And material that appeals to the “prurient interest[s]” of some group of adolescents or postadolescents will almost inevitably appeal to the “prurient interest[s]” of some group of adults as well.

The “lack of serious value” requirement narrows the statute yet further—despite the presence of the qualification “for minors.” That is because one cannot easily imagine material that has serious literary, artistic, political, or scientific value for a significant group of adults, but lacks such value for any significant group of minors. Thus, the statute, read literally, insofar as it extends beyond the legally obscene, could reach only borderline cases. And to take the words of the statute literally is consistent with Congress’ avowed objective in enacting this law; namely, putting material produced by professional pornographers behind screens that will verify the age of the viewer. See S. Rep. No. 105–225, p. 3 (1998) (hereinafter S. Rep.) (“The bill seeks to restrict access to commercial pornography on the Web by requiring those engaged in the business of the commercial distribution of material that is harmful to minors to take certain prescribed steps to restrict access to such material by
BREYER, J., dissenting


These limitations on the statute’s scope answer many of the concerns raised by those who attack its constitutionality. Respondents fear prosecution for the Internet posting of material that does not fall within the statute’s ambit as limited by the “prurient interest” and “no serious value” requirements; for example: an essay about a young man’s experience with masturbation and sexual shame; “a serious discussion about birth control practices, homosexuality, . . . or the consequences of prison rape”; an account by a 15-year-old, written for therapeutic purposes, of being raped when she was 13; a guide to self-examination for testicular cancer; a graphic illustration of how to use a condom; or any of the other postings of modern literary or artistic works or discussions of sexual identity, homosexuality, sexually transmitted diseases, sex education, or safe sex, let alone Aldous Huxley’s Brave New World, J. D. Salinger’s Catcher in the Rye, or, as the complaint would have it, “Ken Starr’s report on the Clinton-Lewinsky scandal.” See G. Dillard, Shame on Me, Lodging 609–612; Reno v. American Civil Liberties Union, 521 U.S. 844, 871 (1997); Brief for Respondents 29 (citing Lodging 732–736); Brief for American Society of Journalists and Authors et al. as Amici Curiae 8, and n. 7 (referring to a guide on the medical advice site www.afraidtoask.com); 322 F. 3d 240, 268 (CA3 2003) (citing Safer Sex Institute, safersex.org/condoms/how.to.use); Complaint ¶1, Lodging 40–41 (“a Mapplethorpe photograph,” referring to the work of controversial artist Robert Mapplethorpe); Id., at 667–669 (Pl. Exh. 80, PlanetOut Youth Message Boards (Internet discussion board for gay teens)); declaration of Adam K.
Breyer, J., dissenting

Glickman, president and CEO, Addazi, Inc. d/b/a Condomania, Supp. Lodging of Petitioner 4–10 (describing how Web site has been used for health education); declaration of Roberta Spyer, president and publisher, OBGYN.net, id., at 15–16 (describing Web site as resource for obstetrics, gynecology, and women's health issues); Brief for Volunteer Lawyers for the Arts et al. as Amici Curiae 15 (listing works of literature removed from some schools); Complaint ¶1, Lodging 40–41.

These materials are not both (1) "designed to appeal to, or . . . pander to, the prurient interest" of significant groups of minors and (2) lacking in "serious literary, artistic, political, or scientific value" for significant groups of minors. §§231(e)(6)(A), (C). Thus, they fall outside the statute's definition of the material that it restricts, a fact the Government acknowledged at oral argument. Tr. of Oral Arg. 50–51.

I have found nothing elsewhere in the statute's language that broadens its scope. Other qualifying phrases, such as "taking the material as a whole," §§231(e)(6)(A), (C), and "for commercial purposes," §231(a)(1), limit the statute's scope still more, requiring, for example, that individual images be considered in context. See Roth v. United States, 354 U. S. 476, 490 (1957). In sum, the Act's definitions limit the statute's scope to commercial pornography. It affects unprotected obscene material. Given the inevitable uncertainty about how to characterize close-to-obscene material, it could apply to (or chill the production of) a limited class of borderline material that courts might ultimately find is protected. But the examples I have just given fall outside that class.

B

The Act does not censor the material it covers. Rather, it requires providers of the "harmful to minors" material to restrict minors' access to it by verifying age. They can do so by inserting screens that verify age using a credit card,
adult personal identification number, or other similar technology. See §231(c)(1). In this way, the Act requires creation of an internet screen that minors, but not adults, will find difficult to bypass.

I recognize that the screening requirement imposes some burden on adults who seek access to the regulated material, as well as on its providers. The cost is, in part, monetary. The parties agreed that a Web site could store card numbers or passwords at between 15 and 20 cents per number. American Civil Liberties Union v. Reno, 31 F. Supp. 2d 473, 488–489, ¶¶45–47 (ED Pa. 1999). And verification services provide free verification to Web site operators, while charging users less than $20 per year. Id., at 489–490, ¶¶48–53. According to the trade association for the commercial pornographers who are the statute's target, use of such verification procedures is "standard practice" in their online operations. See S. Rep., at 7; Legislative Proposals to Protect Children from Inappropriate Materials on the Internet: Hearing on H. R. 3783 et al. before the House Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, 105th Cong., 2d Sess., 46, 48 (1998) (prepared statement of Jeffrey J. Douglas, Executive Director and Chairman, Free Speech Coalition (calling the proposed child-protecting mechanisms "effective and appropriate")).

In addition to the monetary cost, and despite strict requirements that identifying information be kept confidential, see 47 U. S. C. §§231(d)(1), 501, the identification requirements inherent in age-screening may lead some users to fear embarrassment. See 31 F. Supp. 2d, at 495. Both monetary costs and potential embarrassment can deter potential viewers and, in that sense, the statute's requirements may restrict access to a site. But this Court has held that in the context of congressional efforts to protect children, restrictions of this kind do not automati-
Breyer, J., dissenting

cally violate the Constitution. And the Court has approved their use. See, e.g., United States v. American Library Assn., Inc., 539 U. S. 194, 209 (2003) (plurality opinion) ("[T]he Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment"). Cf. Reno, 521 U. S., at 890 (O'Connor, J., concurring in judgment in part and dissenting in part) (calling the age-verification requirement similar to "a bouncer [who] checks a person's driver's license before admitting him to a nightclub").

In sum, the Act at most imposes a modest additional burden on adult access to legally obscene material, perhaps imposing a similar burden on access to some protected borderline obscene material as well.

II

I turn next to the question of "compelling interest," that of protecting minors from exposure to commercial pornography. No one denies that such an interest is "compelling." See Denver Area Ed. Telecommunications Consortium, Inc., 518 U. S., at 743 (opinion of Breyer, J.) (interest in protecting minors is "compelling"); Sable Communications, 492 U. S., at 126 (same); Ginsberg v. New York, 390 U. S. 629, 639–640 (1968). Rather, the question here is whether the Act, given its restrictions on adult access, significantly advances that interest. In other words, is the game worth the candle?

The majority argues that it is not, because of the existence of "blocking and filtering software." Ante, at 8–12. The majority refers to the presence of that software as a "less restrictive alternative." But that is a misnomer—a misnomer that may lead the reader to believe that all we need do is look to see if the blocking and filtering software is less restrictive; and to believe that, because in one sense it is (one can turn off the software), that is the end of the constitutional matter.

But such reasoning has no place here. Conceptually
speaking, the presence of filtering software is not an alternate legislative approach to the problem of protecting children from exposure to commercial pornography. Rather, it is part of the status quo, i.e., the backdrop against which Congress enacted the present statute. It is always true, by definition, that the status quo is less restrictive than a new regulatory law. It is always less restrictive to do nothing than to do something. But “doing nothing” does not address the problem Congress sought to address—namely that, despite the availability of filtering software, children were still being exposed to harmful material on the Internet.

Thus, the relevant constitutional question is not the question the Court asks: Would it be less restrictive to do nothing? Of course it would be. Rather, the relevant question posits a comparison of (a) a status quo that includes filtering software with (b) a change in that status quo that adds to it an age-verification screen requirement. Given the existence of filtering software, does the problem Congress identified remain significant? Does the Act help to address it? These are questions about the relation of the Act to the compelling interest. Does the Act, compared to the status quo, significantly advance the ball? (An affirmative answer to these questions will not justify “[a]ny restriction on speech,” as the Court claims, ante, at 8, for a final answer in respect to constitutionality must take account of burdens and alternatives as well.)

The answers to these intermediate questions are clear: Filtering software, as presently available, does not solve the “child protection” problem. It suffers from four serious inadequacies that prompted Congress to pass legislation instead of relying on its voluntary use. First, its filtering is faulty, allowing some pornographic material to pass through without hindrance. Just last year, in American Library Assn., JUSTICE STEVENS described “fundamental defects in the filtering software that is now available or
that will be available in the foreseeable future." 539 U. S., at 221 (dissenting opinion). He pointed to the problem of underblocking: "Because the software relies on key words or phrases to block undesirable sites, it does not have the capacity to exclude a precisely defined category of images." ibid. That is to say, in the absence of words, the software alone cannot distinguish between the most obscene pictorial image and the Venus de Milo. No Member of this Court disagreed.

Second, filtering software costs money. Not every family has the $40 or so necessary to install it. See 31 F. Supp. 2d, at 492, ¶65. By way of contrast, age screening costs less. See supra, at 7 (citing costs of up to 20 cents per password or $20 per user for an identification number).

Third, filtering software depends upon parents willing to decide where their children will surf the Web and be able to enforce that decision. As to millions of American families, that is not a reasonable possibility. More than 28 million school age children have both parents or their sole parent in the work force, at least 5 million children are left alone at home without supervision each week, and many of those children will spend afternoons and evenings with friends who may well have access to computers and more lenient parents. See United States v. Playboy Entertainment Group, Inc., 529 U. S. 803, 842 (2000) (Breyer, J., dissenting).

Fourth, software blocking lacks precision, with the result that those who wish to use it to screen out pornography find that it blocks a great deal of material that is valuable. As Justice Stevens pointed out, "the software's reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as pornography or sex." American Library
Breyer, J., dissenting

Assn., supra, at 222 (internal quotation marks and citations omitted). Indeed, the American Civil Liberties Union (ACLU), one of the respondents here, told Congress that filtering software "block[s] out valuable and protected information, such as information about the Quaker religion, and web sites including those of the American Association of University Women, the AIDS Quilt, the Town Hall Political Site (run by the Family Resource Center, Christian Coalition and other conservative groups)." Hearing on Internet Indecency before the Senate Committee on Commerce, Science, and Transportation, 105th Cong., 2d Sess., 64 (1998). The software "is simply incapable of discerning between constitutionally protected and unprotected speech." Id., at 65. It "inappropriately blocks valuable, protected speech, and does not effectively block the sites [it is] intended to block." Id., at 66 (citing reports documenting overblocking).

Nothing in the District Court record suggests the contrary. No respondent has offered to produce evidence at trial to the contrary. No party has suggested, for example, that technology allowing filters to interpret and discern among images has suddenly become, or is about to become, widely available. Indeed, the Court concedes that "[f]iltering software, of course, is not a perfect solution to the problem." Ante, at 10.

In sum, a "filtering software status quo" means filtering that underblocks, imposes a cost upon each family that uses it, fails to screen outside the home, and lacks precision. Thus, Congress could reasonably conclude that a system that relies entirely upon the use of such software is not an effective system. And a law that adds to that system an age-verification screen requirement significantly increases the system's efficacy. That is to say, at a modest additional cost to those adults who wish to obtain access to a screened program, that law will bring about better, more precise blocking, both inside and outside the home.
The Court's response—that 40% of all pornographic material may be of foreign origin—is beside the point. *Ante*, at 9 (citing the District Court's findings). Even assuming (I believe unrealistically) that all foreign originators will refuse to use screening, the Act would make a difference in respect to 60% of the Internet's commercial pornography. I cannot call that difference insignificant.

The upshot is that Congress could reasonably conclude that, despite the current availability of filtering software, a child protection problem exists. It also could conclude that a precisely targeted regulatory statute, adding an age-verification requirement for a narrow range of material, would more effectively shield children from commercial pornography.

Is this justification sufficient? The lower courts thought not. But that is because those courts interpreted the Act as imposing far more than a modest burden. They assumed an interpretation of the statute in which it reached far beyond legally obscene and borderline-obscene material, affecting material that, given the interpretation set forth above, would fall well outside the Act's scope. But we must interpret the Act to save it, not to destroy it. *NLRB v. Jones & Laughlin Steel Corp.*, 301 U. S. 1, 30 (1937). So interpreted, see *supra*, at 3–6, the Act imposes a far lesser burden on access to protected material. Given the modest nature of that burden and the likelihood that the Act will significantly further Congress' compelling objective, the Act may well satisfy the First Amendment's stringent tests. Cf. *Sable Communications*, 492 U. S., at 130. Indeed, it does satisfy the First Amendment unless, of course, there is a genuine alternative, "less restrictive" way similarly to further that objective.

III

I turn, then, to the actual "less restrictive alternatives" that the Court proposes. The Court proposes two real
alternatives, *i.e.*, two potentially less restrictive ways in which Congress might alter the status quo in order to achieve its "compelling" objective.

First, the Government might "act to encourage" the use of blocking and filtering software. *Ante*, at 11. The problem is that any argument that rests upon this alternative proves too much. If one imagines enough government resources devoted to the problem and perhaps additional scientific advances, then, of course, the use of software might become as effective and less restrictive. Obviously, the Government could give all parents, schools, and Internet cafes free computers with filtering programs already installed, hire federal employees to train parents and teachers on their use, and devote millions of dollars to the development of better software. The result might be an alternative that is extremely effective.

But the Constitution does not, because it cannot, require the Government to disprove the existence of magic solutions, *i.e.*, solutions that, put in general terms, will solve any problem less restrictively but with equal effectiveness. Otherwise, "the undoubted ability of lawyers and judges," who are not constrained by the budgetary worries and other practical parameters within which Congress must operate, "to imagine some kind of slightly less drastic or restrictive an approach would make it impossible to write laws that deal with the harm that called the statute into being." *Playboy Entertainment Group*, 529 U.S., at 841 (BREYER, J., dissenting). As Justice Blackmun recognized, a "judge would be unimaginative indeed if he could not come up with something a little less 'drastic' or a little less 'restrictive' in almost any situation, and thereby enable himself to vote to strike legislation down." *Illinois Bd. of Elections v. Socialist Workers Party*, 440 U.S. 173, 188-189 (1979) (concurring opinion). Perhaps that is why no party has argued seriously that additional expenditure of government funds to encourage the use of screening is a "less
restrictive alternative."

Second, the majority suggests decriminalizing the statute, noting the "chilling effect" of criminalizing a category of speech. Ante, at 9. To remove a major sanction, however, would make the statute less effective, virtually by definition.

IV

My conclusion is that the Act, as properly interpreted, risks imposition of minor burdens on some protected material—burdens that adults wishing to view the material may overcome at modest cost. At the same time, it significantly helps to achieve a compelling congressional goal, protecting children from exposure to commercial pornography. There is no serious, practically available "less restrictive" way similarly to further this compelling interest. Hence the Act is constitutional.

V

The Court's holding raises two more general questions. First, what has happened to the "constructive discourse between our courts and our legislatures" that "is an integral and admirable part of the constitutional design"? Blakely v. Washington, ante, at 1 (KENNEDY, J., dissenting). After eight years of legislative effort, two statutes, and three Supreme Court cases the Court sends this case back to the District Court for further proceedings. What proceedings? I have found no offer by either party to present more relevant evidence. What remains to be litigated? I know the Court says that the parties may "introduce further evidence" as to the "relative restrictiveness and effectiveness of alternatives to the statute." Ante, at 14–15. But I do not understand what that new evidence might consist of.

Moreover, Congress passed the current statute "[i]n response to the Court's decision in Reno" striking down an
earlier statutory effort to deal with the same problem. Ante, at 3. Congress read Reno with care. It dedicated itself to the task of drafting a statute that would meet each and every criticism of the predecessor statute that this Court set forth in Reno. It incorporated language from the Court’s precedents, particularly the Miller standard, virtually verbatim. Compare 413 U. S., at 24, with §231(e)(6). And it created what it believed was a statute that would protect children from exposure to obscene professional pornography without obstructing adult access to material that the First Amendment protects. See H. R. Rep., at 5 (explaining that the bill was “carefully drafted to respond to the Supreme Court’s decision in Reno”); S. Rep., at 2 (same). What else was Congress supposed to do?

I recognize that some Members of the Court, now or in the past, have taken the view that the First Amendment simply does not permit Congress to legislate in this area. See, e.g., Ginzburg, 383 U. S., at 476 (Black, J., dissenting) (“[T]he Federal Government is without any power whatever under the Constitution to put any type of burden on speech and expression of ideas of any kind”). Others believe that the Amendment does not permit Congress to legislate in certain ways, e.g., through the imposition of criminal penalties for obscenity. See, e.g., ante, at 2 (STEVENS, J., concurring). There are strong constitutional arguments favoring these views. But the Court itself does not adopt those views. Instead, it finds that the Government has not proved the nonexistence of “less restrictive alternatives.” That finding, if appropriate here, is universally appropriate. And if universally appropriate, it denies to Congress, in practice, the legislative leeway that the Court’s language seem to promise. If this statute does not pass the Court’s “less restrictive alternative” test, what does? If nothing does, then the Court should say so clearly.
As I have explained, I believe the First Amendment permits an alternative holding. We could construe the statute narrowly—as I have tried to do—removing nearly all protected material from its scope. By doing so, we could reconcile its language with the First Amendment’s demands. We would “save” the statute, “not . . . destroy it.” NLRB, 301 U. S., at 30. Accord, McConnell v. Federal Election Comm’n, 540 U. S. __, __ (2003) (slip op., at 72) (where a saving construction of the statute’s language “is fairly possible,” we must adopt it (quoting Crowell v. Benson, 285 U. S. 22, 62 (1932))). And in the process, we would permit Congress to achieve its basic child-protecting objectives.

Second, will the majority’s holding in practice mean greater or lesser protection for expression? I do not find the answer to this question obvious. The Court’s decision removes an important weapon from the prosecutorial arsenal. That weapon would have given the Government a choice—a choice other than “ban totally or do nothing at all.” The Act tells the Government that, instead of prosecuting bans on obscenity to the maximum extent possible (as respondents have urged as yet another “alternative”), it can insist that those who make available material that is obscene or close to obscene keep that material under wraps, making it readily available to adults who wish to see it, while restricting access to children. By providing this third option—a “middle way”—the Act avoids the need for potentially speech-spressing prosecutions.

That matters in a world where the obscene and the nonobscene do not come tied neatly into separate, easily distinguishable, packages. In that real world, this middle way might well have furthered First Amendment interests by tempering the prosecutorial instinct in borderline cases. At least, Congress might have so believed. And this likelihood, from a First Amendment perspective, might ultimately have proved more protective of the rights
BREYER, J., dissenting

of viewers to retain access to expression than the all-or-nothing choice available to prosecutors in the wake of the majority's opinion.

For these reasons, I dissent.
§ 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.

[1] So in original. Probably should be “subparagraph (A).”
U.S. 4th Circuit Court of Appeals

ZERAN v AMERICA ONLINE INC

PUBLISHED UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT KENNETH M. ZERAN, Plaintiff-Appellant,
v.

AMERICA ONLINE, INCORPORATED, Defendant-Appellee. Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. T. S. Ellis, III, District Judge. (CA-96-1564-A)

Argued: October 2, 1997

Decided: November 12, 1997

Before WILKINSON, Chief Judge, RUSSELL, Circuit Judge, and BOYLE, Chief United States District Judge for the Eastern District of North Carolina, sitting by designation.

Affirmed by published opinion. Chief Judge Wilkinson wrote the opinion, in which Judge Russell and Chief Judge Boyle joined.

COUNSEL ARGUED: John Saul Edwards, LAW OFFICES OF JOHN S.


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 pursuing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of

angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

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

Meanwhile, an announcer for Oklahoma City radio station KRKO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRKO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRKO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRKO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages. 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 defama-
tory material. Section 230 entered this litigation as an affirmative
defense pled by AOL. The company claimed that Congress immu-
ized 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 free-
dom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communica-
tions 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 mini-
num 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 Con-
gress acted to keep government regulation of the Internet to a mini-
mum, 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 com-
puter." 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 evi-
dent. 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 sub-
scribers"). The amount of information


8/5/2005
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 num- ber and type of messages
posted. Congress considered the weight of the speech interests implicated and
chose to immunize service provid- ers to avoid any such restrictive effect.

Another important purpose of § 230 was to encourage service pro-
viders 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,
There, the plaintiffs sued Prodigy -- an interactive computer service like AOL --
for defama-
tory 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 rea-
soned that Prodigy acted more like an
original publisher than a dis-
tributor 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 dis-
semination of offensive material on their
services risked subjecting themselves to liability, because such regulation cast
the service pro-
vider 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 chil-
dren's access to
objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). In line
with this purpose, § 230 forbids the impos-
sion 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
Zeran, interactive computer service providers like AOL are normally considered
instead to be distributors, like traditional news vendors or book sellers. Dis-
tributors 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 lia-
ibility is predicated. Id.
at 811 (explaining that distributors are not lia-
ble "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 misapplies, 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.

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

Our view that Zeran's complaint treats AOL as a publisher is reinforced because AOL is cast in the same position as the party who originally posted the offensive messages. According to Zeran's logic, AOL is legally at fault because it communicated to third parties an allegedly defamatory statement. This is precisely the theory under which the original poster of the offensive messages would be found liable. If the original party is considered a publisher of the offensive messages, Zeran certainly cannot attach liability to AOL under the same theory without conceding that AOL too must be treated as a publisher of the statements.

Zeran next contends that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA. Like the strict liability imposed by the Stratton Oakmont court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement -- from any party, concerning any message. Each notification would require a careful yet rapid investi- gation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossi- ble 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 discretionary calls"). Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not. See Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 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." It is "a unique and wholly new medium of worldwide human communication." 117 S. Ct. at 2334 (citation omitted). Application of the canon invoked by Zeran here would significantly lessen Congress' power, derived from the Commerce Clause, to act in a field whose international character is apparent. While Congress allowed for the enforcement of "any State law that is consistent with [§ 230]," 47 U.S.C. § 230(d)(3), it is equally plain that Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action. Section 230(d)(3) continues: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." With respect to federal-state preemption, the Court has advised: "[W]hen Congress has 'unmistakably . . . ordained,' that its enactments alone are to regulate a part of com-merce, state laws regulating that aspect of commerce must fall. The result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose." Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977) (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.

III.

The CDA was signed into law and became effective on February 8, 1996. Zeran did not file his complaint until April 23, 1996. Zeran contends that even if § 230 bars the type of claim he brings here, it cannot be applied retroactively to bar an action arising from AOL's alleged misconduct prior to the CDA's enactment. We disagree. Section 230 applies by its plain terms to complaints brought after the CDA became effective. As noted in Part IIB, the statute provides, in part: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." 47 U.S.C. § 230(d)(3).

Initially, it is doubtful that a retroactivity issue is even presented here. Retroactivity concerns arise when a statute applies to conduct predating its enactment. Section 230 does not directly regulate the activities of interactive computer service providers like AOL. Instead, § 230 is addressed only to the bringing of a cause of action. Here, Zeran did not file his complaint until over two months after § 230's immunity became effective. Thus, the statute's application in this litigation is in fact prospective. See St. Louis v. Texas Worker's Compensation Comm'n, 65 F.3d 43, 46 (5th Cir. 1995) (holding "issue is not technically one of retroactivity" when statute applies to "filing of
FOOTNOTES

1. Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

2. Section 230 defines "interactive computer service" as "any informa- tion service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specif- ically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institu- tions." 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 com- puter service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."
§311.6

has determined that the oil is substantially equivalent to new oil for use as engine oil in accordance with the NIST test procedures prescribed under §311.4 of this part, and has based the representation on that determination.

§311.6 Prohibited acts.

It is unlawful for any manufacturer or other seller to represent, on a label or a container of processed used oil, that such oil is substantially equivalent to new oil for use as engine oil unless the manufacturer or other seller has based such representation on the manufacturer's determination that the processed used oil is substantially equivalent to new oil for use as engine oil in accordance with the NIST test procedures prescribed under §311.4 of this part. Violators will be subject to enforcement through civil penalties (as adjusted for inflation pursuant to §1.98 of this chapter), imprisonment, and/or injunctive relief in accordance with the enforcement provisions of Section 526 of the Energy Policy and Conservation Act (42 U.S.C. 6365).

50 FR 5561, Oct. 31, 1985, as amended at 55 FR 69660, Nov. 20, 2000]

PART 312—CHILDREN’S ONLINE PRIVACY PROTECTION RULE

Sec.

312.1 Scope of regulations in this part.

312.2 Definitions.

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.

312.4 Notice.

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 in collection of personal information.

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

312.9 Enforcement.

312.10 Safe harbors.

312.11 Rulemaking review.

312.12 Repealability.


SOURCE: 64 FR 59911, Nov. 3, 1999, unless otherwise noted.

§312.1 Scope of regulations in this part.

This part implements the Children’s Online Privacy Protection Act of 1998, (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 this part is April 21, 2000.

§312.2 Definitions.

Child means an individual under the age of 13.

Collect 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 definition:

(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.

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.

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 definition.

Third party means any person who is not:
(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or
(b) 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 part for any other purpose.

Website or online service directed to children means a commercial website or online service, or portion thereof, that
§ 312.3

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 viewers, 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 part. Generally, under this part, 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

(a) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).

§ 312.4 Notice.

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

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

(1) Placement of the notice. (i) The link to the notice must be clearly labeled as a notice of the website or online service’s information practices with regard to children;

(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and

(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.

(2) Content of the notice. To be complete, the notice of the website or online service’s information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service.
Provided that: the operators of a website or online service may list the
name, address, phone number, and e-
mail address of one operator who will
respond to all inquiries from parents
concerning the operators’ privacy pol-
icy and use of children’s information,
as long as the names of all the opera-
tors 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, record-
keeping, 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 oper-
ator; and that the parent has the op-
tion to consent to the collection and
use of their child’s personal informa-
tion without consenting to the disclo-
sure of that information to third par-
ties;
(v) That the operator is prohibited
from conditioning a child’s participa-
tion in an activity on the child’s dis-
closing more personal information
than is reasonably necessary to partici-
pate in such activity; and
(vi) That the parent can review and
have deleted the child’s personal informa-
tion, and refuse to permit further
collection or use of the child’s informa-
tion, 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 tech-
nology, 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 per-
sonal information, including notice of
any material change in the collection,
use, and/or disclosure practices to
which the parent has previously con-
sented.

(1) Content of the notice to the parent.
(i) All notices must state the following:
(A) That the operator wishes to col-
lect personal information from the
child;
(B) The information set forth in par-
agraph (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 disclo-
sure 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 on-
line contact information to respond to
the child’s request for information and
that the requested information will re-
quire 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 infor-
mation, 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.
(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 partici-
pat ing 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 paragraph 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 in this paragraph. Provided that: For the period until April 21, 2005, methods to obtain verifiable parental consent for uses of information other than the “disclosures” defined by §312.2 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, and the operator uses reasonable efforts to provide a parent notice as described in §312.4(c), where such information is:

(i) Used for the sole purpose of protecting the child's safety;
§312.6 Right of parent to review personal information provided by a 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 sections 6503 and 6505 of the Children’s Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 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 part 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:

385
§ 312.10

(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 through 312.9.

(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 paragraphs (b)(2)(i) or (b)(2)(ii) of this section; 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.

(4) 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 part, 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 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 part; 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 part.

(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 paragraph (c)(1). The statement required under paragraph (c)(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 part 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.
§ 313.1 Purpose and scope.

(a) Purpose. This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§ 313.13, 313.14, and 313.15.

(b) Scope. This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the institutions listed below. This part does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This part applies to "financial institutions" and "other persons" over which the Federal Trade Commission has authority.
United States Court of Appeals
For the First Circuit

No. 02-2138

IN RE PHARMATRAK, INC. PRIVACY LITIGATION,

NOAH BLUMOFE, on behalf of himself and all others similarly situated; ROB BARRING; JIM DARBY; KAREN GRASSMAN, on behalf of herself and all others similarly situated; ROBIN MCCLARY; HARRIS PERLMAN; MARCUS SCHROERS,

Plaintiffs, Appellants,

v.

PHARMATRAK, INC.; GLOCAL COMMUNICATIONS, LTD.,

Defendants, Appellees,

PFIZER, INC.; PHARMACIA CORP.; SMITHKLINE BEECHAM PLC; GLAXO WELLCOME PLC; DOES 1-100; AMERICAN HOME PRODUCTS CORP.; NOVARTIS CORP.,

Defendants.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS
[Hon. Joseph L. Tauro, U.S. District Judge]

Before

Lynch, Circuit Judge,
Bownes, Senior Circuit Judge,
and Howard, Circuit Judge.

Adam J. Levitt with whom Daniel W. Krasner, David A.P. Brower, Wolf Haldenstein Adler Freeman & Herz LLC, Seth R. Lesser, Andrew M. Gschwind, Bernstein Litowitz Berger & Grossmann LLP, Melvyn I. Weiss, Michael M. Buchman, Dennis Stewart, William J. Doyle II, Milberg Weiss Bershad Hynes & Lerach LLP, Nancy Freeman Gans, and Moulton & Gans, P.C. were on brief for appellants.

In sum, pharmaceutical companies invited users to visit their websites to learn about their drugs and to obtain rebates. An enterprising company, Pharmatrak, sold a service, called "NETcompare," to these pharmaceutical companies. That service accessed information about the internet users and collected certain information meant to permit the pharmaceutical companies to do intra-industry comparisons of website traffic and usage. Most of the pharmaceutical companies were emphatic that they did not want personal or identifying data about their website users to be collected. In connection with their contracting to use NETcompare, they sought and received assurances from Pharmatrak that such data collection would not occur. As it turned out, some such personal and identifying data was found, using easily customized search programs, on Pharmatrak's computers. Plaintiffs, on behalf of the purported class of internet users whose data Pharmatrak collected, sued both Pharmatrak and the pharmaceutical companies asserting, inter alia, that they intercepted electronic communications without consent, in violation of the ECPA.

The district court entered summary judgment for defendants on the basis that Pharmatrak's activities fell within an
exception to the statute where one party consents to an interception. The court found the client pharmaceutical companies had consented by contracting with Pharmatrak and so this protected Pharmatrak. See In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 12 (D. Mass. 2002). The plaintiffs dismissed all ECPA claims as to the pharmaceutical companies. This appeal concerns only the claim that Pharmatrak violated Title I of the ECPA.

We hold that the district court incorrectly interpreted the "consent" exception to the ECPA; we also hold that Pharmatrak "intercepted" the communication under the statute. We reverse and remand for further proceedings. This does not mean that plaintiffs' case will prevail: there remain issues which should be addressed on remand, particularly as to whether defendant's conduct was intentional within the meaning of the ECPA.

I.

Pharmatrak provided its NETcompare service to pharmaceutical companies including American Home Products, Pharmacia, SmithKline Beecham, Pfizer, and Novartis from approximately June 1998 to November 2000. The pharmaceutical clients terminated their contracts with Pharmatrak shortly after this lawsuit was filed in August 2000. As a result, Pharmatrak was forced to cease its operations by December 1, 2000.

NETcompare was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its
website with the same information from its competitors' websites. The key advantage of NETcompare over off-the-shelf software was its capacity to allow each client to compare its performance with that of other clients from the same industry.

NETcompare was designed to record the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site (including her points of entry and exit); the visitor's IP address;\(^1\) and, for later versions, the webpage the user viewed immediately before arriving at the client's site (i.e., the "referrer URL").\(^2\) This information-gathering was not visible to users of the pharmaceutical clients' websites. According to Wes Sonnenreich, former Chief Technology Officer of Pharmatrak, and Timothy W. Macinta, former Managing Director for Technology of Pharmatrak, NETcompare was not designed to collect any personal information whatsoever.

---

\(^1\) An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215.

\(^2\) URLs (Uniform Resource Locators) are unique addresses indicating the location of specific documents on the Web. The webpage a user viewed immediately prior to visiting a particular website is known as the referrer URL. Search engines such as Yahoo! are common referrer URLs.
NETcompare operated as follows. A pharmaceutical client installed NETcompare by adding five to ten lines of HTML\(^3\) code to each webpage it wished to track and configuring the pages to interface with Pharmatrak's technology. When a user visited the website of a Pharmatrak client, Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a tiny, invisible graphic image known as a "clear GIF" (or a "web bug"). The purpose of the clear GIF was to cause the user's computer to communicate directly with Pharmatrak's web server. When the user's computer requested the clear GIF, Pharmatrak's web servers responded by either placing or accessing a "persistent cookie" on the user's computer. On a user's first visit to a webpage monitored by NETcompare, Pharmatrak's servers would plant a cookie on the user's computer. If the user had already visited a NETcompare webpage, then Pharmatrak's servers would access the information on the existing cookie.

A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server\(^4\) (such as when the user visits additional webpages at the

---

\(^3\) HTML is a coding language used to create documents for the Web. M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary>.

\(^4\) M. Enzer, "Glossary of Internet Terms," <http://www.matisse.net/files/glossary> (defining and discussing cookies). A browser, in turn, is a user's interface to the Web.
same or related sites). A persistent cookie is one that does not expire at the end of an online session. Cookies are widely used on the internet by reputable websites to promote convenience and customization. Cookies often store user preferences, login and registration information, or information related to an online "shopping cart." Cookies may also contain unique identifiers that allow a website to differentiate among users.

Each Pharmatrak cookie contained a unique alphanumeric identifier that allowed Pharmatrak to track a user as she navigated through a client's site and to identify a repeat user each time she visited clients' sites. If a person visited www.pfizer.com in June 2000 and www.pharmacia.com in July 2000, for example, then the persistent cookie on her computer would indicate to Pharmatrak that the same computer had been used to visit both sites. As NETcompare tracked a user through a website, it used JavaScript and a JavaApplet to record information such as the URLs the user visited. This data was recorded on the access logs of Pharmatrak's web servers.

Pharmatrak sent monthly reports to its clients juxtaposing the data collected by NETcompare about all pharmaceutical clients. These reports covered topics such as the

---

5 Pharmatrak's cookies expired after ninety days.

6 Pharmatrak employees supplemented the information recorded on its access logs (and sorted into databases) by conducting outside research (e.g., connecting a mid-year spike in
most heavily used parts of a particular site; which site was receiving the most hits in particular areas such as investor or media relations; and the most important links to a site.

The monthly reports did not contain any personally identifiable information about users. The only information provided by Pharmatrak to clients about their users and traffic was contained in the reports (and executive summaries thereof). Slides from a Pharmatrak marketing presentation did say the company would break data out into categories and provide "user profiles." In practice, the aggregate demographic information in the reports was limited to the percentages of users from different countries; the percentages of users with different domain extensions (i.e., the percentages of users originating from for-profit, government, academic, or other not-for-profit organizations); and the percentages of first-time versus repeat users. An example of a NETcompare "user profile" is: "The average Novartis visitor is a first-time visitor from the U.S., visiting from a .com domain."

traffic on a particular webpage with the launch of a major online advertising campaign).

The NETcompare installation guide also says, "In the future, we may develop products and services which collect data that, when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors."

The most popular domain extensions are .com (used by for-profit entities), .edu (academic entities), .gov (government), and .org (not-for-profit).
While it was marketing NETcompare to prospective pharmaceutical clients, Pharmatrak repeatedly told them that NETcompare did not collect personally identifiable information. It said its technology could not collect personal information, and specifically provided that the information it gathered could not be used to identify particular users by name. In their affidavits and depositions, executives of Pharmatrak clients consistently said that they believed NETcompare did not collect personal information, and that they did not learn otherwise until the onset of litigation, at which point they promptly terminated the service. Some, if not all, pharmaceutical clients explicitly conditioned their purchase of NETcompare on Pharmatrak's guarantees that it would not collect users' personal information. For example, Pharmacia's April 2000 contract with Pharmatrak provided that NETcompare would not collect personally identifiable information from users. Michael Sonnenreich, Chief Executive Officer of Pharmatrak, stated unequivocally at his deposition that none of his company's clients consented to the collection of personally identifiable information.

Pharmatrak nevertheless collected some personal information on a small number of users. Pharmatrak distributed approximately 18.7 million persistent cookies through NETcompare. The number of unique cookies provides a rough estimate of the
number of users Pharmatrak monitored. Plaintiffs' expert was able to develop individual profiles for just 232 users.

The following personal information was found on Pharmatrak servers: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website. Pharmatrak also occasionally recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website of a Pharmatrak client. Most of the individual profiles assembled by plaintiffs' expert contain some but not all of this information.

The personal information in 197 of the 232 user profiles was recorded due to an interaction between NETcompare and computer code written by one pharmaceutical client, Pharmacia, for one of its webpages. Starting on or before August 18, 2000 and ending sometime between December 2, 2000 and February 6, 2001, the client Pharmacia used the "get" method to transmit information from a

---

9 Different users might have the same cookie (if, say, family members shared a computer and browser) or one user might have multiple cookies (if, for example, he used separate work and home computers to visit sites employing NETcompare, or if he revisited a NETcompare site after his first cookie expired).

10 Plaintiffs claim in their brief that Pharmatrak also collected Social Security numbers. We are unable to tell from the record whether this is so.
rebate form on its Detrol\textsuperscript{11} website; the webpage was subsequently modified to use the "post" method of transmission. This was the source of the personal information collected by Pharmatrak from users of the Detrol website.

Web servers use two methods to transmit information entered into online forms: the get method and the post method. The get method is generally used for short forms such as the "Search" box at Yahoo! and other online search engines. The post method is normally used for longer forms and forms soliciting private information.\textsuperscript{12} When a server uses the get method, the information entered into the online form becomes appended to the next URL. For example, if a user enters "respiratory problems" into the query box at a search engine, and the search engine transmits this information using the get method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results. By contrast, if a website transmits information via the post method, then that information does not appear in the URL. Since NETcompare was designed to record the full URLs of the webpages a user viewed immediately before and during a visit to a client's site,

\textsuperscript{11} Detrol is a bladder control medication.

\textsuperscript{12} An example is the registration page at the New York Times website, which asks for a user's email address, date of birth, income, and other information.
Pharmatrak recorded personal information transmitted using the get method.

There is no evidence Pharmatrak instructed its clients not to use the get method. The detailed installation instructions Pharmatrak provided to pharmaceutical clients ignore entirely the issue of the different transmission methods.

In addition to the problem at the Detroil website, there was also another instance in which a pharmaceutical client used the get method to transmit personal information entered into an online form. The other personal information on Pharmatrak's servers was recorded as a result of software errors. These errors were a bug in a popular email program (reported in May 2001 and subsequently fixed) and an aberrant web browser.

II.

On June 28, 2001, plaintiffs filed an amended consolidated class action complaint on behalf of Pharmatrak; its parent company, Glocal Communications, Ltd.; and five pharmaceutical companies: American Home Products Corp., Glaxo Wellcome, Inc.,

---

Originally, eight lawsuits were filed in the District of Massachusetts and the Southern District of New York. The two lawsuits in the District of Massachusetts were filed on August 18, 2000. On April 18, 2001, the Judicial Panel on Multi-District Litigation issued an order transferring the six New York cases to the District of Massachusetts. The purported class, which has never been certified, consists of all persons who visited one of the defendants' websites "and who, as a result thereof, have had Pharmatrak 'cookies' placed upon their computers and have had information about them gathered by Pharmatrak."

Pharmatrak, Glocal, and a number of the pharmaceutical defendants moved for summary judgment in August 2001. In support of their motion, Pharmatrak and Glocal submitted affidavits by Macinta, Pharmatrak's former Managing Director for Technology, and Wes Sonnenreich, Pharmatrak's former CTO, as well as written descriptions of its technology and installation method and a sample monthly report delivered to pharmaceutical clients. The pharmaceutical defendants also submitted affidavits and other documents in support of their motions.

Plaintiffs argued that before summary judgment they should be allowed to conduct discovery on Pharmatrak's servers and to conduct Fed. R. Civ. P. 30(b)(6) depositions on employees of each defendant. Discovery of the servers was necessary, plaintiffs argued, to determine what information NETcompare had extracted from website users and transferred to Pharmatrak's computers. At a

---

14 Glaxo Wellcome and SmithKline Beecham merged in 2000.
hearing on December 3, 2001, the court ordered discovery of the servers and Rule 30(b)(6) depositions of the defendants.\textsuperscript{15}

The plaintiffs employed computer scientist C. Matthew Curtin and his company, Interhack, to analyze Pharmatrak’s servers between December 17, 2001 and January 18, 2002. In about an hour, Curtin wrote three custom computer programs, including "getneedle.pl," to extract and organize personal information on Pharmatrak’s web server access logs, which he "colloquially termed 'haystacks.'" Curtin then cross-referenced the information he extracted with other sources such as internet telephone books. Plaintiffs also conducted the Rule 30(b)(6) depositions.

After discovery was completed, Pharmatrak, Glocal, and other defendants renewed their motions for summary judgment; plaintiffs opposed these motions and moved for summary judgment against Pharmatrak and Glocal on the claim based on Title I of the ECPA.

Following a hearing on the motions, the district court issued a memorandum and order on August 13, 2002 denying plaintiffs' motion for summary judgment and granting in part defendants' summary judgment motions. In re Pharmatrak Privacy

\textsuperscript{15} At the hearing, plaintiffs also sought additional documentary discovery on the ground that to date defendants had turned over only those documents that supported their defenses. In response, the court instructed both parties to "turn over . . . [a]nything that has to do with the case." The district judge added that, if defendants did not comply with this instruction, then plaintiffs should request a court order or sanctions.
Litig., 220 F. Supp. 2d at 15. The court held that the claim against Pharmatrak under Title I of the ECPA was precluded because "the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's NETcompare service on their websites." Id. at 12. The court granted summary judgment to all defendants on all federal law causes of action; it then declined to retain jurisdiction over the state law causes of action and dismissed them without prejudice. Id. at 15.

III.

A. Standard of Review

This court reviews entry of summary judgment de novo. Dominguez-Cruz v. Suttle Caribe, Inc., 202 F.3d 424, 428 (1st Cir. 2000). The fact that all parties moved for summary judgment does not change the standard of review. Secrets, Inc. v. Gillman Knitwear Co., 207 F.3d 56, 61 (1st Cir. 2000). We view the record in the light most favorable to the party opposing summary judgment, indulging all reasonable inferences in that party's favor. Euromotion, Inc. v. BMW of N. Am., Inc., 136 F.3d 866, 869 (1st Cir. 1998). Summary judgment is appropriate where there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. United Parcel Serv. v. Flores-Galarza, 318 F.3d 323, 330 (1st Cir. 2003).
We also review a district court's interpretation of a statute de novo. Bryson v. Shumway, 308 F.3d 79, 84 (1st Cir. 2002).

B. Elements of the ECPA Cause of Action


The post-ECPA Wiretap Act provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); see 18 U.S.C. § 2520 (providing a private right of action). The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4). Thus, plaintiffs must show five elements to make their claim under Title I of the ECPA: that a defendant (1) intentionally (2) intercepted, endeavored to
intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent.

In its trial and appellate court briefs, Pharmatrak sought summary judgment on only one element of § 2511(1)(a), interception, as well as on the statutory consent exception. We address these issues below. Pharmatrak has not contested whether it used a device or obtained the contents of an electronic communication. This is appropriate. The ECPA adopts a "broad, functional" definition of an electronic communication. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995). This definition includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce," with certain exceptions unrelated to this case. 18 U.S.C. § 2510(12). Transmissions of completed online forms, such as the one at Pharmacia's Detrol website, to the pharmaceutical defendants constitute electronic communications. See United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

The ECPA also says that "'contents,' when used with respect to any wire, oral, or electronic communication, includes
any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). This definition encompasses personally identifiable information such as a party's name, date of birth, and medical condition. See Gelbard, 408 U.S. at 51 n.10. See generally Mii.x v. O'Malley, 160 F.3d 343, 346 n.3 (6th Cir. 1998) ("federal wiretap statute[] broadly define[s] 'contents'"). Finally, it is clear that Pharmatrak relied on devices such as its web servers to capture information from users.

C. Consent Exception

There is a pertinent statutory exception to § 2511(1)(a) "where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act ...." 18 U.S.C. § 2511(2)(d). Plaintiffs, of course, bear the burden of establishing a violation of the ECPA. Williams v. Poulos, 11 F.3d 271, 283-84 (1st Cir. 1993). Our case law is unclear as to who has the burden of showing the statutory exception for consent. United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995), suggests the burden is on the party seeking the benefit of the exception, here the defendant. Lanoue held that, when the defendant sought a mistrial on the grounds that the government violated § 2511(1), the prosecution had the burden to establish the statutory law enforcement exception. See also United States v. Jones, 839 F.2d 1041, 1050 (5th Cir. 1988) (when defendant in
criminal prosecution seeks to suppress intercepted communications, "the burden is on the government to prove consent" pursuant to 18 U.S.C. § 2511(2)(c)).

However, there is language in Poulos which could be read to say that the burden is on the party asserting a violation of the Act. 11 F.3d at 284. The issue of who has the burden to show consent was not directly addressed in Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990), an earlier case. We think, at least for the consent exception under the ECPA in civil cases, that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception, and so hold. That party is more likely to have evidence pertinent to the issue of consent. Plaintiffs do not allege that Pharmatrak acted with a criminal or tortious purpose. Therefore, the question under the exception is limited to whether the pharmaceutical defendants gave consent to the interception. Because the district court disposed of the case on the grounds that Pharmatrak's conduct fell within the consent exception, we start there.

The district court adopted Pharmatrak's argument that the only relevant inquiry is whether the pharmaceutical companies consented to use Pharmatrak's NETcompare service, regardless of how the service eventually operated. In doing so, the district court did not apply this circuit's general standards for consent under

---


This court addressed the issue of consent under the Wiretap Act in Griggs-Ryan. A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. See Griggs-Ryan, 904 F.2d at 117-19. "Thus, 'a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.'" Gilday v. DuBois, 124 F.3d 277, 297 (1st Cir. 1997) (quoting Griggs-Ryan, 904 F.2d at 119). Consent may be explicit or implied, but it must be actual consent rather than constructive consent. Poulos, 11 F.3d at 281-82; see also United States v. Footman, 215 F.3d 145, 155 (1st Cir. 2000) ("The question of consent, either express or implied, may vary with the circumstances of the parties."). Pharmatrak argues that it had implied consent from the pharmaceutical companies.

Consent "should not casually be inferred." Griggs-Ryan, 904 F.2d at 117-18. "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (internal quotation
omitted); accord Lanoue, 71 F.3d at 981; see also Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the capability of monitoring alone cannot be considered implied consent.").

The district court made an error of law, urged on it by Pharmatrak, as to what constitutes consent. It did not apply the standards of this circuit. Moreover, DoubleClick and Avenue A do not set up a rule, contrary to the district court's reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances. If these cases did so hold, they would be contrary to the rule of this circuit established in Griggs-Ryan. DoubleClick and Avenue A, rather, were concerned with situations in which the defendant companies' clients purchased their services for the precise purpose of creating individual user profiles in order to target those users for particular advertisements. See Avenue A, 165 F. Supp. 2d at 1156, 1161; DoubleClick, 154 F. Supp. 2d at 502, 510-11. This very purpose was announced by DoubleClick and Avenue A publicly, as well as being self-evident. See Avenue A, 165 F. Supp. 2d at 1161; DoubleClick, 154 F. Supp. 2d at 502, 510-11. These decisions found it would be unreasonable to infer that the clients had not consented merely because they might not understand precisely how the user demographics were collected. See Avenue A, 165 F. Supp. 2d at 1161-62; DoubleClick, 154 F. Supp. 2d at 510-11. The facts
in our case are the mirror image of those in DoubleClick and Avenue A: the pharmaceutical clients insisted there be no collection of personal data and the circumstances permit no reasonable inference that they did consent.

On the undisputed facts, the client pharmaceutical companies did not give the requisite consent. The pharmaceutical clients sought and received assurances from Pharmatrak that its NETcompare service did not and could not collect personally identifiable information. Further, when plaintiffs brought a suit alleging that Pharmatrak's actions meant it had not lived up to its commitment, the pharmaceutical clients promptly cancelled the service. Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would not collect such information.

The interpretation urged by Pharmatrak would, we think, lead to results inconsistent with the statutory intent. It would undercut efforts by one party to a contract to require that the privacy interests of those who electronically communicate with it be protected by the other party to the contract. It also would lead to irrational results. Suppose Pharmatrak, for example, had intentionally designed its software, contrary to its representations and its clients' expectations, to redirect all possible personal information to Pharmatrak servers, which
collected and mined the data. Under the district court's approach, Pharmatrak would nevertheless be insulated against liability under the ECPA on the theory that the pharmaceutical companies had "consented" by simply buying Pharmatrak's product. Or suppose an internet service provider received a parent's consent solely to monitor a child's internet usage for attempts to access sexually explicit sites -- but the ISP installed code that monitored, recorded and cataloged all internet usage by parent and child alike. Under the theory we have rejected, the ISP would not be liable under the ECPA.

Nor did the users consent. On the undisputed facts, it is clear that the internet user did not consent to Pharmatrak's accessing his or her communication with the pharmaceutical companies. The pharmaceutical companies' websites gave no indication that use meant consent to collection of personal information by a third party. Rather, Pharmatrak's involvement was meant to be invisible to the user, and it was. Deficient notice will almost always defeat a claim of implied consent. See Poulos, 11 F.3d at 281-82; Campiti v. Walonis, 611 F.2d 387, 393-94 (1st Cir. 1979). Pharmatrak makes a frivolous argument that the internet users visiting client Pharmacia's webpage for rebates on Detrol thereby consented to Pharmatrak's intercepting their personal information. On that theory, every online communication would provide consent to interception by a third party.
D. Interception Requirement

The parties briefed to the district court the question of whether Pharmatrak had "intercepted" electronic communications. If this question could be resolved in Pharmatrak's favor, that would provide a ground for affirmance of the summary judgment. See O'Neil v. Baker, 210 F.3d 41, 46 (1st Cir. 2000). It cannot be answered in favor of Pharmatrak.

The ECPA prohibits only "interceptions" of electronic communications. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Id. § 2510(4).

Before enactment of the ECPA, some courts had narrowed the Wiretap Act's definition of interception to include only acquisitions of a communication contemporaneous with transmission. See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460-61 (5th Cir. 1994) (applying pre-ECPA interpretation to post-ECPA case). There was a resulting debate about whether the ECPA should be similarly restricted. The debate is well described in Konop, 302 F.3d at 876-79 & n.6. Other circuits have invoked the contemporaneous, or "real-time," requirement to exclude acquisitions apparently made a substantial amount of time after material was put into electronic storage. Steiger, 318 F.3d at 1048-50 (pornographic images gradually collected on hard drive);
Konop, 302 F.3d at 872-73 (static website content available on an ongoing basis); Steve Jackson Games, 36 F.3d at 458 (accumulation of unread emails). These circuits have distinguished between materials acquired in transit, which are interceptions, and those acquired from storage, which purportedly are not. See, e.g., Konop, 302 F.3d at 878.

We share the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions of online communications. See Steiger, 318 F.3d at 1047 (quoting Konop, 302 F.3d at 874). In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, "[T]echnology has, to some extent, overtaken language. Traveling the internet, electronic communications are often -- perhaps constantly -- both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox." United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003).

The facts here do not require us to enter the debate over the existence of a real-time requirement. The acquisition by Pharmatrak was contemporaneous with the transmission by the internet users to the pharmaceutical companies. Both Curtin, the plaintiffs' expert, and Wes Sonnenreich, Pharmatrak's former CTO,
observed that users communicated simultaneously with the pharmaceutical client's web server and with Pharmatrak's web server. After the user's personal information was transmitted using the get method, both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage; as both Curtin and Wes Sonnenreich acknowledged, Pharmatrak's content (the clear GIF that enabled the interception) sometimes arrived before the content delivered by the pharmaceutical clients.

Even those courts that narrowly read "interception" would find that Pharmatrak's acquisition was an interception. For example, Steiger observes:

[U]nder the narrow reading of the Wiretap Act we adopt . . ., very few seizures of electronic communications from computers will constitute 'interceptions.' . . . 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.'

318 F.3d at 1050 (paragraphing omitted) (quoting J.J. White, Email @Work.com: Employer Monitoring of Employee E-Mail, 48 Ala. L. Rev. 1079, 1083 (1997)). NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak).

Pharmatrak argues that there was no interception because "there were always two separate communications: one between the Web
user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak." This argument fails for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information) exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

E. Intent Requirement

At oral argument this court questioned the parties about whether the "intent" requirement under § 2511(a)(1) had been met.

We remand this issue because it was not squarely addressed by both parties before the district court. When Pharmatrak moved for summary judgment, it did not do so on the grounds that the statutory requirement of intent was unmet. At most, it raised the issue in passing at the hearing on the cross-motions for summary judgment.

Plaintiffs, in their motion for summary judgment, did raise the issue and argued that any interception was intentional; but the district court neither granted the motion nor addressed the issue. In its opposition to plaintiffs' motion, Pharmatrak relied
on its own motion for summary judgment, and so did not address intent. The issue has not been briefed to us.

While it is true that we can affirm the grant of summary judgment on any ground presented by the record, we will usually do so only when the issue has been fairly presented to the trial court. See Pure Distribs., Inc. v. Baker, 285 F.3d 150, 156 (1st Cir. 2002). Here it was not, and we are reluctant to determine ourselves whether there was adequate opportunity for discovery on this issue and whether there are material facts in dispute, and to resolve an issue without briefing.

Still, we wish to avoid uncertainty about the legal standard for intent under the ECPA on remand, and so we address that point. Congress amended 18 U.S.C. § 2511 in 1986 to change the state of mind requirement from "willful" to "intentional." Since "intentional" itself may have different glosses put on it,\(^\text{17}\) we refer to the legislative history, which states:

As used in the Electronic Communications Privacy Act, the term "intentional" is narrower than the dictionary definition of "intentional." "Intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no

\(^{17}\) For example, see the distinction between general intent and specific intent described in United States v. Whiffen, 121 F.3d 18, 20-21 (1st Cir. 1997).
control over the existence of circumstances, one cannot "intend" them.

S. Rep. No. 99-541, at 23 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3577. Congress made clear that the purpose of the amendment was to underscore that inadvertent interceptions are not a basis for criminal or civil liability under the ECPA. Id. An act is not intentional if it is the product of inadvertence or mistake. Sanders v. Robert Bosch Corp., 38 F.3d 736, 742-43 (4th Cir. 1994); United States v. Townsend, 987 F.2d 927, 930 (2d Cir. 1993). There is also authority suggesting that liability for intentionally engaging in prohibited conduct does not turn on an assessment of the merit of a party's motive. See Abraham v. County of Greenville, 237 F.3d 386, 391-92 (4th Cir. 2001) (jury instruction saying "defendant's motive is not relevant" to determination of intent under § 2511 was proper). That is not to say motive is entirely irrelevant in assessing intent. An interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct.

F. Conclusion

We reverse and remand for further proceedings consistent with this opinion.
WHERE'S THE BEEF? DISSECTING SPAM'S PURPORTED HARMs

ERIC GOLDMAN†

I. INTRODUCTION

After many failed attempts over the past six years, Congress finally enacted a law regulating unsolicited commercial e-mails, the **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003** (the "**CAN-SPAM Act**" or "**CAN-SPAM**").¹ **CAN-SPAM** follows significant state-based efforts to regulate spam; from 1997 to 2003, nearly three quarters of the states adopted some spam regulation,² most of which are now preempted by **CAN-SPAM**.³

**CAN-SPAM**, like the state laws preceding it, takes a multi-faceted approach to regulating spam. Among other provisions, **CAN-SPAM** contains provisions that regulate the e-mail content,⁴ restrict specific notorious spammer practices,⁵ give spam recipients the ability to opt-out, and attack the spammer's funding by creating advertiser liability.

The diversity of regulatory approaches inherent in **CAN-SPAM** (and, before that, the superseded state statutes) prompts a fundamental question: exactly what harms are caused by spam that these regulations attempt to redress? There is no consensus answer to this question. Just about everyone seems to agree that spam is a problem that needs to be

† Assistant Professor, Marquette University Law School. E-mail: eric.goldman.marquette.edu. Personal home page: <http://eric_goldman.tripod.com>. The author thanks the participants in the Summer 2003 Spam Seminar at The John Marshall Law School for their enlightening perspectives.

3. See e.g. restrictions on misleading subject lines; requirements that the spam contain contact information and be labeled as an ad or as sexually oriented material.
4. See e.g. restrictions on e-mail harvesting, dictionary attacks, using open mail relays, and signing up for free e-mail accounts.
addressed, but no one seems to agree on why. Without clearly understanding the targeted harms, policy-makers cannot craft regulations designed to fix them.

This Essay examines the purported harms caused by spam in an effort to isolate bona fide areas needing legislative intervention. However, few such needs exist. Instead, most purported harms are illusory, already adequately addressed by existing laws or left to market solutions. This analysis thus undercuts many of the purported justifications for regulating spam.

II. DEFINING THE HARMs OF SPaM

A. DEFINING SPaM

Any attempt to intelligently discuss spam is immediately hampered by the word's imprecision. Simply put, the term “spam” lacks a single well-accepted definition. Usually “spam” refers to some form of unwanted e-mail, although some users generalize the term to describe all forms of unwanted advertising, both in e-mail and other media. CAN-SPAM defines “commercial electronic mail message” as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.” Building on this definition, this Essay refers to “spam” as unsolicited “commercial electronic mail messages.” However, this definition is both under- and over-inclusive because the definition includes e-mails recipients want and does not include all e-mails not wanted by recipients, and thus it may not track recipient expectations.


9. CAN-SPAM Act, supra n. 1, at § 3(2). The law further requires the Federal Trade Commission to promulgate regulations defining “primary purpose.” Id. § 3(2)(C).

10. See Deborah Fellow, Pew Internet & American Life Project, Spam: How it is Hurting E-mail and Degrading Life on the Internet ii <http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf> (Oct. 22, 2003) [hereinafter The Pew Report] (“e-mail users are not entirely clear on just what is spam, an issue that is an absolute stopper for writing effective, enforceable legislation against spam”).
WHERE'S THE BEEF?

B. SPAM IS ANNOYING

1. Distinguishing Wanted and Unwanted Content

Many e-mail recipients castigate spam as annoying, but the reason why are less clear. Some annoyance is attributable to the objectionable content in spam, a point addressed infra in subsection II(D). Otherwise, the annoyance is based (among other factors) on the unsolicited, high-volume, time-consuming or unpreventable nature of spam.

I believe these concerns all derive from the same source: spam is unwanted. A simple example may illustrate this. Assume Jane is ready to purchase a Canon PowerShot S400 digital camera. An unsolicited e-mail arrives in Jane’s in-box from a trustworthy retailer that she has never transacted with. The retailer offers to sell her the camera for $100 less than any other retailer. Is this spam?

Some recipients would say “yes” because the e-mail is unsolicited or otherwise invades their privacy. However, most e-mail recipients would consider this e-mail valuable instead of annoying, in which case they would want this e-mail because it will save them time and money.

Perhaps this example gives us an important insight on the nature of spam. E-mail recipients want e-mail that saves money, saves time, educates on matters of interest, or is otherwise relevant and helpful. Thus, many e-mail recipients gladly would receive unsolicited e-mails that meet those specifications. In contrast, e-mail recipients are annoyed to receive a high volume of irrelevant and unhelpful e-mails.

Unfortunately, frequently spam is irrelevant and unhelpful to recipients because it is relatively untargeted. Like any other marketers, spam advertisers will pay for targeted e-mail lists that are more likely to yield higher results. However, the negligible marginal cost of sending spam lowers the optimal level of targeting for spammers. Thus, spammers can profitably use low-yield and untargeted practices such as e-mail harvest-

---

11. Id. at 27; Taylor, supra n. 6 (ninety-three percent of those surveyed said spam was somewhat or very annoying).


13. See Id.

14. See DoubleClick, 2003 Consumer E-mail Study, Oct. 2003 3 <http://www.doubleclick.com/us/knowledge_central/documents/research/dc_consumer_emailstudy_0310.pdf> (Oct. 2003). The survey considered permission-based e-mail marketing. Respondents were asked what motivated them to act on an e-mail; thirty-eight percent said it was the “product I needed at the time” and thirty-five percent said a “special offer or discount.” Id.

15. The Federal Trade Commission has specifically focused on the high percentage of false claims in spam, Federal Trade Commission, False Claims in Spam <http://www.ftc.gov/reports/spam030429spamreport.pdf> (Apr. 30, 2003). These concerns are effectively subsumed under the category of irrelevant and unhelpful e-mails. Other harms created by false claims are covered under other existing laws like false advertising.
ing and dictionary attacks.\textsuperscript{16}

Even though spammers can profitably send very-low relevance e-mails to lots of recipients, not all spam is bad. Inevitably, some recipients will find a particular spam e-mail helpful and relevant. More specifically, recipients' perceptions about each spam's relevance usually sort into a bell curve: some will find the e-mail completely irrelevant, some will find the e-mail very relevant, and others will find the e-mail somewhat relevant.\textsuperscript{17}

Some empirical data supports this analysis. Several recent surveys show that seven to eight percent of those surveyed have purchased a product or service in response to spam\textsuperscript{18} and approximately thirty percent of those surveyed have responded to spam to get more information about the advertised product or service.\textsuperscript{19} While not high percentages, the statistics seemingly contradict spam's abysmal reputation. For recipients who responded to spam (plus those who were educated but did not respond), the spam was relevant. For those who purchased in response to a particular spam, that e-mail helped the consumer find a desired product or service at an acceptable price.

We should not trivialize these consequences. Spam plays an important role in the marketplace of ideas, perhaps filling gaps left by other media, and can contribute to efficiently functioning economic markets. In some cases, spam creates transaction opportunities that otherwise would not occur due to prohibitive search costs or lack of consumer awareness about products available to solve their needs.

Of course, these conclusions do not change the fact that most spam is unwanted by most recipients. However, it is unclear why individuals seem less tolerant of irrelevant spam than irrelevant ads in other media. Consumers routinely tolerate irrelevant ads in other media with less annoyance than they feel towards spam.

Let us consider ad relevancy in a few media, starting with billboards. Billboard ads target viewers only by geography (if that), so they

\begin{footnotesize}
\begin{enumerate}
\item[16.] See Jack Hitt, Confessions of a Spam King, N.Y. Times Mag., (Sept. 28, 2003) at 48 (describing different methods of acquiring e-mail addresses cheaply); see generally Ian Ayres & Matthew Funk, Marketing Privacy: A Solution for the Blight of Telemarketing (and Spam and Junk Mail), 20 Yale J. on Reg. 77 (2003) (discussing the analogous phenomenon in the telemarketing context).
\item[17.] Recipient assessments of relevancy also vary based on when the e-mail is received. An e-mail to Jane offering a cheap price on the digital camera may be very relevant prior to her purchase and irrelevant afterwards.
\item[18.] See The Pew Report, supra n. 10, at ii-iii (seven percent); Mailshell Survey, supra n. 7 (eight percent); Thomas Leavitt, posting to Politech <http://www.politechbot.com/p-04710.html> (May 2, 2003) (citing a survey on ndp.com that seven percent “sometimes” buy from spam, plus another twenty-three percent “very rarely” buy).
\item[19.] See The Pew Report, supra n. 10, at ii-iii (thirty-three percent); Mailshell Survey, supra n. 7 (twenty-eight percent).
\end{enumerate}
\end{footnotesize}
are fairly low-relevancy advertising tools, meaning that most billboard ads will be irrelevant to most viewers.

The broadcast and newspaper media use differentiated content to segment consumers.\textsuperscript{20} Thus, a TV show will appeal to a certain demographic, and newspapers divide their content into topical sections (e.g. sports, business, metro) that are read by only some readers. This segmentation means that ads can be targeted to consumers attracted by the surrounding content. Nevertheless, even the most targeted content will appeal to multiple demographics, so the associated ads will be less relevant to non-majority audience segments.

In these other media like billboards, broadcasting and newspapers, consumers do not vociferously demand regulation to minimize the irrelevancy of ads delivered through them. Why do consumers feel differently about spam?

2. Sorting Spam Wastes Time

Perhaps recipients penalize spam because it takes time to sort irrelevant spam from wanted e-mails. Sorting also creates the risk of Type I and Type II errors (i.e., legitimate e-mail gets tossed or blocked as spam, and objectionable spam gets through the sorting).\textsuperscript{21}

But once again, spam is not different from other media. Every medium that contains ads requires consumers to sort ads from content and wanted ads from unwanted ads. For example, sorting postal mail requires the recipient to evaluate the envelope’s exterior and, in some cases, open and review the contents. Broadcast ads are even more difficult to sort, because ads are interspersed with content and the viewer cannot reorder or skip the ads.

So while spam does require sorting time, recipients can manually sort e-mail relatively efficiently by reviewing subject lines,\textsuperscript{22} and many

---

\textsuperscript{20} Not all ads are delivered on a segmented basis. For example, infomercials are often broadcast at a time when other programming would fail to generate a sufficient audience, so frequently infomercials make no effort to segment the audience.

\textsuperscript{21} See \textit{CAN-SPAM Act}, supra n. 1, at § 2(a)(4) (legislative finding of Congress).

recipients develop good skills doing so. Spam can also be automatically blocked without any manual sorting using e-mail filters. As a result, the amount of time "wasted" on the e-mail sorting process may very well be less than the time wasted in other media.

All media containing ads demand sorting time and create some risk of erroneous sorting, and no regulatory scheme—other than banning a medium altogether—can eliminate that. Instead, time lost to sorting is unavoidable in a media-based society, and spam is just one of many manifestations of that phenomenon. Thus, the explanation for recipients' antipathy towards spam must lie elsewhere.

3. **Spam Causes Recipients to Lose Control of Their In-Boxes**

Evidence suggests that many recipients are bothered by their inability to stop spam and feel that spam is a loss of privacy. This suggests that recipient frustration with spam may be the result of a feeling that recipients have lost control over their in-boxes.

However, once again this problem arises with other media. Recipients cannot stop spam except by eliminating their e-mail account altogether, but consumers of other media are similarly powerless to change what ads are delivered in that medium except by discontinuing use of that medium. For example, a newspaper or magazine reader cannot control what ads are published; the reader's only choices are to ignore unwanted ads or stop reading the publication altogether. This argument holds true for broadcast media, billboards, and junk mail as well.

Perhaps e-mail can be distinguished from other media because it delivers more important personal content to recipients than other media. Recipients seem to develop a special and personal relationship with their in-box, and this explanation might offer an insight about why telemarketing is so reviled. But this explanation is not totally satisfac-

---

23. The Pew Report, supra n. 10, at 11 ("nearly two-thirds (63%) of all e-mailers say about spam that they 'know it right away when they see it'); see George Johnson, Spam ShEn@ming: That Gibberish in Your In-Box May Be Good News, N.Y. Times (New York, NY) (Jan. 25, 2004), at § 4, p. 16 (discussing how spam filters cause spam to "degenerate[e] into nonsense" and become "word salad").


25. The Pew Report, supra n. 10, at 27 (seventy-five percent of users are bothered by this).

26. See Ayres & Funk, supra n. 16 (discussing a heightened sense of privacy at home).
tory because it does not explain the seeming dichotomy between the outrage over spam and comparative tolerance of junk mail.

A more satisfying explanation can be found by considering the relative adoption curves of spam and other media. We have had many years to develop ways to cope with ads in other media, but we are still developing ways to cope with e-mail ads. It seems likely that users will improve their ability to manage e-mail with more experience, at which point user frustration should decrease.27 Meanwhile, new generations who grow up using e-mail should be more tolerant of spam28 because they will develop coping strategies for spam (and media inputs generally) from an early age.

Thus, current annoyance with spam could merely reflect that user experience with e-mail is evolving. Robust e-mail management tools also should reduce annoyance, and the current annoyance may also reflect that those tools are not yet adequately deployed.29

4. Conclusion on Annoyance

Unwanted e-mails are annoying, but minor annoyances are a fact of life, and no law can eliminate them—from e-mail or otherwise. E-mail recipients’ annoyance at spam appears to be an overreaction when compared to their reactions to other forms of annoying ads. Meanwhile, regulation of spam creates significant risk that some relevant e-mails will be blocked from recipients who want them. It is troubling to regulate content to protect the majority from minor annoyances if the conse-

27. Taylor, supra n. 6 (noting that the percentage of people very annoyed with spam dropped from eighty percent in 2002 to sixty-four percent in May 2003, suggesting that recipients are developing more efficient coping mechanisms); DoubleClick 2003 Consumer E-mail Study 7 <http://www.doubleclick.com/us/knowledge_central/documents/research/ dc_consume-mailstudy_0310.pdf> (Oct. 2003) (describing increased user sophistication in deleting suspected spam without reading it); but see The Pew Report, supra n. 10, at 36 (indicating that veteran Internet users are more sophisticated at managing spam but are also more bothered than average by it).

quence is preventing minority interests from exchanging relevant content.

C. SPammers Imose Costs on Third Parties

As it moves from sender to recipient, spam generates bandwidth and server processing costs for the spammer’s IAP, the recipient and the recipient’s IAP. Depending on a spammer’s practices, they can also impose some costs on unsuspecting third parties, such as server operators with open mail relays and or whose domains are forged. We consider each cost in turn.

1. The Spammer’s IAP

The spammer and its IAP have contractual privity, and the IAP can technologically constrain the spammer’s activities (i.e. capping the quantity of e-mails sent). As a result, a spammer’s IAP has the capacity to charge spammers for any spam-related costs,30 and there are no obvious market failures that require regulatory protection for the spammer’s IAP.

2. Recipients and Their IAPs

It is frequently claimed that recipients pay to receive spam,31 and sometimes spam is likened to junk mail sent with postage due.32 With respect to individuals with a consumer IAP account, this claim is no longer accurate. It was true prior to the mid-1990s, when many IAPs charged customers a time-based fee for Internet connectivity. Because each e-mail took some time to download, recipients paid a small fee for each e-mail they received. Today, consumer IAPs almost universally charge flat-rate pricing for unlimited usage,33 so consumer recipients do not pay for each e-mail received.

30. Frivitv and technological control also apply to IAPs or e-mail service providers who provide spammer “dropboxes,” where the spammer directs replies to a validly-established e-mail account that the spammer knows will be overrun and shut down.


33. See John Borland, CNET News.com, Putting a Lid on Broadband Use <http://news.cnet.com/2102-1034_3-6079624.html?tag=st utilise_print> (Sept. 22, 2003) (but noting that some cable broadband providers are trying to impose some high-end usage limits to avoid line congestion). In contrast, many non-US telephone callers pay per-minute connect charges to make local calls, in which case callers accessing the Internet via dial-up connections pay time-based connection fees for reading or downloading their e-mail. Many service providers do limit the size of a customer’s e-mail account, so in theory a user might procure
However, recipient IAPs bear some bandwidth and server processing costs for each e-mail they process, plus preventative costs (like filtering) and remediation costs (like blocking or database repair) associated with pernicious e-mail. Unlike the spammer's IAP, the recipient's IAP has no contractual privity or technological relationship with the spammer. And where corporations provide Internet connectivity to their employees, they incur these costs as a recipient directly. As a result, recipient IAPs and corporations may benefit from legal systems that allow them to pass those costs back to spammers or avoid the costs altogether.

Until recently, common law trespass to chattels was an important legal mechanism to accomplish that objective.\textsuperscript{34} However, in \textit{Intel Corp. v. Hamidi},\textsuperscript{35} the California Supreme Court recently scaled the doctrine back, rejecting trespass to chattels when a low-volume spammer's e-mails did not threaten to impair (or actually impair) the functioning of Intel's systems.\textsuperscript{36} It remains unclear how subsequent courts will interpret \textit{Intel}, but in all likelihood some future spammers will avoid liability for trespass to chattels.

Irrespective of trespass to chattels, corporations and recipient IAPs can use, and have successfully used, the \textit{Computer Fraud and Abuse Act} ("CFAA") to combat spam.\textsuperscript{37} CAN-SPAM supplements the CFAA (and whatever is left of common law trespass to chattels) by providing recipient IAPs a direct cause of action when the IAP is "adversely affected" by a spammer who fails to comply with selected other provisions of CAN-SPAM.\textsuperscript{38} Depending on how broadly courts interpret the words "adversely affected," this provision may moot Hamidi's common law analysis by providing a statutory cause of action. At minimum, CAN-SPAM expedites recipient IAP causes of action by providing statutory damages and attorneys' fees\textsuperscript{39} and by providing another basis (in addition to the CFAA) for federal court jurisdiction. As a result, CAN-SPAM should a larger e-mail account to ensure enough capacity for both wanted e-mails and spam. However, users who regularly purge their e-mails should rarely encounter a problem.


\textsuperscript{35} 1 Cal. Rptr. 3d 32 (Cal. Sup. Ct. 2003).

\textsuperscript{36} Id. at 43.


\textsuperscript{38} CAN-SPAM Act, supra n. 1, at § 7(g).

\textsuperscript{39} Id. § 7(g)(3)-(4).
help recipient IAPs control some of the e-mail processing costs that are externalized to them.

In addition to bandwidth, server, preventative and maintenance costs, some companies have sought legal recognition for the time employees waste on spam.\textsuperscript{40} Indeed, analysts claim that this lost time creates enormous costs.\textsuperscript{41} However, as discussed in Section II supra, time spent sorting or reading spam is not necessarily wasted, nor is it unique compared to the many other ways that employees waste time (e.g., personal e-mail, junk mail and personal telephone calls). Therefore, lost productivity due to spam is a poor policy basis for regulating spam.

3. Open Mail Relays

Spammers can offload costs to third party computers who have open mail relays, which can cause those server operators to incur some costs like any other recipient IAP. Of course, operators wishing to avoid those costs can simply close their mail relays, and interestingly these operators are often considered part of the problem, not victims.\textsuperscript{42} Thus, forcing them to internalize the spam-created costs (rather than pushing those costs to a spammer) may motivate them to close the relays.\textsuperscript{43}

\textsuperscript{40} See Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32.

\textsuperscript{41} See Nucleus Research, Spam: The Silent ROI Killer, Research Note D59 <http://www.nucleusresearch.com/research/d59.pdf> (accessed July 1, 2003) (claiming that employees have an average lost productivity of 1.4 percent per year, meaning that spam costs $874 per employee per year); Ferris Research, Spam Control: Problems and Opportunities 7, 16-17 <http://www.ferris.com/report/200301/report.pdf> (accessed Jan. 2003) ("In 2002, the total cost of spam to corporate organizations in the United States was $8.9 billion," of which forty-four percent was attributable to lost productivity); Basex, Spam E-mail and Its Impact on IT Spending and Productivity 5 <http://www.basex.com/poty2003.nsf/e8f7dc0f5617d66e9c85256b99006eae8761f7f4be3706985256ea040019f314/$FILE/BasexReportSpam.pdf> (Dec. 2003) ("[t]he cost of spam to companies worldwide is ca. $20 billion and growing at almost 100% per year"). See generally Saul Hansell, Diverging Estimates of the Cost of Spam, N.Y. Times, at C1 (July 28, 2003) (discussing and critiquing these studies).


\textsuperscript{43} Although CAN-SPAM did not expressly set up a cost-shifting mechanism for operators of open mail relays, it did criminalize their use by spammers. See CAN-SPAM Act, supra n. 1, at §§ 4(a)(1), 5(b)(3).
4. Targets of Forged Headers

Spammers also can offload costs to third parties using forged headers. A forged header occurs when a spammer manipulates an e-mail to make it look like the spam originated from X.com when it is really being sent from Y.com.\(^44\) The X.com domain name operator (or its IAP) incurs costs when undeliverable messages and recipient complaints are directed to the operator.

The operator of a forged domain name lacks any contractual or technological way to prevent this activity,\(^45\) so regulatory protection is appropriate. Indeed, thirty states prohibited forged headers,\(^46\) and these state

---

\(^{44}\) See id. at § 3(8) (defining “header information”).

\(^{45}\) Forged headers can be prevented only if e-mail senders are better authenticated. Project Lumes is being developed to tackle that problem. See Hans Peter Brondmo et al., E-mail Service Provider Coalition, Project Lumes: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume E-mail Sender Accountability <http://www.networkadvertising.org/esp/Project_Lumes_White_Paper.pdf> (Sept. 24, 2003); see also Olsen, supra n. 25.


laws may not be preempted by CAN-SPAM.\textsuperscript{47} Meanwhile, CAN-SPAM criminalizes forged headers\textsuperscript{48} and potentially sets up a private cause of action for some victims ("providers of Internet access services" who are "adversely affected").\textsuperscript{49} The robustness of this private cause of action remains to be seen, but this CAN-SPAM provision, plus any coverage under non-preempted state laws and other existing doctrines like trademark law and the CPAA,\textsuperscript{50} should provide substantial protection to the victims of forged headers.

5. Conclusion on Costs

Far too much rhetoric is directed to the costs borne by individual spam recipients. These individuals no longer bear a financial cost to receive spam, and any "costs" associated with the consumption of their attention makes unsupportable assumptions about the e-mail's relevancy to the recipient. Similarly, although sending IAPs may find it desirable to obtain regulatory protection against spam, they can control their financial exposure to spammers' behavior through pricing and technology.

Focusing on the costs borne by individual recipients and sending IAPs detracts from the parties who incur uncontrollable costs from spam, such as recipient IAPs, operators of open mail relays and victims of forged headers. CAN-SPAM provides some useful legal tools to protect these parties, although those tools may be incomplete. A crisper understanding of the real costs borne by these parties would have likely produced a more thoughtful legal solution.

D. Spam Contains or Promotes Objectionable Content

Many spam recipients complain about objectionable content of spam, especially pornographic spam.\textsuperscript{51} Due to deep feelings towards pornographic spam, Congress specifically targeted it in CAN-SPAM by requir-

\textsuperscript{47} See CAN-SPAM Act, supra n. 1, at § 8(b)(1) (state laws that "prohibit falsity or deception in any portion of a commercial electronic mail message or information attached thereto" are not preempted).

\textsuperscript{48} See id. §§ 4(a)(1), 5(a)(1).

\textsuperscript{49} See id. § 7(g)(1).


\textsuperscript{51} See The Pew Report, supra n. 10, at 44 ("[i]n nearly every measure we tested, pornography soared to the top as the most offensive, objectionable, destructive type of spam"); Taylor, supra n. 6 (eighty-six percent of those surveyed said pornographic spam annoyed them a lot); unsspam, Comprehensive Spam Survey (Oct. 2003) <http://www.unspam.com/fight_spam/information/survey Oct2003.html> (Oct. 15, 2003) (ninety-six percent of parents are looking to block pornographic spam from reaching their children); see also CAN-SPAM Act, supra n. 1, at § 2(a)(5) (legislative findings of Congress).
ing warning labels. But to understand the harms pornographic spam causes, it is useful to consider adults and minors separately.

For adults, pornographic spam is no different from any other form of unwanted content discussed in Section II(B) supra. Nevertheless, Congress has tried to help adults avoid unwanted pornographic spam by requiring special labeling of pornographic spam in the subject line. When implemented, this requirement can help recipients who automatically filter e-mail using the appropriate words because the spam will automatically be routed outside the recipient’s ordinary view. Until spammers regularly comply with this law, however, filtering will not be helpful.

The mandatory labeling law may be even less helpful to recipients who manually sort e-mail. These recipients may still see objectionable content if the subject line contains objectionable terms or the recipient’s e-mail software “previews” a message and the previewed content is objectionable.

So how can regulatory intervention help recipients avoid objectionable e-mails? With widely varying perceptions of what constitutes objectionable content, regulating objectionable ads is no more feasible than regulating irrelevant ads. Thus, the only “solution” may be for recipients to manage their exposures themselves, either through technological measures or by looking elsewhere when something offends.

Putting the burden on recipients to avoid pornographic spam is less satisfactory when recipients are minors. In that case, society may be harmed when minors view this inappropriate material.

However, minors’ exposure to pornographic spam is a microcosm of a much greater problem: minors with e-mail accounts. This is a major


53. However, some adults find viewing pornographic spam qualitatively more objectionable than other spam.

54. See CAN-SPAM Act, supra n. 1, at § 5(b).


56. It is well-accepted that states have a compelling state interest in protecting minors from being exposed to materials that are indecent or harmful to them. Reno v. Am. Civ. Liberties Union, 521 U.S. 844 (1997) (“[w]e 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”) (quoting Sable Commun. v. FCC, 492 U.S. 115 (1989)).

social development because historically minors had few communication media that readily bypassed parental oversight. Today, minors can use e-mail, instant messenger, and cell phones to communicate with third parties without any parental oversight and knowledge. With this additional autonomy, minors can get into inappropriate and potentially very dangerous situations, such as interactions with sexual predators.  

Because of these risks, some parents restrict minors’ access to the Internet altogether, and other parents permit only supervised Internet use. The former prevents any risk of exposure to pornographic spam, and the latter approach gives parents the ability to pre-screen pornographic spam or counsel the minor when seeing such spam.

Otherwise, parents who let minors have unsupervised e-mail use make a huge decision, and it is not made lightly. Because these parents accept the risk that their children will engage in dangerous online behavior, the problem of pornographic spam seems almost trivial by comparison. If the parents trust their children enough to give them that autonomy, perhaps we should infer that the parents deem their children responsible enough to cope with pornographic spam.

Regulation cannot easily solve these problems. Efforts to specifically ban pornographic spam are likely unconstitutional and do not affect e-mails from foreign jurisdictions. Lesser efforts, like mandatory labeling, have low efficacy. Ultimately, there can be no substitute for parental involvement in their children’s use of e-mail.

---


III. CONCLUSION

Society is still evolving ways to cope with media saturation. Spam contributes to this problem, but so do other media. Yet, many recipients hate spam more than other ads. As explored by this Essay, this dichotomous attitude is hard to explain. Nevertheless, the anger has caused anti-spam rhetoric to reach hyperbolic levels. But, while many spam opponents decry spam as a system breakdown, the breakdown has been more political than technological. Most state-based attempts to regulate spam, a product of political grandstanding or legislator rage instead of rational policy-making, were ineffectual,\(^\text{60}\) reflecting their weak policy underpinnings. Early feedback on CAN-SPAM suggests the federal law will not be any more effective.\(^\text{61}\)

Even if CAN-SPAM beneficially affects the flow of unwanted e-mails, any legislative solution seems inherently empty. Without legislative intervention, society will find ways to cope with spam, just as we have with other media. Meanwhile, entrepreneurs will continue to develop better tools to sort wanted and unwanted communications. Thus, more patience with the spam “problem” might have facilitated the development of superior results organically.

\(^{60}\) See e.g. E-mail in December Dominated by Spam, L.A. Times (Jan. 3, 2004) (available in LEXIS, News & Business > News > By Individual Publication > L> Los Angeles Times) (citing a study by MessageLabs showing that spam had increased from thirty-four percent of all e-mail in December 2002 to fifty-six percent of all e-mail in December 2003); Brightmail Inc., 60% of Internet E-Mail is Now Spam According to Anti-Spam Leader Brightmail\(^\text{®}\); <http://www.brightmail.com/pressreleases/082003_50-percent-spam.html> (Aug. 20, 2003) (press release of Brightmail Inc.) (quoting Enrique Salem, Brightmail President and CEO, as saying that “In less than 2 years, spam messages have increased from 8% of all e-mail traffic to more than half”).

\(^{61}\) See Stefanie Olsen, CNET News.com, Study: Spammers Turning Blind Eye to the Law <http://news.com.com/2102-1032_3-5156629.html?tag=st.util.print> (Feb. 10, 2004) (citing studies showing that only three percent of bulk commercial e-mail complied with the law, that spam had increased as a percentage of all e-mail following the law’s passage, and that more spam was originating overseas since the law passed).

Then again, many experts never expected the law to be effective, which perhaps reinforces that the predominant problem with spam is political. See Declan McCullagh, CNET News.com, Spam Keeps Cookin’—Despite New Laws <http://news.com.com/2102-1024_3-5065.html?tag=st.util.print> (Feb. 17, 2004) (“[a] U.S. Justice Department prosecutor warned Tuesday that a new spam law’s criminal sanctions likely will not stem the flow of bulk solicitations into e-mail in-boxes”).
Public Law 108–187
108th Congress

An Act

To regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.

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 “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003”, or the “CAN-SPAM Act of 2003”.

SEC. 2. CONGRESSIONAL FINDINGS AND POLICY.

(a) FINDINGS.—The Congress finds the following:

(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and
institutions can handle without further investment in infra-
structure.

(7) Many senders of unsolicited commercial electronic mail 
purposefully disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail 
purposefully include misleading information in the messages'
subject lines in order to induce the recipients to view the 
messages.

(9) While some senders of commercial electronic mail mes-
sages provide simple and reliable ways for recipients to reject 
(or “opt-out” of) receipt of commercial electronic mail from 
such senders in the future, other senders provide no such 
“opt-out” mechanism, or refuse to honor the requests of recip-
ets not to receive electronic mail from such senders in the 
future, or both.

(10) Many senders of bulk unsolicited commercial electronic 
mail use computer programs to gather large numbers of elec-
tronic mail addresses on an automated basis from Internet 
websites or online services where users must post their 
addresses in order to make full use of the website or service.

(11) Many States have enacted legislation intended to regu-
late or reduce unsolicited commercial electronic mail, but these 
statutes impose different standards and requirements. As a 
result, they do not appear to have been successful in addressing 
the problems associated with unsolicited commercial electronic 
mail, in part because, since an electronic mail address does 
not specify a geographic location, it can be extremely difficult 
for law-abiding businesses to know with which of these dis-
parate statutes they are required to comply.

(12) The problems associated with the rapid growth and 
abuse of unsolicited commercial electronic mail cannot be solved 
by Federal legislation alone. The development and adoption 
of technological approaches and the pursuit of cooperative 
efforts with other countries will be necessary as well.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY.—On 
the basis of the findings in subsection (a), the Congress determines 
that—

15 USC 7702.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE CONSENT.—The term “affirmative con-
 sent”, when used with respect to a commercial electronic mail 
message, means that—

(A) the recipient expressly consented to receive the 
message, either in response to a clear and conspicuous 
request for such consent or at the recipient’s own initiative; 
and

(B) if the message is from a party other than the 
party to which the recipient communicating such consent, 
the recipient was given clear and conspicuous notice at
the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

(2) COMMERCIAL ELECTRONIC MAIL MESSAGE.—
   (A) IN GENERAL.—The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

   (B) TRANSACTIONAL OR RELATIONSHIP MESSAGES.—The term "commercial electronic mail message" does not include a transactional or relationship message.

   (C) REGULATIONS REGARDING PRIMARY PURPOSE.—Not later than 12 months after the date of the enactment of this Act, the Commission shall issue regulations pursuant to section 13 defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message.

   (D) REFERENCE TO COMPANY OR WEBSITE.—The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) DOMAIN NAME.—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.

(5) ELECTRONIC MAIL ADDRESS.—The term "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) ELECTRONIC MAIL MESSAGE.—The term "electronic mail message" means a message sent to a unique electronic mail address.


(8) HEADER INFORMATION.—The term "header information" means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message.

(9) INITIATE.—The term "initiate", when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or
transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message.

(10) INTERNET.—The term "Internet" has the meaning given that term in the Internet Tax Freedom Act (47 U.S.C. 151 nt).

(11) INTERNET ACCESS SERVICE.—The term "Internet access service" has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(12) PRODUCE.—The term "produce", when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf.

(13) PROTECTED COMPUTER.—The term "protected computer" has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.

(14) RECIPIENT.—The term "recipient", when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered. If a recipient of a commercial electronic mail message has one or more electronic mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.

(15) ROUTINE CONVEYANCE.—The term "routine conveyance" means the transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.

(16) SENDER.—
(A) IN GENERAL.—Except as provided in subparagraph (B), the term "sender", when used with respect to a commercial electronic mail message, means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message.

(B) SEPARATE LINES OF BUSINESS OR DIVISIONS.—If an entity operates through separate lines of business or divisions and holds itself out to the recipient throughout the message as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.

(17) TRANSACTIONAL OR RELATIONSHIP MESSAGE.—
(A) IN GENERAL.—The term "transactional or relationship message" means an electronic mail message the primary purpose of which is—
(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;
(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide—

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient's standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

(B) MODIFICATION OF DEFINITION.—The Commission by regulation pursuant to section 13 may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this Act to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this Act.

SEC. 4. PROHIBITION AGAINST PREATORY AND ABUSIVE COMMERCIAL E-MAIL.

(a) Offense.—

(1) In general.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

§ 1037. Fraud and related activity in connection with electronic mail

(a) In general.—Whoever, in or affecting interstate or foreign commerce, knowingly—

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic
mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

"(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).

"(b) Penalties.—The punishment for an offense under subsection (a) is—

"(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

"(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

"(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

"(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

"(A) the offense is an offense under subsection (a)(1);

"(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

"(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

"(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

"(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

"(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

"(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

"(c) Forfeiture.—

"(1) In General.—The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—

"(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

"(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

458
“(2) PROCEDURES.—The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

“(d) DEFINITIONS.—In this section:

“(1) LOSS.—The term ‘loss’ has the meaning given that term in section 1030(a) of this title.

“(2) MATERIALLY.—For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

“(3) MULTIPLE.—The term ‘multiple’ means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

“(4) OTHER TERMS.—Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.”.

(2) CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

“Sec. 1037. Fraud and related activity in connection with electronic mail.”.

(b) UNITED STATES SENTENCING COMMISSION.—

(1) DIRECTIVE.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, United States Code, as added by this section, and other offenses that may be facilitated by the sending of large quantities of unsolicited electronic mail.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for—

(A) those convicted under section 1037 of title 18, United States Code, who—

(i) obtained electronic mail addresses through improper means, including—

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(II) randomly generating electronic mail addresses by computer; or

(ii) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and

28 USC 994 note.
(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

(c) Sense of Congress.—It is the sense of Congress that—

(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and

(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18, United States Code (relating to fraud and false statements); chapter 71 of title 18, United States Code (relating to obscenity); chapter 110 of title 18, United States Code (relating to the sexual exploitation of children); and chapter 95 of title 18, United States Code (relating to racketeering), as appropriate.

SEC. 5. OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL.

(a) Requirements for Transmission of Messages.—

(1) Prohibition of False or Misleading Transmission Information.—It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph—

(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;

(B) a “from” line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and

(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) Prohibition of Deceptive Subject Headings.—It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact.
regarding the contents or subject matter of the message (consistent with the criteria used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).

(3) INCLUSION OF RETURN ADDRESS OR COMPARABLE MECHANISM IN COMMERCIAL ELECTRONIC MAIL.—

(A) IN GENERAL.—It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that—

(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

(B) MORE DETAILED OPTIONS POSSIBLE.—The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS.—A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION.—

(A) IN GENERAL.—If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful—

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;

(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic
mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or (iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

(B) SUBSEQUENT AFFIRMATIVE CONSENT.—A prohibition in subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

(5) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN commercial ELECTRONIC MAIL.—(A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—

(i) clear and conspicuous identification that the message is an advertisement or solicitation;

(ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and

(iii) a valid physical postal address of the sender.

(B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(6) MATERIALLY.—For purposes of paragraph (1), the term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

(b) AGGRAVATED VIOLATIONS RELATING TO COMMERCIAL ELECTRONIC MAIL.—

(1) ADDRESS HARVESTING AND DICTIONARY ATTACKS.—

(A) IN GENERAL.—It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that—

(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online
service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or

(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.

(B) DISCLAIMER.—Nothing in this paragraph creates an ownership or proprietary interest in such electronic mail addresses.

(2) AUTOMATED CREATION OF MULTIPLE ELECTRONIC MAIL ACCOUNTS.—It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a).

(3) RELAY OR RETRANSMISSION THROUGH UNAUTHORIZED ACCESS.—It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

(c) SUPPLEMENTARY RULEMAKING AUTHORITY.—The Commission shall by regulation, pursuant to section 13—

(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable after taking into account—

(A) the purposes of subsection (a);
(B) the interests of recipients of commercial electronic mail; and
(C) the burdens imposed on senders of lawful commercial electronic mail; and

(2) specify additional activities or practices to which subsection (b) applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection (a).

(d) REQUIREMENT TO PLACE WARNING LABELS ON COMMERCIAL ELECTRONIC MAIL CONTAINING SEXUALLY ORIENTED MATERIAL.—

(1) IN GENERAL.—No person may initiate or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and—

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only—

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;
(ii) the information required to be included in the message pursuant to subsection (a)(5); and
(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) PRIOR AFFIRMATIVE CONSENT.—Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(3) PRESCRIPTION OF MARKS AND NOTICES.—Not later than 120 days after the date of the enactment of this Act, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.

(4) DEFINITION.—In this subsection, the term "sexually oriented material" means any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

(5) PENALTY.—Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

SEC. 6. BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION.

(a) IN GENERAL.—It is unlawful for a person to promote, or allow the promotion of, that person’s trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person—

(1) knows, or should have known in the ordinary course of that person’s trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;

(2) received or expected to receive an economic benefit from such promotion; and

(3) took no reasonable action—

(A) to prevent the transmission; or

(B) to detect the transmission and report it to the Commission.

(b) LIMITED ENFORCEMENT AGAINST THIRD PARTIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), a person (hereinafter referred to as the “third party”) that provides goods, products, property, or services to another person that violates subsection (a) shall not be held liable for such violation.

(2) EXCEPTION.—Liability for a violation of subsection (a) shall be imputed to a third party that provides goods, products, property, or services to another person that violates subsection (a) if that third party—
(A) owns, or has a greater than 50 percent ownership or economic interest in, the trade or business of the person that violated subsection (a); or
(B)(i) has actual knowledge that goods, products, property, or services are promoted in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1); and
(ii) receives, or expects to receive, an economic benefit from such promotion.

(c) EXCLUSIVE ENFORCEMENT BY FTC.—Subsections (f) and (g) of section 7 do not apply to violations of this section.
(d) SAVINGS PROVISION.—Except as provided in section 7(f)(8), nothing in this section may be construed to limit or prevent any action that may be taken under this Act with respect to any violation of any other section of this Act.

SEC. 7. ENFORCEMENT GENERALLY.

(a) VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.—Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were 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)).

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES.—Compliance with this Act shall be enforced—

(1) under 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, organizations operating under section 23 or 23A of the Federal Reserve Act (12 U.S.C. 601 and 611), and bank holding companies, by the Board;

(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; and

(D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, by the Director of the Office of Thrift Supervision;

(2) under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the Board of the National Credit Union Administration with respect to any Federally insured credit union;

(3) under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to any broker or dealer;

(4) under the Investment Company Act of 1940 (15 U.S.C. 80a–1 et seq.) by the Securities and Exchange Commission with respect to investment companies;

(5) under the Investment Advisers Act of 1940 (15 U.S.C. 80b–1 et seq.) by the Securities and Exchange Commission with respect to investment advisers registered under that Act;
(6) under State insurance law in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 104 of the Gramm-Bliley-Leach Act (15 U.S.C. 6701), except that in any State in which the State insurance authority elects not to exercise this power, the enforcement authority pursuant to this Act shall be exercised by the Commission in accordance with subsection (a);

(7) under 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;

(8) under 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;

(9) under the Farm Credit Act of 1971 (12 U.S.C. 201 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; and

(10) under the Communications Act of 1934 (47 U.S.C. 151 et seq.) by the Federal Communications Commission with respect to any person subject to the provisions of that Act.

(c) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a Federal Trade Commission trade regulation rule. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) ACTIONS BY THE COMMISSION.—The Commission shall prevent any person from violating this Act 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 Act. Any entity that violates any provision of that subtitle is 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 that subtitle.

(e) AVAILABILITY OF CEASE-AND-DESIST ORDERS AND INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE.—Notwithstanding any other provision of this Act, in any proceeding or action pursuant to subsection (a), (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), neither the Commission nor the Federal Communications Commission shall be required to allege or prove the state of mind required by such section or subparagraph.

(f) ENFORCEMENT BY STATES.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency 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 any person who
violates paragraph (1) or (2) of section 5(a), who violates section 5(d), or who engages in a pattern or practice that violates paragraph (3), (4), or (5) of section 5(a), of this Act, the attorney general, official, or agency of 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—

(A) to enjoin further violation of section 5 of this Act by the defendant; or

(B) to obtain damages on behalf of residents of the State, in an amount equal to the greater of—

(i) the actual monetary loss suffered by such residents; or

(ii) the amount determined under paragraph (3).

(2) AVAILABILITY OF INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE.—Notwithstanding any other provision of this Act, in a civil action under paragraph (1)(A) of this subsection, the attorney general, official, or agency of the State shall not be required to allege or prove the state of mind required by section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3).

(3) STATUTORY DAMAGES.—

(A) IN GENERAL.—For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message received by or addressed to such residents treated as a separate violation) by up to $250.

(B) LIMITATION.—For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $2,000,000.

(C) AGGRAVATED DAMAGES.—The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if—

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravating violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES.—In assessing damages under subparagraph (A), the court may consider whether—

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES.—In the case of any successful action under paragraph (1), the court, in its discretion, may award the costs of the action and reasonable attorney fees to the State.

(5) RIGHTS OF FEDERAL REGULATORS.—The State shall serve prior written notice of any action under paragraph (1) upon Notice.

Records.
the Federal Trade Commission or the appropriate Federal regulator determined under subsection (b) and provide the Commission or appropriate Federal regulator with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Federal Trade Commission or appropriate Federal regulator shall have the right—

   (A) to intervene in the action;
   (B) upon so intervening, to be heard on all matters arising therein;
   (C) to remove the action to the appropriate United States district court; and
   (D) to file petitions for appeal.

(6) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act 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—

   (A) conduct investigations;
   (B) administer oaths or affirmations; or
   (C) compel the attendance of witnesses or the production of documentary and other evidence.

(7) VENUE; SERVICE OF PROCESS.—

   (A) VENUE.—Any action brought under paragraph (1) 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.
   (B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

   (i) is an inhabitant; or
   (ii) maintains a physical place of business.

(8) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission, or other appropriate Federal agency under subsection (b), has instituted a civil action or an administrative action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this Act alleged in the complaint.

(9) REQUIRITED SCIENTER FOR CERTAIN CIVIL ACTIONS.—Except as provided in section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), in a civil action brought by a State attorney general, or an official or agency of a State, to recover monetary damages for a violation of this Act, the court shall not grant the relief sought unless the attorney general, official, or agency establishes that the defendant acted with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, of the act or omission that constitutes the violation.

(g) ACTION BY PROVIDER OF INTERNET ACCESS SERVICE.—

(1) ACTION AUTHORIZED.—A provider of Internet access service adversely affected by a violation of section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of section 5(a), may bring a civil action in
any district court of the United States with jurisdiction over
the defendant—

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the
greater of—

(i) actual monetary loss incurred by the provider
of Internet access service as a result of such violation;

or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF “PROCURER”.—In any action
brought under paragraph (1), this Act shall be applied as if
the definition of the term “procure” in section 3(12) contained,
after “behalf” the words “with actual knowledge, or by con-
sciously avoiding knowing, whether such person is engaging,
or will engage, in a pattern or practice that violates this Act”.

(3) STATUTORY DAMAGES.—

(A) IN GENERAL.—For purposes of paragraph (1)(B)(ii),
the amount determined under this paragraph is the amount
calculated by multiplying the number of violations (with
each separately addressed unlawful message that is trans-
mited or attempted to be transmitted over the facilities
of the provider of Internet access service, or that is trans-
mited or attempted to be transmitted to an electronic
mail address obtained from the provider of Internet access
service in violation of section 5(b)(1)(A)(i), treated as a
separate violation) by—

(i) up to $100, in the case of a violation of section
5(a)(1); or

(ii) up to $25, in the case of any other violation
of section 5.

(B) LIMITATION.—For any violation of section 5 (other
than section 5(a)(1)), the amount determined under
subparagraph (A) may not exceed $1,000,000.

(C) AGGRAVATED DAMAGES.—The court may increase
a damage award to an amount equal to not more than
three times the amount otherwise available under this
paragraph if—

(i) the court determines that the defendant com-
mitted the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one
or more of the aggravated violations set forth in section
5(b).

(D) REDUCTION OF DAMAGES.—In assessing damages
under subparagraph (A), the court may consider whether—

(i) the defendant has established and implemented,
with due care, commercially reasonable practices and
procedures designed to effectively prevent such viola-
tions; or

(ii) the violation occurred despite commercially
reasonable efforts to maintain compliance with the
practices and procedures to which reference is made
in clause (i).

(4) ATTORNEY FEES.—In any action brought pursuant to
paragraph (1), the court may, in its discretion, require an
undertaking for the payment of the costs of such action, and
assess reasonable costs, including reasonable attorneys' fees,
against any party.
SEC. 8. EFFECT ON OTHER LAWS.

(a) FEDERAL LAW.—(1) Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231, respectively), chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

(2) Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages.

(b) STATE LAW.—

(1) IN GENERAL.—This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any commercial electronic mail message or information attached thereto.

(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.—This Act shall not be construed to preempt the applicability of—

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or

(B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

(c) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE.—Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

SEC. 9. DO-NOT-E-MAIL REGISTRY.

(a) IN GENERAL.—Not later than 6 months after the date of enactment of this Act, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that—

(1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry;

(2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and

(3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.

(b) AUTHORIZATION TO IMPLEMENT.—The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act.

SEC. 10. STUDY OF EFFECTS OF COMMERCIAL ELECTRONIC MAIL.

(a) IN GENERAL.—Not later than 24 months after the date of the enactment of this Act, the Commission, in consultation with the Department of Justice and other appropriate agencies, shall submit a report to the Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions.
PUBLIC LAW 108–187—DEC. 16, 2003 117 STAT. 2717

(b) REQUIRED ANALYSIS.—The Commission shall include in the report required by subsection (a)—
(1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act;
(2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal Government could pursue through international negotiations, fora, organizations, or institutions; and
(3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic.

SEC. 11. IMPROVING ENFORCEMENT BY PROVIDING REWARDS FOR INFORMATION ABOUT VIOLATIONS; LABELING.

The Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce—
(1) a report, within 9 months after the date of enactment of this Act, that sets forth a system for rewarding those who supply information about violations of this Act, including—
(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that—
(i) identifies the person in violation of this Act; and
(ii) supplies information that leads to the successful collection of a civil penalty by the Commission; and
(B) procedures to minimize the burden of submitting a complaint to the Commission concerning violations of this Act, including procedures to allow the electronic submission of complaints to the Commission; and
(2) a report, within 18 months after the date of enactment of this Act, that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters “ADV” in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan.

SEC. 12. RESTRICTIONS ON OTHER TRANSMISSIONS.

Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting “, or any person outside the United States if the recipient is within the United States” after “United States”.

SEC. 13. REGULATIONS.

(a) IN GENERAL.—The Commission may issue regulations to implement the provisions of this Act (not including the amendments made by sections 4 and 12). Any such regulations shall be issued in accordance with section 553 of title 5, United States Code.
(b) LIMITATION.—Subsection (a) may not be construed to authorize the Commission to establish a requirement pursuant to section 5(a)(5)(A) to include any specific words, characters, marks, or labels in a commercial electronic mail message, or to include the identification required by section 5(a)(5)(A) in any particular part of such a mail message (such as the subject line or body).

SEC. 14. APPLICATION TO WIRELESS.

(a) EFFECT ON OTHER LAW.—Nothing in this Act shall be interpreted to preclude or override the applicability of section 227 of the Communications Act of 1934 (47 U.S.C. 227) or the rules prescribed under section 3 of the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6102).

(b) FCC RULEMAKING.—The Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages. The Federal Communications Commission, in promulgating the rules, shall, to the extent consistent with subsection (c)—

(1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender, except as provided in paragraph (3);

(2) allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the sender;

(3) take into consideration, in determining whether to subject providers of commercial mobile services to paragraph (1), the relationship that exists between providers of such services and their subscribers, but if the Commission determines that such providers should not be subject to paragraph (1), the rules shall require such providers, in addition to complying with the other provisions of this Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages from the provider—

(A) at the time of subscribing to such service; and

(B) in any billing mechanism; and

(4) determine how a sender of mobile service commercial messages may comply with the provisions of this Act, considering the unique technical aspects, including the functional and character limitations, of devices that receive such messages.

(c) OTHER FACTORS CONSIDERED.—The Federal Communications Commission shall consider the ability of a sender of a commercial electronic mail message to reasonably determine that the message is a mobile service commercial message.

(d) MOBILE SERVICE COMMERCIAL MESSAGE DEFINED.—In this section, the term “mobile service commercial message” means a commercial electronic mail message that is transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service (as such term is defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d))) in connection with such service.

SEC. 15. SEPARABILITY.

If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of this Act and the application of such provision to other persons or circumstances shall not be affected.
SEC. 16. EFFECTIVE DATE.

The provisions of this Act, other than section 9, shall take effect on January 1, 2004.


LEGISLATIVE HISTORY—S. 877:
CONGRESSIONAL RECORD, Vol. 149 (2003):
Oct. 22, considered and passed Senate.
Nov. 21, considered and passed House, amended.
Nov. 25, Senate concurred in House amendment with an amendment.
Dec. 8, House concurred in Senate amendment.
burden, when balanced against the offsetting benefit of allowing email recipients to choose to
limit further unwanted commercial electronic mail messages from particular senders. The
Commission has not received any comments that lead it to believe that the final Rule will unduly
burden either the entities who sell, or those consumers who purchase, commercial products and
services through email messages.

List of Subjects in 16 CFR Part 316

Advertising, Business and industry, Computer technology, Consumer protection,
Labeling.

Accordingly, for the reasons set forth in the preamble above, the Commission amends title
16, Chapter I, Code of Federal Regulations, by revising Part 316 to read as follows:

PART 316—RULES IMPLEMENTING THE CAN-SPAM ACT OF 2003

Sec.

316.1 Scope.

316.2 Definitions.

316.3 Primary purpose.

316.4 Requirement to place warning labels on commercial electronic mail that contains sexually
oriented material.

316.5 Severability.


§ 316.1 Scope.

This part implements the Controlling the Assault of Non-Solicited Pornography and Marketing
§ 316.2 Definitions.

(a) The definition of the term “affirmative consent” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(1).


(c) The definition of the term “commercial electronic mail message” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(2).

(d) The definition of the term “electronic mail address” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(5).

(e) The definition of the term “electronic mail message” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(6).

(f) The definition of the term “initiate” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(9).

(g) The definition of the term “Internet” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(10).

(h) The definition of the term “procure” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(12).

(i) The definition of the term “protected computer” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(13).

(j) The definition of the term “recipient” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(14).
(k) The definition of the term “routine conveyance” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(15).

(l) The definition of the term “sender” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(16).

(m) The definition of the term “sexually oriented material” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7704(d)(4).

(n) The definition of the term “transactional or relationship message” is the same as the definition of that term in the CAN-SPAM Act, 15 U.S.C. 7702(17).

§ 316.3 Primary purpose.

(a) In applying the term “commercial electronic mail message” defined in the CAN-SPAM Act, 15 U.S.C. 7702(2), the “primary purpose” of an electronic mail message shall be deemed to be commercial based on the criteria in paragraphs (a)(1) through (a)(3) and (b) of this section:

(1) If an electronic mail message consists exclusively of the commercial advertisement or promotion of a commercial product or service, then the “primary purpose” of the message shall be deemed to be commercial.

(2) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as transactional or relationship content as set forth in paragraph (c) of this section, then the “primary purpose” of the message shall be deemed to be commercial if:

\[ \text{72} \]

\[ \text{476} \]

1The Commission does not intend for these criteria to treat as a “commercial electronic mail message” anything that is not commercial speech.
(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message contains the commercial advertisement or promotion of a commercial product or service; or

(ii) The electronic mail message’s transactional or relationship content as set forth in paragraph (c) of this section does not appear, in whole or in substantial part, at the beginning of the body of the message.

(3) If an electronic mail message contains both the commercial advertisement or promotion of a commercial product or service as well as other content that is not transactional or relationship content as set forth in paragraph (c) of this section, then the “primary purpose” of the message shall be deemed to be commercial if:

(i) A recipient reasonably interpreting the subject line of the electronic mail message would likely conclude that the message contains the commercial advertisement or promotion of a commercial product or service; or

(ii) A recipient reasonably interpreting the body of the message would likely conclude that the primary purpose of the message is the commercial advertisement or promotion of a commercial product or service. Factors illustrative of those relevant to this interpretation include the placement of content that is the commercial advertisement or promotion of a commercial product or service, in whole or in substantial part, at the beginning of the body of the message; the proportion of the message dedicated to such content; and how color, graphics, type size, and style are used to highlight commercial content.

(b) In applying the term “transactional or relationship message” defined in the CAN-SPAM Act, 15 U.S.C. § 7702(17), the “primary purpose” of an electronic mail message shall be
deemed to be transactional or relationship if the electronic mail message consists
exclusively of transactional or relationship content as set forth in paragraph (c) of this
section.

(c) Transactional or relationship content of email messages under the CAN-SPAM Act is
content:

(1) To facilitate, complete, or confirm a commercial transaction that the recipient has
previously agreed to enter into with the sender;

(2) To provide warranty information, product recall information, or safety or security
information with respect to a commercial product or service used or purchased by
the recipient;

(3) With respect to a subscription, membership, account, loan, or comparable ongoing
commercial relationship involving the ongoing purchase or use by the recipient of
products or services offered by the sender, to provide –
  (i) Notification concerning a change in the terms or features;
  (ii) Notification of a change in the recipient's standing or status; or
  (iii) At regular periodic intervals, account balance information or other type of
        account statement;

(4) To provide information directly related to an employment relationship or related
benefit plan in which the recipient is currently involved, participating, or enrolled;
or

(5) To deliver goods or services, including product updates or upgrades, that the
recipient is entitled to receive under the terms of a transaction that the recipient has
previously agreed to enter into with the sender.
§ 316.4 Requirement to place warning labels on commercial electronic mail that contains sexually oriented material.

(a) Any person who initiates, to a protected computer, the transmission of a commercial electronic mail message that includes sexually oriented material must:

(1) Exclude sexually oriented materials from the subject heading for the electronic mail message and include in the subject heading the phrase "SEXUALLY-EXPLICIT:" in capital letters as the first nineteen (19) characters at the beginning of the subject line;²

(2) Provide that the content of the message that is initially viewable by the recipient, when the message is opened by any recipient and absent any further actions by the recipient, include only the following information:

(i) The phrase "SEXUALLY-EXPLICIT:" in a clear and conspicuous manner;³

(ii) Clear and conspicuous identification that the message is an advertisement or solicitation;

(iii) Clear and conspicuous notice of the opportunity of a recipient to decline to receive further commercial electronic mail messages from the sender;

(iv) A functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that –

²The phrase "SEXUALLY-EXPLICIT" comprises 17 characters, including the dash between the two words. The colon (:) and the space following the phrase are the 18th and 19th characters.

³This phrase consists of nineteen (19) characters and is identical to the phrase required in section 316.4(a)(1).
(A) A recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and

(B) Remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message;

(v) Clear and conspicuous display of a valid physical postal address of the sender; and

(vi) Any needed instructions on how to access, or activate a mechanism to access, the sexually oriented material, preceded by a clear and conspicuous statement that to avoid viewing the sexually oriented material, a recipient should delete the email message without following such instructions.

(b) Prior affirmative consent. Paragraph (a) of this section does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

§ 316.5 Severability.

The provisions of this part 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, Commissioner Leibowitz not participating.

Donald S. Clark
Secretary
MEMORANDUM OPINION AND ORDER GRANTING PRELIMINARY INJUNCTION

JAMES F. HOLDERMAN, District Judge:

Before this court is the Federal Trade Commission's ("FTC") request for a preliminary injunction to be entered against defendants Daniel J. Lin, Mark M. Sadek, James Lin, and Christopher Chung. A Temporary Restraining Order ("TRO") against these defendants was entered on April 23, 2004 (Dkt. No. 6) and has continued by consent pending this ruling. Defendants Phoenix Avatar, LLC and DJL, LLC have failed to appear and a preliminary injunction was entered against these defendants on May 6, 2004. (Dkt. No. 14.) The request for a preliminary injunction against remaining defendants Daniel Lin, Mark Sadek, James Lin, and Christopher Chung is based on purported violations of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. § 7701 et seq. and 15 U.S.C. §§ 45(a), 52(a) ("FTC Act").

For the following reasons, the request for a preliminary injunction is granted.
JURISDICTION AND VENUE

This court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331; 1337(a) & 1345. The defendants have made a request that this action be transferred to the United States District Court for the Eastern District of Michigan for further proceedings, or, in the alternative, for this court to stay these proceedings. Neither of these requests are supported with any argument or law and are denied. Venue is appropriate in the Northern District of Illinois because defendants have transacted business here1, see 15 U.S.C. § 53(b), and defendants have provided no sufficient reason why these proceedings should be stayed.

FINDINGS OF FACT

Based on the evidence presented in the record, the court makes the following factual findings.

I. Background: FTC’s Preliminary Investigation Which Led to Avatar

Theresa J. Bresnahan (“Bresnahan”), paralegal specialist with the FTC, presented most of the FTC’s evidence in support of a preliminary injunction. Bresnahan testified that an e-mail consists of two parts, a header and a body.2 (PX 1.) Among other things, the header usually contains identifying information fields such as the intended recipient, the sender of the e-mail, the date, and a subject line. Oftentimes, the e-mail body will contain a hyperlink, which is a link to a specific Web site on the Internet. When a user “clicks” on a hyperlink, that user’s Internet browser opens up on the specified Web site. A domain name, which is usually purchased by a user, is a unique name that identifies a Web site. For example, www.xyz.com. A sub-page designation identifies subsequent

1 See (PX 1, ¶¶ 13-28); (PX 1 ¶ 23, Att. J at 5); (PX 1 ¶¶ 32-33); (PX 1, ¶ 35(d)).

2 Bresnahan submitted declarations. At the hearing, Bresnahan briefly testified on direct, affirming these previous declarations. For convenience, the court refers to statements in Bresnahan’s declarations as testimony.
Web pages within the main Web site. For example, "info" is the sub-page designation in
www.xyz.com/info, and clicking on this as a hyperlink would take the user to the "info" sub-page
within the www.xyz.com Web site.

According to Bresnahan, Internet promoters will often use an "affiliate system" to promote
their products or services. Promoters recruit affiliates to assist in advertising, oftentimes resulting
in affiliates sending out e-mails advertising the promoter’s product. Affiliates are ordinarily paid
on a commission basis and are assigned a unique identifier or "affiliate moniker." This affiliate
moniker is usually appended to the end of a hyperlink contained in an e-mail advertising the
promoter’s product. The affiliate moniker allows the promoter to track the affiliate's success, and
allows the affiliate to obtain commissions. For example, in the hyperlink
www.xyz.com/info/?id=123, "123" is the affiliate moniker. The promoter is able to track sales
generated by this hyperlink to the person assigned the particular affiliate moniker "123."

Bresnahan testified that the FTC maintains, for law enforcement purposes, an e-mail address
where consumers can forward unsolicited commercial e-mail messages, commonly referred to as
"spam." These e-mails are stored in a searchable database ("spam database"). As part of her duties
as a paralegal specialist with the FTC, Bresnahan was asked to search the FTC’s spam database as
well as commercial Internet newsgroups for suspected misleading or deceptive spam. After
reviewing a number of spam messages containing a variety of domain names, Bresnahan began to
recognize two similarities among certain hyperlinks. First, she noticed that the structure of certain
hyperlinks was similar in that these hyperlinks shared similar sub-page designations ending in similar
affiliate monikers. For example, Bresnahan testified that a typical hyperlink in the spam she
reviewed was formatted as follows: "www.keeyouirmatchhappy.biz/m2/index.php?aff_id=m4," or
“www.countupandlookaway.com/m2/index.php?aff_id=m4.” Second, Bresnahan began to notice that hyperlinks with these similar sub-page designations were linked to Web sites selling certain products. For example, hyperlinks containing the sub-page designation “m2” were linked to Web sites selling the Med Diet Patch, a purported weight-loss product.

Finally, Bresnahan began to notice that the hyperlinks described above, containing similar sub-page designations and affiliate monikers, frequently linked to Web sites with similar looking content. The hyperlinks with similar sub-page designations and affiliate monikers led to Web sites with similar content even though the domain names were often different. This led Bresnahan to draw the inference that this certain variety of domain names she encountered were all related to the same enterprise. As a result of this inference, Bresnahan and others at the FTC began to compile a list of all these domain names they believed to be related. The FTC designated these related domain names the “Avatar” domain names. According to Bresnahan, the FTC identified 108 Avatar domain names. (PX 1, Att. A.)

In the course of this investigation, FTC personnel visited the Web sites of domain name registrars to obtain information on who had registered the various Avatar domain names. The 103 Avatar domain names for which domain name registration information was available are purportedly registered to twenty-two persons or entities located in various countries throughout the world, including: South Africa, Lithuania, India, Singapore, Taiwan, Korea, France, Russia, Argentina, Malaysia, Turkey, Mexico and China. (PX 1, Att. B.)

II. Undercover Purchases

For purposes of investigating the Avatar domain names, Bresnahan posed as a consumer, using an alias and undercover information, including a shipping address, telephone line, e-mail
address and a VISA credit card account. Bresnahan made four purchases from Web sites with Avatar domain names, two of which are relevant to the instant request for a preliminary injunction. Bresnahan linked to these Web sites by clicking on hyperlinks contained in spam received from the spam database or commercial Internet news groups.

A. First Undercover Purchase: Med Diet Patch from countupandlookaway.com

On January 9, 2004, Bresnahan used a personal computer to visit the Web site www.countupandlookaway.com/m2/index.php?AFF_ID=m4 ("countupandlookaway.com"), for the purpose of purchasing the product sold on that Web site, a Med Diet Patch. A printed copy of the countupandlookaway.com Web site was admitted into evidence. (PX 1, Att. C.) The home page, or initial page encountered when visiting countupandlookaway.com, included five links leading to five separate sub-pages: PRODUCT INFO, TESTIMONIALS, FAQ'S, CONTACT, ORDER NOW. Despite the sub-page entitled CONTACT, this Web site contained no information identifying the seller. There was no telephone number, address, e-mail address or other identifying information. The CONTACT sub-page purportedly allowed a consumer to contact the seller by submitting an online form. (PX 1, Att. C, p. 6.)

To purchase the Med Diet Patch, Bresnahan clicked on the hyperlink “ORDER NOW” which took her Internet browser to the sub-page used to place orders (“Order Page”). (PX 1, Att. C at 8-9.) The Order Page was entitled “Diet Patch Secure Order Form,” and it required the entry of identifying and payment information. Bresnahan entered the corresponding undercover information and clicked on a button marked “Click to Authorize” to complete the $59.95 purchase for the Med Diet Patch.3

3 The completed Order Page was admitted into evidence with the undercover FTC information redacted. See (PX 1, Att. C at 8-9.)
After submitting the order, Bresnahan’s Internet browser was directed to a confirmation page. This page stated that the charge appearing on the FTC’s undercover credit card would appear as “AIT” or “MYPAYSYSTEMS.” (PX 1., Att. C at 10.)

MyPaySystems is a credit card processor located in Quebec, Canada, which maintains its own Web site: www.mypaysystems.com. This Web site allows consumers to inquire about credit card charges processed by MyPaySystems. Upon entering the credit card information used to make a purchase processed through MyPaySystems, a consumer can access an “Order Details” page produced by MyPaySystems. With respect to Bresnahan’s purchase of the Med Diet Patch, on January 14, 2004, MyPaySystems listed the Vendor Company Name as “PHOENIX AVATAR, LLC,” the Vendor’s Customer Support Line as (866) 248-1101, and the Vendor’s Web site as www.avatarnutrition.com. See (PX1, Att. D.)

On or about January 14, 2004, a package was received in response to Bresnahan’s undercover purchase of the Med Diet Patch. The package was addressed to the undercover alias used by Bresnahan and it was marked as having been sent by Avatar Nutrition at P.O. Box 251570, West Bloomfield, Michigan. See (PX 1, Att. F.) Contained in the package was an invoice dated January 9, 2004, from “AIT Herbal Marketing/Avatar Nutrition.” (PX 1, Att. H.) The telephone number appearing on the invoice – (866) 248-1101 – was the same telephone number appearing on the MyPaySystems’s Order Details page. The invoice also listed an e-mail address at support@aitmarketing.com, and a Web site address at www.avatarnutrition.com. A printed copy of www.avatarnutrition.com was entered into evidence. (PX 1, Att. I.) The package contained a product called “Premium Diet Patch.” (PX 1, Att. G.)
B. Second Undercover Purchase: Slim Form Patch from keepyourmatehappy.biz

On February 24, 2004, Bresnahan purchased a product entitled Slim Form Patch from www.keepyourmatehappy.biz/m2/index.php?AFF_ID=4 ("keepyourmatehappy.biz"). (PX 1, Att. J at 1-9.) This Web site was similar to the countupandlookaway.com Web site in that it contained no information identifying the seller. In a manner similar to the first undercover purchase, Bresnahan submitted a $59.95 order for a Slim Form Patch, and just as with the first purchase, her Internet browser was directed to a confirmation page that informed her the charge appearing on her credit card statement would appear as “AIT.” (PX 1 at 12.)

In response to this purchase, the FTC’s undercover credit card account was billed the $59.95 by AIT Herbal Marketing. (PX 4, Att. A.) The FTC offered evidence that this credit card charge was facilitated by a credit card processor called First Data. See (PX 5.) Records from First Data show defendant Daniel Lin, as the purported owner of AIT Herbal Marketing, opened a merchant account with First Data. (PX 5, FDC003.) These records also show the actual FTC credit card charge for this second undercover purchase in a log compiled by First Data for AIT Herbal Marketing charges. (PX 5, FDC00386).

On or about February 26, 2004, a package was received at the undercover address in response to the purchase of the Slim Form Patch. The box was addressed to the alias used by Bresnahan and sent via FedEx delivery. There was no invoice in the box. However, the FedEx label was marked as having been sent by Avatar Nutrition from P.O. Box 251570, West Bloomfield, Michigan. (PX 1, Att. K.) This address and the name Avatar Nutrition were also listed on the invoice received from the first undercover purchase. The product contained in the package was a Premium Diet Patch, the same product the FTC received in response to its first purchase. (PX 1, Att. L.)
III. Representations on the Web Sites and Product Packaging

The Web site countupandlookaway.com contained various representations about the Med Diet Patch. A banner is sprawled across the top of the home page and sub-pages in a font larger than most of the other text on the pages. The banner contains the term “Med DIET PATCH,” with three purported attributes listed directly under the term in similarly large font: “BURNS FAT”, “INCREASES ENERGY”, “CONTROLS APPETITE”. (PX 1, Att. C., p.1.) Also present in large font near the top of the home page are the following phrases: “LOSE WEIGHT THE EASY WAY,” “IT'S NOT A DIET... IT'S A PATCH.” (Id.) The body of the text on the home page begins with, “Med Diet Patch is a cutting-edge, advanced appetite suppressant, metabolism booster, and energy enhancer ... all in one!” and also contains the sentence, “Just place a new adhesive skin patch anywhere on your body, each day for continuous, safe, and effective weight loss.” (Id.)

This Web site keepyourmatehappy.biz contained this representation: “About The Patch: Slim Form Patch is a highly effective weight loss patch developed in Europe by Danish scientists and French biologists.” (PX 1, Att. J at 1.) The same page contained the representation: “Non-invasive safe and easy to use, this patch guarantees weight loss with dramatic results.” (Id.) The Web site also stated: “Slim For Patch is a 'steady' weight loss system. This means you lose fat. While the patch is working to turn fat into toned muscle, you can eat normally..., without dieting.” (Id., at 3.)

The FTC received a Premium Diet Pact in both of its purchases. (PX 1, Att. G, Att. L.) On the front of the packaging of this product, directly under the name Premium Diet Patch, is the phrase “WEIGHT LOSS FORMULA.” The back of the package states the following:

The Premium Diet Patch is specifically formulated to safely stimulate your metabolism, causing your body to use and absorb food more efficiently and to burn fat rather than store it. The patch will assist in decreasing your appetite as well as
increasing your energy, helping your body to lose weight naturally. Use the Premium Diet Patch every day until you reach your desired weight. It's safe, natural, and easy to use.

(Id.) The back of the package also contains a set of directions, a list of ingredients, and the following disclaimer: "These statements have not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure or prevent any disease." (Id.)

IV. Paper Trail Leading to the Defendants

A. Corporate Information

The FTC introduced evidence regarding the following information. Phoenix Avatar, LLC (the name MyPaySystems listed as the vendor of the first undercover purchase) was organized in Nevada on September 30, 2003, with a registered agent listed as EastBiz.com, Inc. (PX 1, Att. M.) Records from EastBiz.com pertaining to the formation of Phoenix Avatar, LLC were also introduced into evidence. (PX 10.) These records show that defendant James Lin, with a billing address of 1350 Chapin, Birmingham, MI, 48009 paid the $833 fee to EastBiz.com required to form an LLC in Nevada. (PX 10, EB003.) As described below, the records for bank account number 884282030 with National City Bank, controlled by defendants Daniel Lin, James Lin and Mark Sadek, show an $833 payment to EastBiz.com. (PX 7, EB 00105.)

The FTC introduced into evidence a filing for a Michigan Business Fictitious Name; "AIT HERBAL MARKETING," with a business address of 634 Woodward Ave., 4th F, Detroit, 48226. (PX 15.) The record listed a contact name and contact address as defendant Christopher Chung, 7080 Ten Hill Dr., West Bloomfield, MI. (PX 15.) The FTC also offered evidence showing that "Ait Herbal Mkt," with an address of 7080 Ten Hill Dr., W. Bloomfield, MI, through Mark Sadek, applied for P.O. Box 251570 in West Bloomfield Michigan (the address both undercover purchases
were received from). (PX 4, Att. P.) The FTC also introduced evidence received from AT&T Corporation relating to the telephone number information it received in making the first undercover purchase of the Med Diet Patch. This telephone number – (866) 248-1101, which was provided by MyPaySystems as the Vendor’s Customer Support Line for the first undercover purchase, and listed on the invoice the FTC received in regard to the first undercover purchase – was registered to AIT Herbal Marketing, located at 7080 10 Hill Street, West Bloomfield Michigan. (PX 1, Att. P). AT&T listed the contact name on the account as defendant Mark Sadek. (Id.)

Finally, the FTC offered evidence regarding a filing for a Michigan domestic limited liability company, DJL, LLC. (PX 1, Att. O.) Defendant Daniel Lin was listed as the agent for DJL, LLC in this filing, which listed the registered office address as 1350 Chapman, Birmingham, MI, 48009. (Id.)

B. Financial Records

The FTC also offered evidence regarding a bank account number 884282030 with National City Bank in the name of DJL, LLC. (PX 1, Att. Q; PX 7, NCB0095.) The signatories on this bank account are defendant Daniel Lin, President; defendant James Lin, Vice President; and defendant Mark Sadek, Director of Operations. Examination of the records of this bank account showed frequent deposits from various credit card merchant processors. (PX 7, NCB0095, NCB 00107-110.) According to Bresnahan, examination of the bank records indicates that from September 2003 to January 2003 the total amount deposited into this bank account was approximately $462,600. (PX 1 ¶ 34(c).) The records also indicate that a payment of $833 was made to EastBiz.com. (PX 7, EB 00105).

The FTC also introduced evidence regarding an account with the credit card processor First
Data. (PX 5.) Defendant Daniel Lin opened a merchant account with First Data under the name AIT Herbal Marketing. (PX 5, FDC003.) The AIT Herbal Marketing merchant account with First Data was identified as account number 267765788885. (PX 5, FDC00386.) The AIT Herbal Marketing merchant application with First Data instructed that credit card payments be deposited into bank account number 884282030. (PX 5, FDC003.) The records of bank account number 884282030 identify repeated deposits from “MERCHAND BANKCD 26776578885” from September 2003 through March 2003. (PX 7, NCB 0097-98, 107-110, 132-33.)

The FTC also offered evidence showing that the defendants purchased numerous Premium Diet Patches from a company called EyeFive in California. Defendant James Lin first contacted EyeFive in late August of 2003 to make a wholesale inquiry that led to the purchase of 500 bottles of VP-RX virility pills. See (PX 12, EF00505-06.) In early November 2003, EyeFive informed Defendant James Lin that it was now marketing the Premium Diet Patch. (PX 12, EF00389-91.) In mid-November 2003, Lin bought 500 premium diet patches for $5.67 each. (PX 12, EF00402; EF0023.) He bought another 200 diet patches in March of 2004, (PX 12, EF0035), and he ordered another 100 diet patches on April 27, 2004. (PX 12, EF0047; EF0027.) All of these products were shipped to DJL, LLC, with an address in New York, New York. (PX 12, EF0023; EF0035; EF0047.)

V. Expert Testimony Regarding the Efficacy of the Premium Diet Patch

The FTC presented evidence from Michael Jensen M.D. (“Jensen”). Jensen is a professor of medicine at the Mayo Medical School, located in Rochester, Minnesota, and a member of the Endocrine Research Unit of the Mayo Clinic. (PX 2 ¶ 1.) Jensen reviewed printouts of the two Websites, countupandlookaway.com and keepyourmatehappy.biz, as well as a photocopy of the Premium
Diet Patch. Jensen found, based upon his professional experience and knowledge, "that none of the ingredients listed on the weight-loss patch label and web site, separately or together, could cause any weight-loss." (Id. ¶ 9.) Jensen also found that "none of the ingredients listed on the weight loss patch label and web site, separately or together, could cause an increase in metabolism, a decrease in appetite, and a reduction of food cravings, thereby enabling users to lose substantial, or any weight." (Id. ¶ 10.)

Under cross-examination Jensen stated that "the standard scientific approach to testing a patch product would be to give an active patch to a group of people and a placebo patch to a group of people and determine the effects between the two groups." (June 4, 2004 Hrg. Tr. at 44.) Jensen did not perform this type of scientific testing and testified that such testing would not have been helpful because the ingredients listed on the Web sites and on the Premium Diet Patch packaging had not been found "individually or in combination in the literature to provide a reasonable mechanism of action that could allow one to predict that they would have the effects they were claimed to have." (Id.)

The defendants introduced into evidence an excerpt from a television broadcast. (DX H.) In this excerpt, a television news show identified as channel 4, but with no city or geographic location noted, compared the effects of four common weight loss products: Slim Fast, a diet patch, diet and exercise, and surgical intervention. (June 4 2004 Hrg. Tr. at 69.) Four contestants were each asked to utilize one of the respective diet methods over a period of four weeks, and the result was that a Mr. Ortiz, who utilized a diet patch, claimed to have lost 25 pounds over a four week period. (Id.) In response to this evidence, Dr. Jensen testified that (1) four weeks is not an adequate time test for treatments of obesity, the Food and Drug Administration, for example, requires one to
two years of testing to approve a new product for obesity treatment (June 4 2004 Hrg. Tr. at 66); (2) Mr. Ortiz's claimed success with a diet patch was not probative because Mr. Ortiz was biased as to the outcome of using the patch (Id. at 69); and (3) that this test was at most anecdotal evidence.⁴

VI. Expert Testimony Regarding Spam

The defendants called Paul H. Howell ("Howell"), Chief Information Technology Security Officer at the University of Michigan, Ann Arbor, Michigan to testify. See (Defs.' Ex. V; Dkt. No. 39, Att. N.) In his “Preliminary Report,” Howell explained that e-mail sender and receiver information can be easily forged. (Defs.' Ex. W at 1; Dkt. No. 39, Att. M at 1.) To explain how this information is forged, Howell analogized e-mail to regular mail (e.g., United States Postal Service). (Id. at 2.) Howell explained that both types of mail utilize an outer envelope. The senders of both types of mail generally place their return address on the outer envelope. However, with both types of mail it is possible to provide misleading information in the form of a false return address, which is unreliable for determining the source of the mail. Both types of mail also contain postmarks: computers, which process and forward e-mail, insert a line of test that is analogous to a postmark stamp in regular mail. This “electronic postmark” includes date and time stamps that can be used to trace back the origin of an e-mail. It is possible, however, to insert misleading electronic postmarks in an attempt to conceal the source of an e-mail. Howell testified that the sender information on the e-mails introduced into evidence by the FTC had been forged in an attempt to thwart the identification of the true sender.

According to Howell, the only reliable method for tracing an e-mail back to its true origin

⁴ The defendants also introduced a number of documents relating to the efficacy of certain herbal supplements in weight loss. Defendants have chosen not to rely upon any of these exhibits in their closing argument, and the court, accordingly, will not consider these documents.
is to confirm the validity of the electronic postmarks and follow those back to the original sending computer. Once the originating computer has been identified, various means may be used to determine who actually sent the e-mail. Howell testified that the FTC failed to follow this procedure by not attempting to identify the sending computer of the e-mails by tracking back the information in the electronic postmarks. Howell concluded that there is no circumstantial or direct technical evidence that links the sending of the e-mails in this case to any particular person. Howell also concluded that the sender information on the e-mails introduced into evidence by the FTC had been forged in an attempt to thwart the identification of the true sender.

The FTC introduced an expert report from Brent Dylan-Rudy Deterding ("Deterding"), Senior Security Analyst at LURHQ, a managed security services provided in Chicago, Illinois. (PX 25.) Deterding testified that senders of spam ("spammers") go to great lengths to obfuscate the true and complete transmission path spam takes.

Deterding testified that spammers' preferred method for hiding their identity is to utilize an "open proxy." (Id.) An open proxy is a computer that, with or often without the owner's knowledge, accepts connections from anyone, anywhere, and forwards the e-mails from those connections as if the e-mails had originated from the open proxy. According to Deterding, these open proxies result from either (1) insecure software that allows a spammer to utilize the open proxy or (2) software maliciously installed on a computer, such as worms, Trojan horses or viruses that turn the computer into an open proxy. (Id. at 2.) Deterding's report stated that it is a widely held opinion in the computer industry that a majority of spam is sent using open proxies. (Id.) Furthermore, ComCast, the nation's largest Internet Service Provider, estimates that nearly 90% of e-mail sent on its network is spam sent through open proxies. (Id.) (citation omitted). Deterding testified that the use of open
proxies makes tracing e-mail back to its true source near impossible. (Id. at 3.) Finally, Deterding concluded that the e-mails introduced by the FTC, that led to the two Web sites countupandlookaway.com and keepyourmatehappy.biz, were sent through open proxies, and, therefore, that there is not a reliable, accurate, technical method to determine the sender of these spam messages. (Id. at 4.)

STANDARD OF REVIEW

This court reviews the FTC's request for an injunction pursuant to 15 U.S.C. $ 45(b) under the "public interest" test, which requires that this court to (1) determine the FTC's likelihood of success on the merits, and (2) balance the equities. FTC v. Word Travel Vacation Brokers, Inc., 861 F.2d 1020, 1028-29 (7th Cir. 1988) ("We believe that the legislative history of section 13(b) makes it quite clear that the 'public interest' test is the correct approach."). Under the "public interest" test, the FTC need not prove irreparable injury to obtain a preliminary injunction. Kinney v. Int'l Union of Operating Eng'rs, Local 150, AFL-CIO, 994 F.2d 1271, 1277 (7th Cir. 1993). The threshold showing of a likelihood to succeed under the traditional test is a better than negligible chance of success on the merits, and this court adopts that standard here. See Cooper v. Salazar, 196 F.3d 809, 813 (7th Cir. 1999).

Under the public interest test, "private concerns may certainly be considered, [but] public equities must receive far greater weight." World Travel Vacation Brokers, Inc., 861 F.2d at 1029; see also FTC v. Weyerhaeuser Co., 665 F.2d 1072, 1083 (D.C. Cir. 1981) ("When the Commission demonstrates a likelihood of ultimate success, a countershowing of private equities alone would not suffice to justify denial of a preliminary injunction."). That is not to say, however, that private equities receive no weight, as the Seventh Circuit has explained: "While not giving controlling
weight to 'private equities'—of course not—the cases give them some weight.” FTC v. Elders Grain, Inc., 868 F.2d 901, 903 (7th Cir. 1989). “[P]rivate equities are entitled to serious consideration,” especially where the defendant “can show irreparable injury to it from the grant of an injunction.” Id. “[I]f the defendant can show irreparable injury to it from the grant of the injunction, then merits and harms must be evaluated in the usual way.” Id. This “usual way” would involve a “sliding scale” approach. Id.; see also Ty, Inc. v. Jones Group Inc., 237 F.3d 891, 895-96 (7th Cir. 2001). This sliding scale approach requires that the court factor the FTC’s probability of success on the merits into the balance of the harms. Thus, “[a]lthough the plaintiff’s likelihood of success on the merits . . . the less harm from denial of the preliminary injunction the plaintiff need show in relation to the harm that the defendant will suffer if the preliminary injunction is granted.” Elders Grain, Inc., 868 F.2d at 903. “The sliding scale approach is not mathematical in nature, rather it is more properly characterized as subjective and intuitive, one which permits district courts to weigh the competing considerations and mold appropriate relief.” Ty, Inc., 237 F.3d at 896 (citations omitted).

ANALYSIS

I. FTC’s Likelihood of Success on the Merits

To establish a likelihood of success on the merits, the FTC must show a violation of the law that the defendants committed. The two statutes allegedly violated by the defendants are the FTC Act and CAN-SPAM. The court will first address whether these statutes have been violated and then, evaluating all of the evidence, the court will analyze the FTC’s likelihood of success in establishing the defendants’ liability at a trial on the merits.
A. Violations of the FTC Act and CAN-SPAM

(i) FTC Act

The FTC Act states, in pertinent part: "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." 15 U.S.C. § 45(a)(1). The FTC Act also prohibits the dissemination of false advertisement for the purpose of inducing the purchase of a drug or device. 15 U.S.C. § 52(a). The FTC Act deems such dissemination of false advertisement "an unfair or deceptive act of practice in or affecting commerce within the meaning of section 45." 15 U.S.C. § 52(b). The Seventh Circuit has explained that "representations ... likely [to] mislead consumers, acting reasonably, to their detriment" are deceptive within the meaning of section 45(a)(1) of the FTC Act. FTC v. World Travel Vacation Brokers, Inc., 861 F.2d 1020, 1029 (7th Cir. 1988) (citation omitted). "In addition, '[m]isrepresentations of material facts made for the purpose of inducing consumers to purchase services constitute unfair or deceptive acts or practices." Id. (citation omitted). The "misrepresentation or practice need not be made with an intent to deceive" to violate the FTC Act. In general, advertisements are considered deceptive if the proponent lacked a reasonable basis for asserting its truth. See Kraft, Inc. v. FTC, 970 F.2d 311, 314 (7th Cir. 1992); FTC v. Pantron I Corp., 33 F.3d 1088, 1096 (9th Cir. 1994); Thompson Medical Co. v. FTC, 791 F.2d 189, 193-94 (D.C. Cir. 1986). See also FTC v. Sabal, 32 F.Supp.2d 1004, 1007 (N.D. Ill. 1998).

This court rules that the FTC has a better than negligible chance of success on the merits of its claim that the representations regarding the Premium Diet Patch ("diet patch") are deceptive. The Web sites and packaging of the diet patch made express claims that the diet patch would cause weight loss by suppressing appetite and boosting metabolism. The packaging represented that the
diet patch was a “weight loss formula,” and that using the diet patch would “safely stimulate your metabolism, causing your body to use and absorb food more efficiently and to burn fat rather than store it.” The two Web sites that the FTC utilized to purchase the product contained similar representations, describing the diet patch as “a highly effective weight loss patch.”

The evidence presented at the hearing showed that these representations were false. In sum, Dr. Jensen testified that there is no scientific evidence relied upon by the medical community that would suggest that the diet patch the defendants sold or advertised on the two Web sites would cause any weight loss, increase metabolism, or decrease appetite. The evidence submitted by the defendants to the contrary does not detract from Dr. Jensen’s conclusions, and certainly does not provide substantiation for the defendants’ contention that the diet patch representations are not deceptive.

The defendants argue that the following disclaimer, present on the diet patch packaging, proves that it does not violate the FTC Act: “These statements have not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure or prevent any disease.” But this disclaimer does not address, much less deny, the representations regarding weight loss and therefore cannot cure the deceptive representations. FTC v. US Sales Corp., 785 F. Supp.737, 751 (N.D. Ill. 1992) (“Disclaimers or qualifications in any particular ad are not adequate to avoid liability unless they are sufficiently prominent and unambiguous to change the apparent meaning of the claims and to leave an accurate impression.”)

The main thrust of defendants’ opposition to liability under the FTC Act is the argument, without any citation to legal authority, that the FTC cannot be successful on the merits of its claims without providing evidence of a specific consumers being “defrauded” or harmed. The FTC has
made the required showing that the defendants’ claims are false, and therefore “deceptive” under the act. The FTC has also made the required showing that consumers relied upon these deceptive claims. “[O]nce the FTC shows (1) that a reasonably prudent person would rely on the deceptive advertisements, (2) that these advertisements were widely disseminated, and (3) that consumers purchased the product, ‘[t]he burden shifts to the defendants to prove that the representations were not relied upon by the consumers.’” FTC v. World Traveler Vacation Brokers, Inc., 861 F.2d 1020, 1029 (7th Cir. 1988)(citation omitted). The false representations about weight loss were disseminated over the Internet and the FTC has presented evidence establishing that the defendants purchased at least 800 diet patches in three separate orders over a six-month period. The fact that defendants continued to purchase diet patches leads to the conclusion that consumers were purchasing the diet patches – a conclusion buttressed by the bank records indicating numerous deposits into the defendants’ bank account from credit card processors.

Accordingly, this court rules that the FTC has demonstrated a better than negligible chance of success on the merits of its claims that representations on the Web sites countupandlookaway.com and keepyourmatehappy.biz, as well as on the packaging of the diet patch violate the FTC Act.

(ii) Violations of CAN-SPAM

On January 1, 2004, the Controlling the Assault of Non-solicited Pornography and Marketing Act of 2003 ("CAN-SPAM") went into effect. In this legislation, Congress made the finding that electronic mail had not only “become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis,” but that it also served an important role “for the development of frictionless commerce.” 15 U.S.C. § 7701(a)(1). These great benefits for society and economy are, however, “threatened by the extremely rapid growth in the volume of unsolicited
commercial electronic mail.” § 7701(a)(2). According to Congress, unsolicited commercial
electronic mail, or spam, “account[s] for over half of all electronic mail traffic, up from an estimated
7 percent in 2001.” § 7701(a)(2). The prevalence of spam significantly detracts from the efficiency
and convenience of electronic mail. See §§ 7701(a)(3), (a)(4), (a)(5), (a)(6). Congress specifically
listed what it considered to be the evils of spam: that its source and purpose for being sent are often
disguised, §§ 7701(a)(7), (a)(8); that senders of spam often do not provide its recipients with the
ability “to reject (or “opt-out” of) receipt” of the spam, § 7701(a)(9); and that senders of spam are
able “to gather large numbers of electronic mail address on an automated basis from Internet
websites . . . where users must post their addresses in order to make full use of the website or
service.” § 7701(a)(10).

Based upon these findings, Congress determined that:

(1) there is a substantial government interest in regulation of commercial electronic
mail on a nationwide basis;
(2) senders of commercial electronic mail should not mislead recipients as to the
source or content of such mail; and
(3) recipients of commercial electronic mail have a right to decline to receive
additional commercial electronic mail from the same source.

§ 7701(b). Finally, CAN-SPAM specifically notes that “[i]t is the sense of Congress that . . . Spam
has become the method of choice for those who distribute pornography, perpetrate fraudulent
schemes, and introduce viruses, worms, and Trojan horses into personal and business computer
systems.” § 7703(c).

In accordance with the preceding Congressional findings, CAN-SPAM imposes certain
requirements on those who “initiate the transmission of commercial electronic mail message[s].”
§ 7704(a)(1). Commercial e-mail messages must not contain materially false or misleading information regarding its source or deceptive subject headings. §§ 7704(a)(1), (a)(2). Commercial e-mail messages must contain: (1) a return email address or other "opt-out" mechanism that allows a recipient to voice his or her objection to further receipt, (2) a clear identification that it is a commercial advertisement or solicitation, (3) a clear notice of the ability to "opt-out," and (4) the sender's physical postal address. §§ 7704(a)(3), (a)(5). CAN-SPAM also makes it unlawful to send commercial e-mails to a recipient who has "opted-out." § 7704(a)(4). A violation of CAN-SPAM "shall be enforced by the [FTC] as if the violation . . . were an unfair or deceptive act or practice." § 7706(a)

There is no dispute that the e-mails in question violate CAN-SPAM. These e-mails, in fact, violate most, if not all, of CAN-SPAM's major provisions. Both of the technical experts testified at the preliminary injunction hearing that the e-mail messages marketing the two Web sites countupandlookaway.com and keepyourmatehappy.biz concealed the identity of the sender, violating section 7704(a)(1)'s requirement that e-mail messages shall not contain "header information that is materially false or materially misleading." Furthermore, the e-mails do contain neither a

5 "The term 'initiate,' when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message." 15 U.S.C. § 7702(9).

6 This requirement does not apply "if the recipient has given prior affirmative consent to receipt of the message." § 7704(a)(5)(B).

7 "The term 'header information' means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." § 7702(8).
conspicuous notice of the ability to “opt-out,” nor the sender’s physical postal address, nor a clear notice that the e-mails are commercial solicitations. All of these omissions violate CAN-SPAM. § 7704(a)(5)(A).

While defendants have not disputed that the e-mails violate CAN-SPAM, they have attempted to mount a constitutional challenge to CAN-SPAM itself. According to the defendants, CAN-SPAM “prohibits various e-mail messages which omit certain information, and accordingly, is a content-based Internet restriction, which is presumed invalid.” (Defs.’ Closing at 21.) Defendants support this conclusory statement with a quote from the Supreme Court’s recent decision in Ashcroft v. American Civil Liberties Union, 124 S.Ct. 2783 (2004), in which the Supreme Court held that the Child Online Protection Act (“COPA”), 47 U.S.C. § 231, was an invalid content based restriction. This court will only consider the single constitutional argument raised by defendants. Defendants contention that a prohibition on e-mails omitting certain information – or a requirement of disclosures – amounts to content-based restrictions on speech is rejected because it “overlooks material differences between disclosure requirements and outright prohibitions on speech.” Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio, 471 U.S. 626, 105 S.Ct. 2265, 2281 (1985). In short, requiring disclosure of information does not amount to a content-based restriction. See Id. Accordingly, defendants constitutional claim fails.

B. Defendants’ Responsibility for Violations of the FTC Act and CAN-SPAM

In the Finding of Facts section, the court has laid out in detail the evidence the FTC has presented to tie the defendants to the deceptive practices and violations of CAN-SPAM. The evidence connects the defendants to the entities selling the diet patches from the two Web sites countupandlookaway.com and keepyourmatehappy.biz and also establishes that the money spent
purchasing the diet patches ended up in the defendants' possession.

Phoenix Avatar, LLC was listed by MyPaySystems as the vendor selling diet patches from countupandlookaway.com, and AIT Herbal Marketing was listed on the invoice from this purchase, and AIT Herbal Marketing appeared on the FTC’s credit card statement for the second purchase. Thus, the evidence establishes that Phoenix Avatar, LLC, and AIT Herbal Marketing were selling the diet patches marketed on the Web sites countupandlookaway.com and keepyourmatehappy.biz.

The fact that these entities used these Web sites to sell their products establishes that they are likely responsible for the content of the Web sites. Similarly, the entities are likely responsible for the offending spam, which functioned as advertisements for the Web sites. The offending spam contained hyperlinks to these Web sites and also contained advertisements such as “Amazing patch makes you shed the pounds!” which directed recipients of the spam to the Web sites. (PX 4, Att. L, M.) Accordingly, it is quite likely that the entities utilizing the Web sites to sell diet patches initiated the transmission of the spam advertising the Web sites.

This conclusion is not undermined by the absence of technical evidence tracing the spam in this case back to its source. Both experts testified to the difficulties of determining the source of spam, due to the fact that those who send spam go to great lengths to hide their identities. And both experts testified that the e-mails in this case contain misleading information inserted for the purpose of obfuscating their true source. The FTC’s expert also testified that no technical method existed to determine the source of the e-mails because of the use of open proxies. Technical evidence connecting a person or an entity to spam would certainly be persuasive. However, it is not necessary to prove a violation of CAN-SPAM, as the definition of “initiate” in CAN-SPAM makes clear. Liability is not limited to those who physically cause spam to be transmitted, but also extends to
those who "procure the origination" of offending spam. 15 U.S.C. § 7702(9). The technical evidence attested to by defendants' expert Howell could not establish who "procure[d] the origination" of spam. Therefore, the statute necessarily contemplates the use of non-technical evidence to prove the source of offending spam.

Finally, the evidence connects the defendants to these two entities that are likely responsible for the deceptive practices and CAN-SPAM violations described above. Defendant James Lin, utilizing his bank account 884282030 jointly controlled with defendants Daniel Lin and Mark Sadek, paid the fee required to form Phoenix Avatar, LLC. The record also establishes that defendant Christopher Chung registered the Fictitious Business Name AIT Herbal Marketing, which was listed on the invoice the FTC received from its first undercover purchase. AIT Herbal Marketing, through M. Sadek, applied for the P.O. Box 251570, from which both undercover purchases were shipped. The FTC's undercover credit card was billed by AIT Herbal Marketing for the second undercover purchase. The evidence establishes that credits to AIT Herbal Marketing's merchant account with a credit card processor were deposited into bank account 884282030. The FTC has shown that the defendants are likely the individuals acting through the entities Phoenix Avatar, LLC and AIT Herbal Marketing.

At this stage of the litigation, the court is also not swayed by defendants' mere assertion that the FTC has failed to offer evidence of the defendants' "actual knowledge and/or participation in what the FTC claims to be deceptive acts and practices." (Defs.' Closing at 18.) See FTC v. Amy Travel Service, Inc., 875 F.2d 564, 573-74 (7th Cir. 1989). This standard applies when determining which individuals to hold liable after corporate liability is established. Id. However, AIT Herbal Marketing, the entity purporting to sell both diet patches is not a corporation. It is simply a fictitious
business name, and the evidence introduced by the FTC shows that the individuals using and
profiting from this name are the defendants. Finally, the FTC has shown the defendants "active
involvement in [the] business affairs" of Phoenix Avatar, LLC, which is "probative of [their]
knowledge" of that company's deceptive acts and practices. Id. at 574.

Accordingly, this court finds that the FTC has a better than negligible chance of success in
showing that the individual defendants are responsible for the violations of the FTC Act and CAN-
SPAM.

II. Balancing The Equities

As this court has explained, under the "public interest" test, public interests are given far
greater weight than private equities, which is not to say though that private equities should not be
considered, especially where the defendant may face irreparable injury. See FTC v. Elders Grain,
Inc., 868 F.2d 901, 903 (7th Cir. 1989). The defendants contend that the public equities in this case
are low or nonexistent because the FTC has failed to produce evidence of consumers complaining
of harm from the defendants' practices. This court disagrees. The public has an important interest
in a violation of the law. The public would be harmed by continued violations of the law. The FTC
has shown a high likelihood success on its claim that the defendants have violated both the FTC Act
and CAN-SPAM. Accordingly, the public interest in this case is great. Id. (Ripple, J. concurring)
("A strong showing by the government that a violation of law has occurred necessarily produces
'public equities' that must 'receive far greater weight' than 'private equities.'").

Furthermore, despite defendants' argument to the contrary, the FTC has shown a concrete
harm to individual members of the public. The FTC has shown (1) that it is likely that the
defendants are misrepresenting the effects of their product to the public and (2) that the defendants
Ticketmaster Corp. v. Tickets.com, Inc.
United States District Court for the Central District of California
2003 U.S. Dist. LEXIS 6483
March 6, 2003, Decided
March 7, 2003, Filed

This motion by defendant Tickets.com, Inc. (hereafter TX) for summary judgment on plaintiffs Ticketmaster Corporation and Ticket Online-CitySearch, Inc. (hereafter collectively TM), intellectual property issues is denied as to the contract claim of TM and granted as to the copyright and trespass to chattels claims, which are dismissed by this minute order.

At this point in the case, both parties have narrowed their claims. TM, the original plaintiff, has narrowed its intellectual property claims to a contract theory, a copyright theory, and a trespass to chattels theory. The court finds triable issues of fact on the contract theory and finds no triable issues of fact and grants summary judgment on the copyright and trespass to chattels claims.

Many of the factual items are not contested, although the legal result of applying the law to the uncontested facts is heavily contested. Among the uncontested facts are the following: Both TM and TX are in the business of selling tickets to all kinds of “events” (sports, concerts, plays, etc.) to the public. They are in heavy competition with one another, but operate in distinctive ways. TM is the largest company in the industry. It sells tickets by the four methods of ticket selling—venue box office, retail outlets, by telephone, and over the internet. Telephone and internet sales require the customer to establish credit with the ticket seller (usually by credit card). Internet sales have been the fastest growing segment of the industry. TX at the time of the events considered in this motion was primarily (but not exclusively) an internet seller. Both TM and TX maintain a web page reachable by anyone with an internet connection. Each of their web pages has many subsidiary (or interior) web pages which describe one event each and provide such basic information as to location, date, time, description of the event, and ticket prices. The TM interior web pages each have a separate electronic address or Uniform Resource Locator (“URL”) which, if possessed by the internet user, allows the user to reach the web page for any particular event by by-passing the “home” web page and proceeding past the index to reach the interior web page for the event in question. The TM interior web pages provide telephone numbers for customers or allow the customer to order tickets to the event by interactive computer use. A charge is made for the TM service.

TM principally does business by exclusive contracts with the event providers or their producers, and its web pages only list the events for which TM is the exclusive ticket seller. TX also sells tickets to a number of events for which it is the ticket seller. At one point, its web pages attempted to list all events for which tickets were available whether or not TX sold the tickets. Its interior web pages also listed the event, the date, time, ticket prices, and provided for internet purchase if TX could sell the tickets. When TX could not sell the tickets, it listed ticket brokers who sold at premium prices. In early 2000, TX discontinued this practice of listing events with tickets sold by other ticket brokers. Until early 2000, in situations where TM was the only source of tickets, TX provided a “deep link” by which the customer would be transferred to the interior web page of TM’s web site, where the customer could purchase the ticket from TM. This process
of “deep linking” is the subject of TM’s complaint in this action, of which there is now left the contract, copyright, and trespass theories.

Starting in 1998 and continuing to July 2001, when it stopped the practice, TX employed an electronic program called a “spider” or “crawler” to review the internal web pages (available to the public) of TM. The “spider” “crawled” through the internal web pages to TM and electronically extracted the electronic information from which the web page is shown on the user’s computer. The spider temporarily loaded this electronic information into the Random Access Memory (“RAM”) of TX’s computers for a period of from 10-15 seconds. TX then extracted the factual information (event, date, time, tickets prices, and URL) and discarded the rest (which consisted of TM identification, logos, ads, and other information which TX did not intend to use; much of this discarded material was protected by copyright). The factual information was then organized in the TX format to be displayed on the TX internal web page. The TX internal web page carried no TM identification and had only the factual information about the event on it which was taken from TM’s interior web page but rearranged in TX format plus any information or advertisement added by TX. From March 1998, to early 2000, the TX user was provided the deep linking option described above to go directly from the TX web site to the relevant TM interior web page. This option stopped (or was stopped by TM) in early 2000. For an unknown period afterward, the TX customer was given the option of linking to the TM home page, from which the customer could work his way to the interior web page in which he was interested. (The record does not reveal whether this practice still exists or whether TM objects to it.) Thus, the intellectual property issues in this case appear to be limited to events which occurred between November 1998, when spidering started, and July 2001, when it stopped. The “deep linking” aspect of the case is relevant only from March 1998, to early 2000, when it stopped.

The contract aspect of the case derives from a notice placed on the home page of the TM web site which states that anyone going beyond that point into the interior web pages of the web site accepts certain conditions, which include, relevant to this case, that all information obtained from the website is for the personal use of the user and may not be used for commercial purposes. Earlier in this case (and at the time of the motion for preliminary injunction) the notice was placed at the bottom of the home page of the TM web site, so that a user without an especially large screen would have to scroll down the page to read the conditions of use. Since then, TM has placed in a prominent place on the home page the warning that proceeding further binds the user to the conditions of use. As one TX executive put it, it could not be missed. At the time of the preliminary injunction motion, the court commented that there was no evidence that the conditions of use were known to TX. Since then, there has been developed evidence that TX was fully familiar with the conditions TM claimed to impose on users, including a letter from TM to TX which quoted the conditions (and a reply by TX stating that it did not accept the conditions). Thus, there is sufficient evidence to defeat summary judgment on the contract theory if knowledge of the asserted conditions of use was had by TX, who nevertheless continued to send its spider into the TM interior web pages, and if it is legally concluded that doing so can lead to a binding contract. For reasons dealing with the desirability of clear unmistakable evidence of assent to the conditions on trial of such issues, the court would prefer a rule that required an unmistakable assent to the conditions easily provided by requiring clicking on an icon which says “I agree” or the equivalent. Such a rule would provide certainty in trial and make it clear
that the user had called to his attention the conditions he or she accepted when using the website. (The court notes that Professor Lemley also approves this approach, but this is treated as a legal opinion, not a fact). However, the law has not developed this way. Use of a cruise ship ticket with a venue provision printed on the back commits one to the venue provided. (Carnival Cruise Lines v. Shute (‘91), 499 U.S. 585, 113 L. Ed. 2d 622, 111 S. Ct. 1522.) The Carriage of Goods by Sea Act, the Carmack Act, and the Warsaw Convention provide that limitations of liability on the bill of lading, air waybill, or airplane ticket are enforceable if the services are used by the customer. The “shrinkwrap” cases find the printed conditions plainly wrapped around the cassette or CD enforceable. Even the back of your parking lot ticket may be enforceable. The principle has been applied to cases similar to this. (Register.com, Inc. v. Verio, Inc. (SDNY’00) 126 FSupp2d 238; Pollstar v. Gigmania Ltd. (EDCA’00) 170 FSupp2d 974.) The principle has long been established that no particular form of words is necessary to indicate assent—the offeror may specify that a certain action in connection with his offer is deemed acceptance, and ripens into a contract when the action is taken. (Binder v. Aetna Life Ins. Co. (’99) 75 Cal. App. 4th 832, 89 Cal. Rptr. 2d 540; Penn Sec. Life Ins. Co. v. Rising 62 CA3d 302, 133 Cal. Rptr. 59.) Thus, as relevant here, a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so. In Specht v. Netscape Communs. Corp. (2Cir’02) 306 F.3d 17, the court found that there was no mutual assent when a notice of the existence of license terms governing the use of software was visible to internet users only if they scrolled down the screen. That case is distinguishable from the facts at hand on the grounds that in Specht, the plaintiff’s terms of use were not plainly visible or known to defendants. See id. at 31. Moreover, Specht involved a different set of circumstances, that of consumers invited to download free software from an internet site that did not contain a plainly visible notice of license terms. See id. at 32. As a result, the TX motion for summary judgment on the contract issue is denied.

The trespass to chattels issue requires adapting the ancient common law action to the modern age. No cases seem to have reached the appellate courts although there appears to be a number of district court cases. One case (Intel Corp. v. Hamadi (‘01) 94 Cal. App. 4th 325, 114 Cal. Rptr. 2d 244) is pending in the California Supreme Court since it granted a hearing which has the effect of vacating the state Court of Appeal opinion (and which has no precedent value once the hearing was granted). The court is informed that the eBay, Inc. v. Bidder’s Edge, Inc. (NDCA’00) 100 F. Supp. 2d 1058 preliminary injunction was not appealed. At the time of the preliminary injunction motion, only the eBay case was before the court. Since then, there have been a number of district court cases discussing the chattel theory (some published and some not). These cases tend to support the proposition that mere invasion or use of a portion of the web site by a spider is a trespass (leading at least to nominal damages), and that there need not be an independent showing of direct harm either to the chattel (unlikely in the case of a spider) or tangible interference with the use of the computer being invaded. However, scholars and practitioners alike have criticized the extension of the trespass to chattels doctrine to the internet context, noting that this doctrinal expansion threatens basic internet functions (i.e., search engines) and exposes the flaws inherent in applying doctrines based in real and tangible property to cyberspace. See, Laura Quilter, Cyberlaw: The Continuing Expansion of Cyberspace Trespass to Chattels, 17 Berkeley Tech. L. J. 421 (2002); Clifton Merrell, Trespass to Chattels in the Age of the Internet, 80 Wash. U. L. Q. 675 (2002); Mary Anne Bendotoff and Elizabeth R. Gosse, “Stay Off My Cyberproperty!”: Trespass to Chattels on the Internet (2001), 6 Intell. Prop. L.
Bull. 12; Edward Lee, Rules and Standards for Cyberspace, 77 Notre Dame L. Rev. 1275, 1283-1284 (2002). Pending appellate guidance, this court comes down on the side of requiring some tangible interference with the use or operation of the computer being invaded by the spider. Restatement (Second) of Torts § 219 requires a showing that “the chattel is impaired as to its condition, quality, or value.” Therefore, unless there is actual dispossessing of the chattel for a substantial time (not present here), the elements of the tort have not been made out. Since the spider does not cause physical injury to the chattel, there must be some evidence that the use or utility of the computer (or computer network) being “spiderized” is adversely affected by the use of the spider. No such evidence is presented here. This court respectfully disagrees with other district courts’ finding that mere use of a spider to enter a publically available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.

TM complains that the information obtained by the use of the spider was valuable (and even that it was sold by TX), and that it spent time and money attempting to frustrate the spider, but neither of these items shows damage to the computers or their operation. One must keep in mind that we are talking about the common law tort of trespass, not damage from breach of contract or copyright infringement. The tort claim may not succeed without proof of tort-type damage. Plaintiff TM has the burden to show such damage. None is shown here. The motion for summary judgment is granted to eliminate the claim for trespass to chattels. This minute order is the order eliminating that claim. This approach to the tort of trespass to chattels should hurt no one’s policy feelings; after all, what is being attempted is to apply a medieval common law concept in an entirely new situation which should be disposed of by modern law designed to protect intellectual property interests.

The copyright issues are more difficult. They divide into three issues. The first is whether the momentary resting in the TX computers of all of the electronic signals which are used to form the video representation to the viewer of the interior web pages of the TX computer constitutes actionable copyright infringement. The second is whether the URLs, which were copied and used by TX, contain copyrightable material. The third is whether TX’s deeplinking caused the unauthorized public display of TM event pages. In examining these questions, we must keep in mind a prime theorem of copyright law--facts, as such, are not subject to copyright protection. What is subject to copyright protection is the manner or mode of expression of those facts. Thus, addresses and telephone numbers contained in a directory do not have copyright protection (Feist Publications v. Rural Tel. Serv. Co., 499 U.S. 340, 113 L. Ed. 2d 358, 111 S. Ct. 1282), despite the fact that time, money, and effort went into compiling the information. Similarly, in this case, the existence of the event, its date and time, and its ticket prices, are not subject to copyright. Anyone is free to print (or show on the internet) such information. Thus, if TX had sat down a secretary at the computer screen with instructions manually to go through TM’s web sites and pick out and write down purely factual information about the events, and then feed it into the TX web pages (using the TX distinctive format only), no one could complain. The objection is that the same thing was done with an electronic program. However, the difference is that the spider picks up all of the electronic symbols which, if it had been put on a monitor with the right software, would duplicate the TM web page. However, this is not the way it was done. The spider picks up the electronic symbols and loads them momentarily (for 10 to 15 seconds) into the RAM of the TX computers, where a program picks up the factual data (not protected), places same into the TX format for its web pages, and immediately discards the balance, which may
consist of TM logos, TM advertisements, TM format for presentation of the material, and other material which is copyrightable. Thus, the actual copying (if it can be called that) is momentary while the non-protected material, all open to the public, is extracted. Is this momentary resting of the electronic symbols from which a TM web page could be (but is not) constructed fair use where the purpose is to obtain nonprotected facts? The court thinks the answer is “yes”. There is not much law in point. However, there are two Ninth Circuit cases which shed light on the problem. They are Sony Computer Entm’t, Inc. v. Connectix Corp. (9Cir’00) 203 F3d 596 and Sega Enters. v. Accolade, Inc. (9Cir’92) 977 F2d 1510. In each of these cases, the alleged infringer attempted to get at non-protected source code by reverse engineering of the plaintiff’s copyrighted software. In doing so, the necessary method was to copy the software and work backwards to derive the unprotected source code. The copied software was then destroyed. In each case, this was held to be fair use since it was necessary to temporarily copy the software to obtain the non-protected material. There may be a difference with this case, however; at least TM claims so. It asserts in its points and authorities that taking the temporary copy in this case was not the only way to obtain the unprotected information, and that TX was able to, and in actuality did purchase such information from certain third-parties. Both Sony and Sega stated that the fair use was justified because reverse engineering (including taking a temporary copy) was the only way the unprotected information could be obtained. Although this court recognizes that the holdings of Sony and Sega were limited to the specific context of “disassembling” copyrighted object code in order to access unprotected elements contained in the source code, this court believes that the “fair use” doctrine can be applied to the current facts.

Taking the temporary copy of the electronic information for the limited purpose of extracting unprotected public facts leads to the conclusion that the temporary use of the electronic signals was “fair use” and not actionable. In determining whether a challenged use of copyrighted material is fair, a court must keep in mind the public policy underlying the Copyright Act: to secure a fair return for an author’s creative labor and to stimulate artistic creativity for the general good. This court sees no public policy that would be served by restricting TX from using spiders to temporarily download TM’s event pages in order to acquire the unprotected, publicly available factual event information. The rest of the event page information (which consisted of TM identification, logos, ads, and other information) was discarded and not used by TX and is not exposed to the public by TX. In temporarily downloading TM’s event pages to its RAM through the use of spiders, TX was not exploiting TM’S creative labors in any way: its spiders gathered copyrightable and non-copyrightable information alike but then immediately discarded the copyrighted material. It is unlikely that the spiders could have been programmed to take only the factual information from the TM web pages without initially downloading the entire page.

Consideration of the fair use factors listed in 17 USC § 106 supports this result. First, TX operates its site for commercial purposes, and this fact tends to weigh against a finding of fair use. Campbell v. Acuff-Rose Music (‘94), 510 U.S. 569 at 585, 127 L. Ed. 2d 500 at 519, 114 S. Ct. 1164. TX’s use of the data gathered from TM’s event pages was only slightly transformative. As for the second factor, the nature of the copyrighted work, the copying that occurred when spiders download the event page, access the source code for each page, and extract the factual data embedded in the code, is analogous to the process of copying that the Sony court condemned (however, the Court recognizes that the fair use holding from that decision does not fit perfectly onto the facts at hand). Third, because TX’s final product—the TX web site—did not contain any
infringing material, the “amount and substantiality of the portion used” is of little weight. Connectix (9Cir’00) 203F3d at 606 (quoting Sega(9Cir’93) 977 F2d at 1526-1537). The fourth factor (the effect on the market value of the copyrighted work) is, of course nil, and weighs towards finding fair use. TM’s arguments and evidence regarding loss of advertising revenue, as well as the loss of potential business with Volt Delta, are not persuasive.

The second copyright problem is whether the URLs (Uniform Resource Locator) are subject to copyright protection. The URLs are copied by TX and, while TX was deep hyper-linking to TM interior web pages, were used by TX to allow the deep-linking (by providing the electronic address of the particular relevant TM interior web page). This electronic address is kept in TX’s computer (not provided to the customer) but was used to connect the customer to the TM interior web page when the customer pushed the button to be transferred to the web page of the broker who sells the tickets. In fact, anyone who uses the TM interior web page-TM customer or not--uses the URL to get there, although sometimes through another computer which also has the URL. TM contends that, although the URLs are strictly functional, they are entitled to copyright protection because there are several ways to write the URL, and, thus, original authorship is used. The court disagrees. A URL is simply an address, open to the public, like the street address of a building, which, if known, can enable the user to reach the building. There is nothing sufficiently original to make the URL a copyrightable item, especially the way it is used. Feist Publications (’91), 499 U.S. 340, 113 L. Ed. 2d 358 at 369, 111 S. Ct. 1282. There appear to be no cases holding the URLs to be subject to copyright. On principle, they should not be.

The third copyright problem is whether TX’s deep linking caused the unauthorized public display of TM event pages in violation of TM’s exclusive rights of reproduction and display under 17 U.S.C. § 106. The Ninth Circuit in Kelly v. Arriba Soft Corp. (9Cir’02) 280 F3d 934, recognized that inline linking and framing of full-sized images of plaintiff’s copyrighted photographs within the defendant’s web site violated the plaintiff’s public display rights. In that case, defendant’s web site contained links to plaintiff’s photographs (which were on plaintiff’s publicly available website). Users were able to view plaintiff’s photographs within the context of defendant’s site: Plaintiff’s images were “framed” by the defendant’s window, and were thus surrounded by defendant web page’s text and advertising. In one short paragraph in a declaration offered on the preliminary injunction motion, TM alleges that when a user was deep-linked from the TX site to a TM event page, a smaller window was opened. The smaller window was described as containing a page from the TM web site which was “framed” by the larger window. At the time of the preliminary injunction motion, TX stated that whether “framing” occurs or not depends on the settings on the user’s computer, over which TX has no control. Thus, framing occurred on some occasions but not on others. However, TX says that it “did not try to disguise a sale by use of frames occurring on the Tickets.com website.” (Reply, p. 10) TX further states that when users were linked to TM web pages, the TM event pages were clearly identified as belonging to TM.

However, even if the TM interior web site page was “framed” within the TX web page, this case is distinguishable from Kelly. In Kelly, the defendant’s site would display a variety of “thumbnail” images as a result of the user’s search. By clicking on the desired thumbnail image, a user could view the “Images Attributes” page, which displayed the original full-size image, a description of its dimensions, a link to the originating web site, and defendant’s banner and
advertising. The full-size image was not technically located on defendant’s web site, but was taken directly from the originating web site. However, only the image itself, and not any other part of the originating web site, was displayed on the “Images Attributes” page. The Ninth Circuit determined that by importing plaintiff’s images into its own web page, and by showing them in the context of its own site, defendant infringed upon plaintiff’s exclusive public display right.

In this case, a user on the TX site was taken directly to the originating TM site, containing all the elements of that particular TM event page. Each TM event page clearly identified itself as belonging to TM. Moreover, the link on the TX site to the TM event page contained the following notice: “Buy this ticket from another online ticketing company. Click here to buy tickets. 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.” (2d Am. Compl. Ex.1) (emphasis in original) Even if the TM site may have been displayed as a smaller window that was literally “framed” by the larger TX window, it is not clear that, as matter of law, the linking to TX event pages would constitute a showing or public display in violation of 17 U.S.C. § 106(5). Accordingly, summary judgment is granted on the copyright claims of TM and it is eliminated from this action.
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

PLAYBOY ENTERPRISES, INC.,
Plaintiff-Appellant,
v.
NETSCAPE COMMUNICATIONS
CORPORATION,
Defendant-Appellee.

No. 00-56648
D.C. No.
CV-99-00320-AHS

PLAYBOY ENTERPRISES
INTERNATIONAL, INC.,
Plaintiff-Appellant,
v.
EXCITE, INC.,
Defendant-Appellee.

No. 00-56662
D.C. No.
CV-99-00321-AHS-02
OPINION

Appeal from the United States District Court
for the Central District of California
Alicemarie H. Stotler, District Judge, Presiding

Argued and Submitted
September 11, 2001—Pasadena, California

Filed January 14, 2004

Before: Betty B. Fletcher, Thomas G. Nelson, and
Marsha S. Berzon, Circuit Judges.

Opinion by Judge Thomas G. Nelson;
Concurrence by Judge Berzon

359
COUNSEL

Barry G. Felder, Brown Raysman Millstein Felder & Steiner LLP, Los Angeles, California, for the plaintiff-appellant.

Jeffrey K. Riffer, Jeffer, Mangels, Butler & Marmaro LLP, Los Angeles, California, for the defendants-appellees.

OPINION

T.G. NELSON, Circuit Judge:

Playboy Enterprises International, Inc. (PEI) appeals from the district court’s grant of summary judgment in favor of Netscape Communications Corporation and Excite, Inc. PEI sued defendants for trademark infringement and dilution. We have jurisdiction pursuant to 28 U.S.C. § 1291. Because we conclude that genuine issues of material fact preclude summary judgment on both the trademark infringement and dilution claims, we reverse and remand.

I. FACTS

This case involves a practice called “keying” that defendants use on their Internet search engines. Keying allows advertisers to target individuals with certain interests by linking advertisements to pre-identified terms. To take an innocuous example, a person who searches for a term related to gardening may be a likely customer for a company selling seeds. Thus, a seed company might pay to have its advertisement displayed when searchers enter terms related to gardening. After paying a fee to defendants, that company could
have its advertisements appear on the page listing the search results for gardening-related terms: the ad would be "keyed" to gardening-related terms. Advertisements appearing on search result pages are called "banner ads" because they run along the top or side of a page much like a banner.¹

Defendants have various lists of terms to which they key advertisers' banner ads. Those lists include the one at issue in this case, a list containing terms related to sex and adult-oriented entertainment. Among the over-400 terms in this list are two for which PEI holds trademarks: "playboy" and "playmate."² Defendants require adult-oriented companies to link their ads to this set of words. Thus, when a user types in "playboy," "playmate," or one of the other listed terms, those companies' banner ads appear on the search results page.³

PEI introduced evidence that the adult-oriented banner ads displayed on defendants' search results pages are often graphic in nature and are confusingly labeled or not labeled at all. In addition, the parties do not dispute that buttons on the banner ads say "click here." When a searcher complies, the search results page disappears, and the searcher finds him or herself at the advertiser's website. PEI presented uncontested evidence that defendants monitor "click rates," the ratio between the number of times searchers click on banner ads and the number of times the ads are shown. Defendants

¹Not all banner ads are keyed. Some advertisers buy space for their banner ads but only pay to have their ads displayed randomly. Such ads cost less because they are un-targeted and are therefore considered less effective.

²The other terms are generally un-trademarked words associated with adult entertainment, ranging from the expected (sex, parts of the human anatomy, etc.) to the disturbing (gangbangers).

³The search results page lists websites relevant to the search terms pursuant to the search engine's computer program. A user can click on any item in the list to link to the website of the organization listed. Defendants' search results pages for the terms "playboy" and "playmate" include links to PEI's websites.
use click rate statistics to convince advertisers to renew their keyword contracts. The higher the click rate, the more successful they deem a banner ad.

PEI sued defendants, asserting that they were using PEI’s marks in a manner that infringed upon and diluted them. The district court denied PEI’s request for a preliminary injunction, and this court affirmed in an unpublished disposition. On remand, the parties filed cross-motions for summary judgment. The district court granted summary judgment in favor of defendants. We reverse.

II. STANDARD OF REVIEW

We review the district court’s grant of summary judgment de novo. Viewing the evidence in the light most favorable to PEI, and drawing all reasonable inferences in PEI’s favor, we must determine whether there are any genuine issues of material fact and whether the district court correctly applied the relevant substantive law. The moving party — in this case, the defendants — bears the “initial burden of identifying for the court the portions of the materials on file that it believes demonstrate the absence of any genuine issue of material fact.” If the moving party meets its initial burden, the burden shifts to the non-moving party to “set forth, by affidavit or as otherwise provided by Rule 56, ‘specific facts showing that there is a genuine issue for trial.’”

4Playboy Enters., Inc. v. Netscape Communications Corp., 55 F. Supp. 2d 1070 (C.D. Cal.), aff’d, 202 F.3d 278 (9th Cir. 1999).

5Lopez v. Smith, 203 F.3d 1122, 1131 (9th Cir. 2000).

6Id.


8Id. (quoting Fed. R. Civ. P. 56(e)).
or determine the truth of the matter but may only determine whether there is a genuine issue for trial.

III. DISCUSSION

A. Trademark Infringement

With regard to PEI’s trademark infringement claim, the parties disagree on three points. First, the parties dispute whether a direct or a contributory theory of liability applies to defendants’ actions. We conclude that defendants are potentially liable under one theory and that we need not decide which one. Second, the parties disagree regarding whether PEI has successfully shown that a genuine issue of material fact exists regarding the likelihood of consumer confusion resulting from defendants’ use of PEI’s marks. We conclude that a genuine issue of material fact does exist. Finally, the parties dispute whether any affirmative defenses apply. We conclude that no defenses apply. We will address each dispute in turn.

1. Theory of liability.

Whether the defendants are directly or merely contributorily liable proves to be a tricky question. However, we need not decide that question here. We conclude that defendants are either directly or contributorily liable. Under either theory, PEI’s case may proceed. Thus, we need not decide this issue.

2. PEI’s case for trademark infringement.

[1] The “core element of trademark infringement,” the likelihood of confusion, lies at the center of this case.¹⁰ No dis-

¹⁰Brookfield Communications, Inc. v. West Coast Entm’t Corp., 174 F.3d 1036, 1053 (9th Cir. 1999). Because California trademark law claims are “substantially congruent,” we do not examine them separately in this opinion, just as the district court did not. Denbicare U.S.A. Inc. v. Toys “R” Us, Inc., 84 F.3d 1143, 1152 (9th Cir. 1996) (internal quotation marks omitted).
pute exists regarding the other requirements set forth by the statute: PEI clearly holds the marks in question and defendants used the marks in commerce\textsuperscript{11} without PEI's permission.\textsuperscript{12}

[2] PEI's strongest argument for a likelihood of confusion is for a certain kind of confusion: initial interest confusion.\textsuperscript{13} Initial interest confusion is customer confusion that creates initial interest in a competitor's product.\textsuperscript{14} Although dispelled before an actual sale occurs, initial interest confusion impossibly capitalizes on the goodwill associated with a mark and is therefore actionable trademark infringement.\textsuperscript{15}

[3] PEI asserts that, by keying adult-oriented advertisements to PEI's trademarks, defendants actively create initial interest confusion in the following manner. Because banner advertisements appear immediately after users type in PEI's marks, PEI asserts that users are likely to be confused regarding the sponsorship of unlabeled banner advertisements.\textsuperscript{16} In addition, many of the advertisements instruct users to "click

\textsuperscript{11} Federal jurisdiction over trademark cases rests on the Commerce Clause, sweeps as broadly as possible, and clearly encompasses the circumstances of this case. 15 U.S.C. § 1127 (defining "commerce" for jurisdictional purposes as "all commerce which may lawfully be regulated by Congress"); see Steele v. Bulova Watch Co., 344 U.S. 280, 283-84 (1952). In addition to defining "commerce," 15 U.S.C. § 1127 also defines "use in commerce." 15 U.S.C. § 1127. That latter definition applies to the required use a plaintiff must make in order to have rights in a mark, as defined by 15 U.S.C. § 1051. See Planetary Motion, Inc. v. Techsplosion, Inc., 261 F.3d 1188, 1194-95 (11th Cir. 2001). It does not enter into our jurisdictional analysis.

\textsuperscript{12} 15 U.S.C. § 1114(1)(a).

\textsuperscript{13} Indeed, we find insufficient evidence to defeat summary judgment on any other theory.

\textsuperscript{14} Brookfield, 174 F.3d at 1062-63.

\textsuperscript{15} Id. at 1057.

\textsuperscript{16} Note that if a banner advertisement clearly identified its source or, even better, overtly compared PEI products to the sponsor's own, no confusion would occur under PEI's theory.
here.” Because of their confusion, users may follow the instruction, believing they will be connected to a PEI site. Even if they realize “immediately upon accessing” the competitor’s site that they have reached a site “wholly unrelated to” PEI’s, the damage has been done: Through initial consumer confusion, the competitor “will still have gained a customer by appropriating the goodwill that [PEI] has developed in its [ ] mark.”

PEI’s theory strongly resembles the theory adopted by this court in *Brookfield Communications, Inc. v. West Coast Entertainment Corporation.* In *Brookfield,* a video rental company, West Coast Entertainment Corporation, planned on using “moviebuff.com” as a domain name for its website and using a similar term in the metatags for the site. Brookfield had trademarked the term “MovieBuff,” however, and sued West Coast for trademark infringement. The court ruled in favor of Brookfield. It reasoned that Internet users entering Brookfield’s mark (plus “.com”) or searching for Brookfield’s mark on search engines using metatags, would find themselves at West Coast’s website. Although they might “realize, immediately upon accessing 'moviebuff.com,' that they have reached a site operated by West Coast and wholly unrelated to Brookfield,” some customers who were originally seeking Brookfield’s website “may be perfectly content with West Coast’s database (especially as it is offered free of charge).” Because those customers would have found West Coast’s site due to West Coast’s “misappropriation of Brookfield’s goodwill” in its mark, the court concluded that Brookfield withstood summary judgment.

---

17 *Brookfield,* 174 F.3d at 1057.
18 174 F.3d 1036 (9th Cir. 1999).
19 *Id.* at 1042.
20 *Id.* at 1043.
21 *Id.* at 1057.
22 *Id.*
In this case, PEI claims that defendants, in conjunction with advertisers, have misappropriated the goodwill of PEI’s marks by leading Internet users to competitors’ websites just as West Coast video misappropriated the goodwill of Brookfield’s mark. Some consumers, initially seeking PEI’s sites, may initially believe that unlabeled banner advertisements are links to PEI’s sites or to sites affiliated with PEI. Once they follow the instructions to “click here,” and they access the site, they may well realize that they are not at a PEI-sponsored site. However, they may be perfectly happy to remain on the competitor’s site, just as the Brookfield court surmised that some searchers initially seeking Brookfield’s site would happily remain on West Coast’s site. The Internet user will have reached the site because of defendants’ use of PEI’s mark. Such use is actionable.\textsuperscript{23}

Although analogies to Brookfield suggest that PEI will be able to show a likelihood of confusion sufficient to defeat summary judgment, we must test PEI’s theory using this circuit’s well-established eight-factor test for the likelihood of confusion to be certain. Accordingly, we turn to that test now.

The Ninth Circuit employs an eight-factor test, originally set forth in AMF Inc. v. Sleekcraft Boats,\textsuperscript{24} to determine the likelihood of confusion. The eight factors are:

1. strength of the mark;
2. proximity of the goods;
3. similarity of the marks;
4. evidence of actual confusion;

\textsuperscript{23}Id. at 1062-65.
\textsuperscript{24}599 F.2d 341, 348-49 (9th Cir. 1979).
5. marketing channels used;

6. type of goods and the degree of care likely to be exercised by the purchaser;

7. defendant’s intent in selecting the mark; and

8. likelihood of expansion of the product lines.  

In the Internet context, courts must be flexible in applying the factors, as some may not apply. Moreover, some factors are more important than others. For example, a showing of actual confusion among significant numbers of consumers provides strong support for the likelihood of confusion. For that reason, we turn first to an examination of factor four: evidence of actual confusion.


The expert study PEI introduced establishes a strong likelihood of initial interest confusion among consumers. Thus, factor four alone probably suffices to reverse the grant of summary judgment.

PEI’s expert, Dr. Ford, concluded that a statistically significant number of Internet users searching for the terms “playboy” and “playmate” would think that PEI, or an affiliate, sponsored banner ads containing adult content that appear on the search results page. When study participants were shown

26 Id.
27 Brookfield, 174 F.3d at 1054. In this case, we conclude that only the final factor — the likelihood of expansion of product lines — does not apply.
28 Thane Int’l, Inc. v. Trek Bicycle Corp., 305 F.3d 894, 902 (9th Cir. 2002) (“Evidence of actual confusion constitutes persuasive proof that future confusion is likely. . . . If enough people have been actually confused, then a likelihood that people are confused is established.”) (internal quotation marks omitted).
search results for the term "playboy," 51% believed that PEI sponsored or was otherwise associated with the adult-content banner ad displayed. When shown results for the term "playmate," 31% held the same belief. Using control groups, Dr. Ford also concluded that for 29% of those participants viewing "playboy" searches and 22% of those viewing "playmate" searches, the confusion stemmed from the targeting of the banner advertisements. The individuals were not confused by random, un-targeted advertisements.

Defendants criticize Dr. Ford’s procedures and conclusions. They offer their own interpretations of his data, with significantly lower rates of confusion. Defendants cite cases identifying probabilities of confusion of 7.6% and less as de minimis and then argue that Dr. Ford’s results showed de minimis confusion as well. Their critique of Dr. Ford’s methods and interpretations formed the basis of a motion to exclude his expert testimony and report before the district court. The district court denied that motion, however, and allowed the introduction of the evidence.

Defendants may have valid criticism of Dr. Ford’s methods and conclusions, and their critique may justify reducing the weight eventually afforded Dr. Ford’s expert report. The district court’s evidentiary ruling is not before us on appeal, however, and weighing admissible evidence at this stage is improper. Defendants’ arguments prove the point that a genuine issue of material fact exists regarding actual confusion. The presence of Dr. Ford’s criticized (but uncontradicted) report, with its strong conclusions that a high likelihood of initial interest confusion exists among consumers, thus generates a genuine issue of material fact on the actual confusion issue.

28Surveys are commonly introduced as probative evidence of actual confusion. See Schering Corp. v. Pfizer Inc., 189 F.3d 218, 225 (2d Cir. 1999).

29Abdul-Jabbar, 85 F.3d at 410.
Because actual confusion is at the heart of the likelihood of confusion analysis, Dr. Ford's report alone probably precludes summary judgment. In the interest of being thorough, however, we will examine the other seven Sleekcraft factors. On balance, they also support PEI.

b. *Factor One: Strength of the Mark.*

PEI has established that strong secondary meanings for its descriptive marks exist, and that a genuine issue of material fact exists as to whether it created the secondary meanings. Thus, the first Sleekcraft factor favors PEI.

At this point, defendants concede that they use the marks for their secondary meanings. Thus, they concede that the marks have secondary meanings. They offer only a weak argument regarding the strength of the meanings. Given that

---

30 Thane, 305 F.3d at 902.

31 Sleekcraft, 599 F.2d at 349 n. 12 (noting that, once a party establishes that it has created secondary meaning, "the protection afforded should be commensurate with the degree of consumer association proven").

32 Indeed, to argue that they use the marks for their primary meaning, as defendants did below, is absurd. Defendants obviously do not use the term "playmate," for example, for its dictionary definition: "a companion, especially of a child, in games and play." WEBSTER'S NEW WORLD DICTIONARY, 3d coll. ed. (1988).

33 Defendants cite third-party use of the mark as evidence that the secondary meanings of PEI's marks are weak. However, as discussed in the dilution context in section III.B, the degree of third-party use is in dispute in this case, and we do not find their evidence helpful here. Although evidence of extensive third-party use of a mark may be useful in evaluating the strength of the secondary meaning of a mark, we note that such evidence can cut both ways. On the one hand, extensive third-party use of a mark might tend to show that consumers are likely to associate the mark with companies and meanings other than the markholder's. See, e.g., Amstar Corp. v. Domino's Pizza, Inc., 615 F.2d 252, 259-60 (5th Cir. 1980). However, if consumers associate the mark with the markholder, and the markholder's secondary meaning, despite extensive third-party use, the third-party uses would tend to show the strength of the association...
defendants themselves use the terms precisely because they believe that Internet searchers associate the terms with their secondary meanings, disputing the strength of the secondary meanings is somewhat farfetched. The only meaningful dispute is whether PEI created the strong secondary meanings associated with the mark.

PEI offered evidence, in the form of expert reports, tending to show that PEI did create the secondary meanings of “playboy” and “playmate.” PEI’s expert evidence countered the defendants’ expert evidence to the contrary, and suffices to generate a genuine issue of material fact on this issue.

c. **Factor Two: Proximity of the Goods.**

From an Internet searcher’s perspective, the relevant “goods” are the links to the websites being sought and the goods or services available at those sites. The proximity between PEI’s and its competitor’s goods provides the reason Netscape keys PEI’s marks to competitor’s banner advertisements in the first place. Accordingly, this factor favors PEI as well.

d. **Factor Three: Similarity of the Marks.**

No doubt exists regarding this factor. Aside from their lack of capitalization, their font, and the fact that defendants use

created by the markholder. Finally, the markets in which the markholder and the third parties use the mark must be considered. See Nat’l Lead Co. v. Wolfe, 223 F.2d 195, 204 (9th Cir. 1955) (considering, and rejecting, evidence of third-party use because use within the relevant market, for paint, was de minimis). Evidence of third-party use in markets similar to the markholder’s is more compelling than evidence of third-party use in unrelated markets. See id. Thus, even if relevant to our inquiry in the infringement context, the evidence would not be dispositive on summary judgment.
the plural form of “playmate,” the terms defendants use are identical to PEI’s marks. Thus, they are certainly similar.\footnote{See Sleekcraft, 599 F.2d at 350-52.}

e. \textit{Factor Five: Marketing Channels Used.}

This factor is equivocal. PEI and the advertisers use identical marketing channels: the Internet. More specifically, each of their sites appears on defendants’ search results pages. Given the broad use of the Internet today, the same could be said for countless companies. Thus, this factor merits little weight.

f. \textit{Factor Six: Type of Goods and Degree of Consumer Care Expected.}

This factor favors PEI. Consumer care for inexpensive products is expected to be quite low.\footnote{See Brookfield, 174 F.3d at 1060 (“[W]hen dealing with inexpensive products, customers are likely to exercise less care, thus making confusion more likely.”).} Low consumer care, in turn, increases the likelihood of confusion.\footnote{id.}

In addition to price, the content in question may affect consumer care as well. We presume that the average searcher seeking adult-oriented materials on the Internet is easily diverted from a specific product he or she is seeking if other options, particularly graphic ones, appear more quickly. Thus, the adult-oriented and graphic nature of the materials weighs in PEI’s favor as well.

g. \textit{Factor Seven: Defendants’ Intent in Selecting the Mark.}

This factor favors PEI somewhat. A defendant’s intent to
confuse constitutes probative evidence of likely confusion.\textsuperscript{36} Courts assume that the defendant’s intentions were carried out successfully. In this case, the evidence does not definitively establish defendants’ intent. At a minimum, however, it does suggest that defendants do nothing to prevent click-throughs\textsuperscript{37} that result from confusion. Moreover, they profit from such click-throughs.

Defendants monitor “click-through” rates on the advertisements they display. That is, they monitor the number of times consumers are diverted to their advertisers’ sites. They use the click-through rates as a way to gauge the success of the advertisements and to keep advertisers coming back to their services. Although some click-throughs may be the result of legitimate consumer interest, not confusion, some may be expected to result from confusion. Defendants will profit from both kinds of click-throughs. And they do nothing to ensure that only click-throughs based on legitimate interest, as opposed to confusion, occur.

PEI introduced evidence suggesting that labeling the advertisements would reduce click-through rates. It would also reduce confusion. However, although defendants control the content of advertisements in other contexts, defendants do not require that advertisers identify themselves on their banner ads. Moreover, they do not label the advertisements themselves. Perhaps even more telling, defendants refuse to remove the highly-rated terms “playboy” and “playmate” from their lists of keywords, even when advertisers request that they do so.\textsuperscript{38}

\textsuperscript{36}See Sleekcraft, 599 F.2d at 348 n.9.

\textsuperscript{37}If users click on a banner advertisement, Netscape has designed its program to link them immediately to the advertiser’s website. Thus, the user has “clicked-through” the advertisements to the advertiser’s website.

\textsuperscript{38}PEI introduced evidence that, even when advertisers objected to using PEI’s marks to key advertisements, defendants refused to remove the marks from the keying list. This places advertisers in a difficult situation, as described infra.
The above evidence suggests, at a minimum, that defendants do nothing to alleviate confusion, even when asked to do so by their advertisers, and that they profit from confusion. Although not definitive, this factor provides some evidence of an intent to confuse on the part of defendants. This factor thus favors PEI.

h. Factor Eight: Likelihood of Expansion of Product Lines.

Because the advertisers' goods and PEI's are already related, as discussed within factor two, this factor is irrelevant.

[7] Having examined all of the Sleekcraft factors, we conclude that the majority favor PEI. Accordingly, we conclude that a genuine issue of material fact exists as to the substantial likelihood of confusion. We now proceed to the defenses advanced by defendants.

3. Defenses.

[8] Defendants assert three defenses: fair use, nominative use, and functional use. Because we have found that a genuine issue of fact exists as to likelihood of confusion under Sleekcraft, we must deny summary judgment as to the fair use defense. A fair use may not be a confusing use. To

---

39 Lindy Pen Co., Inc. v. Bic Pen Corp., 725 F.2d 1240, 1248 (9th Cir. 1984) (declining to adopt an interpretation of fair use under which a use might be fair "even where likelihood of confusion has been shown," but noting that liability may not be imposed for truthful comparative advertising, an example of a nominative use).

40 See PEI v. Welles, 279 F.3d 796, 801 (9th Cir. 2002) (citing New Kids on the Block v. News America Publ'g, Inc., 971 F.2d 302, 309 (9th Cir. 1992)).
be considered a nominative use, the use of a mark must meet the following three-factor test:

First, the product or service in question must be one not readily identifiable without use of the trademark; second, only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and third, the user must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.41

Before we apply this test to the facts at hand, we would like to emphasize what facts are not at hand. We note that defendants’ use of PEI’s marks to trigger the listing of PEI sites, and other sites that legitimately use PEI’s marks,42 is not at issue here. In addition, we note that we are not addressing a situation in which a banner advertisement clearly identifies its source with its sponsor’s name,43 or in which a search engine clearly identifies a banner advertisement’s source. We are also not addressing a situation in which advertisers or defendants overtly compare PEI’s products to a competitor’s — saying, for example “if you are interested in Playboy, you may also be interested in the following message from [a different, named company].” Rather, we are evaluating a situation in which defendants display competitors’ unlabeled banner advertisements, with no label or overt comparison to PEI, after Internet users type in PEI’s trademarks.

[10] The situation with which we are dealing runs afoul of the first requirement for nominative use. Accordingly, we do not consider the other prongs.

41New Kids on the Block, 971 F.2d at 308 (footnote omitted).
42See, e.g., PEI v. Welles, 279 F.3d at 803-04 (concluding that defendant’s use of PEI’s marks in the metatags of her website was a permissible, nominative use).
43Doing so might eliminate the likelihood of initial interest confusion that exists in this case.
[11] Defendants could use other words, besides PEI's marks, to trigger adult-oriented banner advertisements. Indeed, they already do so. The list they sell to advertisers includes over 400 terms besides PEI's marks. There is nothing indispensable, in this context, about PEI's marks.\textsuperscript{44} Defendants do not wish to identify PEI or its products when they key banner advertisements to PEI's marks.\textsuperscript{46} Rather, they wish to identify consumers who are interested in adult-oriented entertainment so they can draw them to competitors' websites. Accordingly, their use is not nominative. Thus, we reverse the district court's grant of summary judgment based on nominative use.

[12] Defendants' final asserted defense, functional use, also fails. Defendants appear not to have raised this defense before the district court. Even if they have not waived the defense, however, it fails. Under the functional use doctrine, parts of a design that have a functional use may not receive trademark protection.\textsuperscript{46} We do not have such a case here.

[13] Nothing about the marks used to identify PEI's products is a functional part of the design of those products. PEI could easily have called its magazine and its models entirely

\textsuperscript{44}Compare Welles, 279 F.3d at 802 (explaining that, because Welles would have to use absurd and lengthy turns of phrase to describe her title as a Playboy Playmate of the Year without using the marks, her use of the marks satisfied the first requirement of nominative use).

\textsuperscript{46}Id. at 801 (noting that, unlike a traditional fair use, a nominative use is a defendant's use of a mark to identify "not its own product, but the plaintiff's").

different things without losing any of their intended function. Thus, the marks are not functional and may be granted trademark protection.\textsuperscript{47}

The fact that the marks make defendants' computer program more functional is irrelevant. Defendants designed their program to identify consumers interested in adult-oriented entertainment so that some percentage of those consumers might be attracted to competitors' websites, thereby helping defendants generate advertising revenue. Thus, defendants might conceivably be unable to trademark some of the terms used in their program because those terms are functional within that program. Because we are not dealing with defendants' wish to trademark their computer program, but with PEI's ability to protect the trademarks it already uses to identify its products, the doctrine of functional use does not help defendants here.

\textbf{[14]} We hold that genuine issues of material fact exist with respect to defendants' keying practices. Thus, we conclude that summary judgment was inappropriate on the trademark infringement claim.

\section*{B. Trademark Dilution}

We reverse the district court's grant of summary judgment on PEI's second cause of action, trademark dilution,\textsuperscript{48} and remand for further proceedings. We conclude that PEI has established that genuine issues of material fact exist regarding two of the three elements that the parties dispute: the famousness of the marks and defendants' commercial use of the mark.\textsuperscript{49} We will address each of the three disputed elements in turn.

\textsuperscript{47}Qualitex, 514 U.S. at 169-70.

\textsuperscript{48}PEI asserted claims under federal and state law. Analysis of the state law is substantially similar to analysis of the federal law. See Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 874 (9th Cir. 1999). Accordingly, we do not separately address state law claims.

\textsuperscript{49}The dilution statute, 15 U.S.C. § 1125(c), provides relief to the owners of famous marks by providing "an injunction against another person's
IV. CONCLUSION

[19] Genuine issues of material fact exist as to PEI’s trademark infringement and dilution claims. Accordingly, we reverse the district court’s grant of summary judgment in favor of defendants and remand for further proceedings.

REVERSED AND REMANDED.

BERZON, Circuit Judge, concurring:

I concur in Judge Nelson’s careful opinion in this case, as it is fully consistent with the applicable precedents. I write separately, however, to express concern that one of those precedents was wrongly decided and may one day, if not now, need to be reconsidered en banc.

I am struck by how analytically similar keyed advertisements are to the metatags found infringing in Brookfield Communications v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999). In Brookfield, the court held that the defendant could not use the trademarked term “moviebuff” as one of its metatags. Metatags are part of the HTML code of a web page, and therefore are invisible to internet users. Search engines use these metatags to pull out websites applicable to search terms. See also Promatek Indus., Ltd. v. Equitrac Corp., 300 F.3d 808, 812-13 (7th Cir. 2002) (adopting the Brookfield holding).

Specifically, Brookfield held that the use of the trademarked terms in metatags violated the Lanham Act because it caused “initial interest confusion.” Brookfield, 174 F.3d at 1062-66. The court explained that even though “there is no source confusion in the sense that consumers know [who] they are patronizing, . . . there is nevertheless initial interest confusion in the sense that, by using ‘moviebuff.com’ or
'MovieBuff' to divert people looking for 'MovieBuff' to its website, [the defendant] improperly benefits from the goodwill that [the plaintiff] developed in its mark.” Id. at 1062.

As applied to this case, Brookfield might suggest that there could be a Lanham Act violation even if the banner advertisements were clearly labeled, either by the advertiser or by the search engine. I do not believe that to be so. So read, the metatag holding in Brookfield would expand the reach of initial interest confusion from situations in which a party is initially confused to situations in which a party is never confused. I do not think it is reasonable to find initial interest confusion when a consumer is never confused as to source or affiliation, but instead knows, or should know, from the outset that a product or web link is not related to that of the trademark holder because the list produced by the search engine so informs him.

There is a big difference between hijacking a customer to another website by making the customer think he or she is visiting the trademark holder’s website (even if only briefly), which is what may be happening in this case when the banner advertisements are not labeled, and just distracting a potential customer with another choice, when it is clear that it is a choice. True, when the search engine list generated by the search for the trademark ensconced in a metatag comes up, an internet user might choose to visit westcoastvideo.com, the defendant’s website in Brookfield, instead of the plaintiff’s moviebuff.com website, but such choices do not constitute trademark infringement off the internet, and I cannot understand why they should on the internet.

For example, consider the following scenario: I walk into Macy’s and ask for the Calvin Klein section and am directed upstairs to the second floor. Once I get to the second floor, on my way to the Calvin Klein section, I notice a more prominently displayed line of Charter Club clothes, Macy’s own brand, designed to appeal to the same people attracted by the
style of Calvin Klein’s latest line of clothes. Let’s say I get diverted from my goal of reaching the Calvin Klein section, the Charter Club stuff looks good enough to me, and I purchase some Charter Club shirts instead. Has Charter Club or Macy’s infringed Calvin Klein’s trademark, simply by having another product more prominently displayed before one reaches the Klein line? Certainly not. See Gregory Shea, Note, Trademarks and Keyword Banner Advertising, 75 S. Cal. L. Rev. 529, 554 (2002) (comparing keyed banner advertisements to a customer entering a supermarket, requesting Tylenol, and then being directed to the pain reliever section which includes generic Acetaminophen, along with other generic and name-brand pain relievers); Julie A. Rajzer, Comment, Misunderstanding the Internet: How Courts are Overprotecting Trademarks Used in Metatags, 2001 L. Rev. Mich. St. U. C. L. 427, 462-63 (2001) (highlighting the brick-and-mortar world in which Kellogg’s Raisin Bran and Post Raisin Bran both appear next to one another on the same aisle).

Similarly, suppose a customer walks into a bookstore and asks for Playboy magazine and is then directed to the adult magazine section, where he or she sees Penthouse or Hustler up front on the rack while Playboy is buried in back. One would not say that Penthouse or Hustler had violated Playboy’s trademark. This conclusion holds true even if Hustler paid the store owner to put its magazines in front of Playboy’s.

One can test these analogies with an on-line example: If I went to Macy’s website and did a search for a Calvin Klein shirt, would Macy’s violate Calvin Klein’s trademark if it responded (as does Amazon.com, for example) with the requested shirt and pictures of other shirts I might like to consider as well? I very much doubt it.

Accordingly, I simply cannot understand the broad principle set forth in Brookfield. Even the main analogy given in Brookfield belies its conclusion. The Court gives an example
of Blockbuster misdirecting customers from a competing video store, West Coast Video, by putting up a highway billboard sign giving directions to Blockbuster but telling customers that a West Coast Video store is located there. Brookfield, 174 F.3d at 1064. Even though customers who arrive at the Blockbuster realize that it is not West Coast Video, they were initially misled and confused. Id.

But there was no similar misdirection in Brookfield, nor would there be similar misdirection in this case were the banner ads labeled or otherwise identified. The Brookfield defendant’s website was described by the court as being accurately listed as westcoastvideo.com in the applicable search results. Consumers were free to choose the official moviebuff.com website and were not hijacked or misdirected elsewhere. I note that the billboard analogy has been widely criticized as inapplicable to the internet situation, given both the fact that customers were not misdirected and the minimal inconvenience in directing one’s web browser back to the original list of search results. See J. Thomas McCarthy, McCarthy on Trademarks & Unfair Competition §25:69 (4th ed. 2003); Shea, supra at 552.

The degree to which this questionable aspect of Brookfield affects this case is not clear to me. Our opinion limits the present holding to situations in which the banner advertisements are not labeled or identified. See ante at 377. Whether, on remand, the case will remain so limited is questionable. PEI may seek to reach labeled advertisements as well.

There will be time enough to address the continuing vitality of Brookfield should the labeled advertisement issue arise later. I wanted to flag the issue, however, as another case based on the metatag aspect of Brookfield was decided recently, Horphag Research Ltd. v. Pellegrini, 337 F.3d 1036 (9th Cir. 2003), so the issue is a recurring one. Should the question arise again, in this case or some other, this court
needs to consider whether we want to continue to apply an insupportable rule.
Spyware: Background and Policy Issues for Congress

Summary

The term “spyware” is not well defined. Generally it is used to refer to any software that is downloaded onto a person’s computer without their knowledge. Spyware may collect information about a computer user’s activities and transmit that information to someone else. It may change computer settings, or cause “pop-up” advertisements to appear (in that context, it is called “adware”). Spyware may redirect a Web browser to a site different from what the user intended to visit, or change the user’s home page. A type of spyware called “keylogging” software records individual keystrokes, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor. Thus, passwords, credit card numbers, and other personally identifiable information may be captured and relayed to unauthorized recipients.

Some of these software programs have legitimate applications the computer user wants. They obtain the moniker “spyware” when they are installed surreptitiously, or perform additional functions of which the user is unaware. Users typically do not realize that spyware is on their computer. They may have unknowingly downloaded it from the Internet by clicking within a website, or it might have been included in an attachment to an electronic mail message (e-mail) or embedded in other software.

According to a survey and tests conducted by America Online and the National Cyber Security Alliance, 80% of computers in the test group were infected by spyware or adware, and 89% of the users of those computers were unaware of it. The Federal Trade Commission (FTC) issued a consumer alert on spyware in October 2004. It provided a list of warning signs that might indicate that a computer is infected with spyware, and advice on what to do if it is.

Several states have passed spyware laws, but there is no specific federal law regarding spyware. The 109th Congress is considering H.R. 29, H.R. 744, S. 687, and S. 1004. H.R. 29 was reported from the House Energy and Commerce Committee on April 12, 2005 (H.Rept. 109-32). The House Judiciary Committee approved H.R. 744 on May 18, 2005. The Senate Commerce, Science, and Transportation Committee held a hearing on spyware on May 11, 2005.

A central point of the debate is whether new laws are needed, or if industry self-regulation, coupled with enforcement actions under existing laws such as the Federal Trade Commission Act, is sufficient. The lack of a precise definition for spyware is cited as a fundamental problem in attempting to write new laws. FTC representatives and others caution that new legislation could have unintended consequences, barring current or future technologies that might, in fact, have beneficial uses. They further insist that, if legal action is necessary, existing laws provide sufficient authority. Consumer concern about control of their computers being taken over by spyware, and resulting impacts on their privacy, leads others to conclude that legislative action is needed.

This report will be updated as warranted.
Spyware: Background and Policy Issues for Congress

Background

Congress is debating whether to enact new legislation to deal with the growing problem of "Spyware." Spyware is not well defined, but generally includes software emplaced on a computer without the user's knowledge that takes control of the computer away from the user, such as by redirecting the computer to unintended websites, causing advertisements to appear, or collecting information and transmitting it to another person. The lack of a firm definition of the term adds to the complexities of drafting new laws.

The Federal Trade Commission (FTC) and others argue that industry self-regulation, and enforcement of existing laws, are sufficient. They worry that further legislation could have unintended consequences that, for example, limit the development of new technologies that could have beneficial uses. The 108th Congress debated spyware legislation, and two bills passed the House, but neither cleared Congress. Debate has resumed in the 109th Congress. Pending legislation is discussed later in this report.

What is Spyware?

The term "spyware" is not well defined. Jerry Berman, President of the Center for Democracy and Technology (CDT), explained in testimony to the Subcommittee on Communications of the Senate Commerce, Science, and Transportation Committee in March 2004 that "The term has been applied to software ranging from 'keystroke loggers' that capture every key typed on a particular computer; to advertising applications that track users' web browsing; to programs that hijack users' system settings." He noted that what these various types of software programs "have in common is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections."

Software programs that include spyware may be sold or available for free ("freeware"). They may be on a disk or other media, downloaded from the Internet, or downloaded when opening an attachment to an electronic mail (e-mail) message. Typically, users have no knowledge that spyware is on their computers. Because the

---

spyware is resident on the computer's hard drive, it can generate pop-up ads, for example, even when the computer is not connected to the Internet.

One example of spyware is software products that include, as part of the software itself, a method by which information is collected about the use of the computer on which the software is installed, such as Web browsing habits. Some of these products may collect personally identifiable information (PII). When the computer is connected to the Internet, the software periodically relays the information back to another party, such as the software manufacturer or a marketing company. Another oft-cited example of spyware is "adware," which may cause advertisements to suddenly appear on the user's monitor—called "pop-up" ads. In some cases, the adware uses information that the software obtained by tracking a user's Web browsing habits to determine shopping preferences, for example. Some adware companies, however, insist that adware is not necessarily spyware, because the user may have permitted it to be downloaded onto the computer because it provides desirable benefits.

As Mr. Berman explained, spyware also can refer to "keylogging" software that records a person's keystrokes. All typed information thus can be obtained by another party, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor (such as when entering a password). Commercial key logging software has been available for some time. In the context of the spyware debate, the concern is that such software can record credit card numbers and other personally identifiable information that consumers type when using Internet-based shopping and financial services, and transmit that information to someone else. Thus it could contribute to identity theft.

As discussed below, the lack of a precise definition for spyware is often cited by opponents of legislation as a reason not to legislate. They argue that without a definition, legislation could have unintended consequences, banning current or future technologies and activities that, in fact, could be beneficial. Some of these software applications, including adware and keylogging software, have legitimate uses. The question is whether the user has given consent for it to be installed.

The Chief Executive Officer of Webroot Software, C. David Moll, explained at a May 11, 2005 Senate Commerce Committee hearing that spyware presents a

---

2 The existence of keylogging software was publicly highlighted in 2001 when the FBI, with a search warrant, installed such software on a suspect's computer, allowing them to obtain his password for an encryption program he used, and thereby evidence. Some privacy advocates argued that wiretapping authority should have been obtained, but the judge, after reviewing classified information about how the software works, ruled in favor of the FBI. Press reports also indicate that the FBI is developing a "Magic Lantern" program that performs a similar task, but can be installed on a subject's computer remotely by surreptitiously including it in an e-mail message, for example.

3 For more on identity theft, see CRS Report RS22082, Identity Theft: The Internet Connection, by Marcia S. Smith; and CRS Report RL31919, Remedies Available to Victims of Identity Theft, by Angie A. Welborn.
threat in four ways: data security, online privacy, network and computer performance, and Internet commerce broadly.\textsuperscript{4}

\textbf{Prevalence of Spyware}

In October 2004, America Online (AOL) and the National Cyber Security Alliance (NCSA)\textsuperscript{5} released the results of a survey of 329 dial-up and broadband computer users regarding online threats, including spyware.\textsuperscript{6} According to the study:

\begin{itemize}
  \item 80\% of the computers they tested were infected with spyware or adware, and 89\% of the users of those computers were unaware of it;
  \item the average infected computer had 93 spyware/adware components on it, and the most found on a single computer was 1,059; and
  \item most users do not recognize the symptoms of spyware — 63\% of users with a pop-up blocker said they got pop-up ads anyway, 43\% of users said their home page had been changed without their permission, and 40\% said their search results are being redirected or changed.
\end{itemize}

Separately, Webroot Software, a provider of privacy and protection software, released the results of a survey of 287 corporate information technology managers on October 27, 2004. That survey concluded that although more than 70\% of corporations expressed increased concern about spyware, less than 10\% had implemented commercially available anti-spyware software.\textsuperscript{7}

\textbf{FTC Advice to Consumers}

The FTC issued a consumer alert about spyware in October 2004 offering a list of warning signs that might indicate that a computer is infected with spyware.\textsuperscript{8} The FTC alert listed the following clues:

\begin{itemize}
  \item a barrage of pop-up ads;
\end{itemize}


\textsuperscript{5} According to its website [http://www.staysafeonline.info], NCSA is a public-private partnership, with government sponsors including the Department of Homeland Security and the FTC. Its Board of Officers includes representatives from Cisco Systems, Symantec, RSA Security, AOL, McAfee, Microsoft, and BellSouth.


\textsuperscript{7} Spyware Infiltration Rises in Corporate Networks, but Webroot Survey Finds Companies Still Neglect Threat. PR Newswire, October 27, 2004, 06:00 (via Factiva).

\textsuperscript{8} Available at [http://www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm].
• a hijacked browser — that is, a browser that takes you to sites other than those you type into the address box;
• a sudden or repeated change in your computer’s Internet home page;
• new and unexpected toolbars;
• new and unexpected icons on the system tray at the bottom of your computer screen;
• keys that don’t work (for example, the “Tab” key that might not work when you try to move to the next field in a Web form);
• random error messages; and
• sluggish or downright slow performance when opening programs or saving files.

The FTC alert also offered preventive actions consumers can take.

• update your operating system and Web browser software;
• download free software only from sites you know and trust;
• don’t install any software without knowing exactly what it is;
• minimize “drive-by” downloads by ensuring that your browser’s security setting is high enough to detect unauthorized downloads;
• don’t click on any links within pop-up windows;
• don’t click on links in spam that claim to offer anti-spyware software; and
• install a personal firewall to stop uninvited users from accessing your computer.

Finally, the FTC alert advised consumers who think their computers are infected to get an anti-spyware program from a vendor they know and trust; set it to scan on a regular basis, at startup and at least once a week; and delete any software programs detected by the anti-spyware program that the consumer does not want.

Reviews of some of the commercially available anti-spyware programs are available in magazines such as PC World and Consumer Reports, or at [http://www.spywarerarior.com]. Consumers must be cautious about choosing a spyware product, however. At a May 11, 2005 Senate Commerce, Science, and Transportation Committee hearing, the point was raised that some websites masquerade as anti-spyware sites selling spyware solutions, but instead download spyware onto an unwitting consumer’s computer.

Other FTC Activities

The FTC held a workshop on spyware on April 19, 2004. The director of FTC’s Bureau of Consumer Protection, Howard Beales, summarized the workshop at a hearing before the Subcommittee on Telecommunications and the Internet of the

---


10 The transcript of the workshop is available at [http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf].
House Energy and Commerce Committee 10 days later. He listed a number of ways in which spyware can harm consumers and businesses.

.... It seems clear from the workshop's discussions spyware may harvest personally identifiable information from consumers through monitoring computer use without consent. It also may facilitate identity theft by surreptitiously planting a keystroke logger on a user's computer.

Spyware may create security risks if it exposes communications channels to hackers. It also may effect [sic] the operation of personal computers, causing crashes, browser hijacking, homepage resetting and the like. These harms are problems in themselves and could lead to a loss in consumer confidence in the Internet as a medium of communication and commerce.

Second, many of the panelists discussed how spyware may cause problems for businesses, too. Companies may incur costs as they seek to block and remove spyware from computers of their employees or their customers. Employees will also be less productive if spyware causes their computers to crash or if they're distracted...by a barrage of pop-up ads. Spyware that captures the keystrokes of employees could be used to obtain trade secrets and confidential information from businesses. 11

Mr. Beale also listed a number of ways in which the computer industry is attempting to help consumers and businesses cope with the spyware problem, for example through development of anti-spyware programs.

An FTC staff report on the results of the workshop was published in March 2005. 12 The report concluded that addressing the spyware problem will require a coordinated and sustained effort on the part of the private sector and government.

The FTC also has taken legal action to stop spyware practices. The Commission filed its first spyware case in October 2004 in response to a complaint filed by the Center for Democracy and Technology (CDT). In an October 12, 2004 press release, 13 the FTC explained that it was charging Sanford Wallace and two companies with which he is associated, Smartbot.Net and Seismic Entertainment Productions, Inc., with unfair and deceptive practices for using a variety of techniques to direct consumers to their websites where spyware was downloaded onto their computer without notice or consent. The FTC asserts that the spyware created serious problems on those computers, and the defendants thereupon offered to sell the consumers software for $30 to fix the problems. The FTC asked the U.S. District Court, District of New Hampshire, "to issue an order preventing the defendants from

---

12 An FTC press release, and a link to the report, are at [http://www.ftc.gov/opa/2005/03/spywarept.htm].

**State Laws**

In March 2004, Utah became the first state to enact spyware legislation (although a preliminary injunction in is place preventing it from taking effect). In testimony to a House Energy and Commerce subcommittee the next month, FTC Commissioner Mozelle Thompson asked states to "be cautious" about passing such legislation because "a patchwork of differing and inconsistent state approaches might be confusing to industry and consumers alike."

Nonetheless, several more states passed such legislation in 2004 or 2005, and others are considering it. According to the National Conference of State Legislatures (NCSL), California, Virginia, Arkansas, and Arizona have joined Utah in enacting spyware legislation, and legislatures in Georgia, Iowa and Washington have passed such legislation and sent it the Governor for signature. A list of the state laws that have passed or are under consideration is available at the NCSL's website at [http://www.ncsl.org/programs/lis/spyware04.htm] for 2004, and [http://www.ncsl.org/programs/lis/spyware05.htm#arizona] for 2005.

**Issues for Congress**

The 109th Congress has resumed debate on the spyware issue. Two bills are pending in the House: H.R. 29 (Bono) and H.R. 744 (Goodlatte). Two bills also are pending in the Senate: S. 687 (Burns-Wyden) and S. 1004 (Allen). Those bills are summarized later in this report. In the 108th Congress, the House passed two spyware bills, and a bill was reported from committee in the Senate. They are summarized in the Appendix.

---

14 FTC press release, Ibid.


17 WhenU, an adware company, filed suit against the Utah law on constitutional grounds. (WhenU’s President and CEO, Avi Naider, testified to the Senate Commerce Committee’s Subcommittee on Communications about spyware in March 2004. See Industry Positions, below.) The Third Judicial District Court in Salt Lake City, Utah granted a preliminary injunction on June 22, 2004, preventing the law from taking effect. See Judge Grants NY Pop-Up Company Preliminary Injunction Against Spyware Law. Associated Press, June 23, 2004, 06:06 (via Factiva).

Debate Over the Need for Federal Spyware Legislation

The main issue for Congress is whether to enact new legislation specifically addressing spyware, or to rely on industry self-regulation and enforcement actions by the FTC and the Department of Justice under existing law.

Advocates of legislation want specific laws to stop spyware. For example, they want software providers to be required to obtain the consent of an authorized user of a computer ("opt-in") before any software is downloaded onto that computer. Skeptics contend that spyware is difficult to define and consequently legislation could have unintended consequences, and that legislation is likely to be ineffective. One argument is that the "bad actors" are not likely to obey any opt-in requirement, but are difficult to locate and prosecute. Also, some are overseas and not subject to U.S. law. Other arguments are that one member of a household (a child, for example) might unwittingly opt-in to spyware that others in the family would know to decline, or that users might not read through a lengthy licensing agreement to ascertain precisely what they are accepting.

In many ways, the debate over how to cope with spyware parallels the controversy that led to unsolicited commercial electronic mail ("spam") legislation. Whether to enact a new law, or rely on enforcement of existing law and industry self-regulation, were the cornerstones of that debate as well. Congress chose to pass the CAN-SPAM Act (P.L. 108-187). Questions remain about that law’s effectiveness. MX Logic, a provider of "email defense solutions," reported in January 2005 that 97% of spam in 2004 did not comply with the CAN-SPAM Act. Such reports fuel the argument that spyware legislation similarly cannot stop the threat. In the case of spam, FTC officials emphasized that consumers should not expect any legislation to solve the spam problem — that consumer education and technological advancements also are needed. The same likely is true for spyware, too.

Several subcommittee or full committee hearings on spyware have been held in 2004 and 2005 at which witnesses from the government, industry, and consumer groups have laid out their various points of view. Chronologically they are: House Energy and Commerce Committee, Subcommittee on Telecommunications and the Internet, April 29, 2004; Senate Commerce, Science, and Transportation Committee, Communications Subcommittee, March 23, 2004; House Energy and Commerce Committee, January 26, 2005; and Senate Commerce, Science, and Transportation Committee, May 11, 2005.

**FTC’s Position.** The FTC has not taken a formal position on the spyware issue, but two commissioners have stated that they do not support new legislation at this time. Commissioner Orson Swindle reportedly told a March 4, 2005 technology forum sponsored by Citizens Against Government Waste that the government should

---


“walk slowly” on such issues, noting that participants in the spyware debate cannot
even agree on a definition of the term. 21 He reportedly called for Congress to focus
on expanding enforcement of existing laws against bad actors, rather than further
regulation of software makers. At a November 5, 2004 luncheon sponsored by the
Cato Institute, 22 Mr. Swindle expressed similar views, and also called on industry to
develop effective approaches to counteract spyware — through self-regulation,
adopting standards, consumer education, business education, assisting the
government in finding the people doing the harm, and monitoring their own
advertising (and whom they hire to do advertising on their behalf). He added that
if industry did not solve the problem, by necessity the government would need to act.

At the 2004 House Energy and Commerce subcommittee hearing,
Commissioner Mozelle Thompson argued that industry should be given an
opportunity to solve the problem and the government should step in only if necessary.
Mr. Thompson reviewed challenges he had given to industry at the FTC’s spyware
workshop: to develop a set of “best practices ... including meaningful notice and
choice so that consumers can make informed decisions about whether or not they
wish to deal with an online business that uses monitoring software or partners with
companies that do”; to develop a campaign to educate consumers and businesses
about spyware and how to cope with it; and to establish a mechanism to allow
businesses and consumers to have a dialog “on how government can take action
against those who do wrong and undermine consumer confidence through the misuse
of spyware.” 23

Industry Positions. At the 2004 Senate Commerce subcommittee hearing,
industry witnesses discussed the difficulties in legislating in an area where definitions
are unclear, and that the pace of technology might quickly render any such definitions
obsolete. Robert Holleyman, representing the Business Software Alliance, testified
that the focus of legislation should be regulating bad behavior, not technology. He
expressed reservations about legislation which then was pending in the Senate, and
called on Congress not to preclude the evolution of tools and marketplace solutions
to the problem.

While there is concern generally about any software product installed without
the user’s knowledge or consent, adware is a particular area of controversy. Many
users object to pop-up ads as vigorously as they do to spam. The extent to which
pop-up ads are, or should be, included in a definition of spyware was discussed at the
2004 Senate Commerce subcommittee hearing. Avi Naider, President and CEO of
WhenU.com, argued that although his company’s WhenU software does create pop-
up ads, it is not spyware because users are notified that the program is about to be
installed, must affirmatively consent to a license agreement, and may decline it. Mr.

21 As reported in: “Walk Slowly” on Privacy Legislation, FTC Comr. Says. Warren’s
Washington Internet Daily, March 7, 2005 (via Factiva).

22 A video of the presentation is available at [http://www.cato.org/event.php?eventid=1725].
See also: FTC’s Swindle: Leave Spyware Solution to Industry. Warren’s Washington
Internet Daily, November 8, 2004 (via Factiva).

provided by Federal Document Clearing House (via Factiva).
Naider explained that his program often is "bundled" with software that users obtain for free (called "free-ware"), or a software developer may offer users a choice between paying for the software or obtaining it for free if they agree to receive ads from WhenU. While agreeing that spyware is a serious concern, and that Congress and the FTC should regulate in this area, Mr. Naider urged that legislation be written carefully to exclude products like his that offer notice and choice and therefore should not be considered spyware. As noted above, WhenU has filed suit against a Utah law regulating spyware.

At the 2004 House Energy and Commerce subcommittee hearing, David Baker, representing Earthlink, described his company's efforts to combat spyware, and supported legislation to protect consumers. Jeffrey Friedberg, from Microsoft, said that his company supports a "holistic" solution, and that if existing law is inadequate, then additional legislation would be appropriate.

At the 2005 House Energy and Commerce Committee hearing, representatives of Microsoft and Earthlink generally supported H.R. 29, with some minor alterations. Modifications were made to that bill during subcommittee and full committee markup, reportedly in response to industry and Senate concerns.24

At the 2005 Senate Commerce Committee hearing, the Network Advertising Initiative (NAI) called for federal legislation that preempts state laws, and that focuses on fraudulent and deceptive behaviors. NAI's Executive Director, J. Trevor Hughes, stated that NAI supports Section 2 of H.R. 29, which deals with deceptive practices, but not other provisions of that bill that would set standards for online advertising. He argued that "Online advertising is the primary economic force that creates the enormous amount of free content we enjoy online today. Proscribing online advertising will compromise that economic model, and may threaten the available of free resources online."25 He added that "Spyware is not caused by technology. Indeed, in many cases the technology is irrelevant to the practice involved. If legislation were to limit a certain technology, the purveyors of spyware would simply move to, or develop, other technologies to continue their activities. Prohibiting or proscribing technologies is not good public policy."26 He argued that industry self regulation and technology solutions are needed in addition to narrowly-based legislation, and cautioned that spyware should not be confused with privacy, and the two should be treated separately. Conversely, at the same hearing, Webroot


26 Hughes, May 11, 2005 Senate Commerce Committee testimony, Ibid.
Software CEO C. David Moll, specifically linked spyware and online privacy, saying that “spyware is the cyber-age equivalent of someone trespassing into your home.”\(^{27}\)

The Information Technology Association of America (ITAA) reportedly is backing H.R. 744 (described below).\(^{28}\)

**Consumer Groups and Others.** At the 2004 Senate Commerce subcommittee hearing, John L. Levine, author of The Internet for Dummies and similar books, concluded that legislation should ban spyware entirely, or consumers should be able to give a one-time permanent notice (akin to the telemarketing Do Not Call list) that they do not want spyware on their computers. He also said that the legislation should allow consumers to sue violators, rather than relying only on the FTC and state Attorneys General to enforce the law.

At the same 2004 hearing, CDT’s Jerry Berman noted that three existing laws can be used to address spyware concerns: the Federal Trade Commission Act (the FTC Act), the Electronic Communications Privacy Act (ECPA), and the Computer Fraud and Abuse Act (CFAA). He added that technology measures, self-regulation and user education also are important to dealing with spyware. He concluded that CDT believes that new legislation specifically targeted at spyware would be useful, but that Congress also should pass broad Internet privacy legislation that could address the privacy aspects of the spyware debate. Another CDT representative, Ari Schwartz, made similar arguments at the other three hearings.

---

**109th Congress Legislation**

Two bills are pending in the House — H.R. 29 (Bono) and H.R. 744 (Goodlatte) — both of which are very similar to legislation that passed the House in 2004 (H.R. 2929 and H.R. 4661, respectively). Two bills are pending in the Senate — S. 687 (Burns), which is similar to legislation that was considered in 2004, but did not reach the floor (S. 2145); and S. 1004 (Allen). Action in the 108th Congress is summarized in the Appendix.

**H.R. 29 (Bono), Spy Act.** H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act (Spy Act), is a revised version of H.R. 2929, which passed the House in 2004 (see Appendix). The House Energy and Commerce Committee held a hearing on H.R. 29 on January 26, 2005. The only change made to the bill's language when it was reintroduced was changing the date when the act would sunset to 2010 (instead of 2009) so that it still would have a five-year lifetime. Other modifications (including changing SPY ACT to Spy Act) were made during subcommittee markup on February 4, 2005, and full committee markup on March 9, 2005. The bill was reported from committee on April 12, 2005 (H. Rept. 109-32).

---


UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term 2003
(Argued April 5, 2004 Decided June 27, 2005)
Docket Nos. 04-0026-cv(L), 04-0446-cv(CON)

1-800 CONTACTS, INC.,

Plaintiff-Appellee,

v.

WHENU.COM, INC. and VISION DIRECT, INC.,

Defendants-Appellants.

Before: WALKER, Chief Judge, and STRAUB, Circuit Judge.¹

Interlocutory appeal in a trademark infringement action
challenging the district court's issuance of a preliminary
injunction that, inter alia, enjoins defendant from causing
"pop up" advertisements to appear on computer screens
contemporaneously with the appearance of plaintiff's internet
website or otherwise using plaintiff's trademarks.

REVERSED and REMANDED with instructions.

¹The Honorable Ellsworth Van Graafeiland, of the United
States Court of Appeals for the Second Circuit, was part of
this panel, but passed away following oral argument. The
appeal is being decided by the remaining two members of the
panel, who are in agreement. See 2d Cir. R. § 0.14(b).
TERENCE P. ROSS, Gibson, Dunn & Crutcher, L.L.P. (Rachel A. Clark, Prasanth R. Akkapeddi, and Amy E. Barrier, on the brief), Washington, DC, for Plaintiff-Appellee 1-800 Contacts, Inc.

CELIA GOLDWAG BARENHOLTZ, Kronish, Lieb, Weiner & Hellman (Michael D. Paley, Jason M. Koral, and Ian Ross Shapiro, on the brief), New York, NY, for Defendant-Appellant WhenU.Com, Inc.

JEFFREY E. OSTROW, Simpson Thacher & Bartlett LLP (Patrick E. King and Theodore J. McEvoy, on the brief), New York, NY, for Defendant-Appellant Vision Direct, Inc.

Mark A. Lemley, Keker & Van Nest, LLP, San Francisco, CA, for amicus curiae Google Inc. urging reversal of the district court


Professor Eric Goldman, Marquette University Law School, Milwaukee, WI; Cindy Cohn, Fred von Lohmann, Electronic Frontier Foundation, San Francisco, CA, for amicus curiae
JOHN M. WALKER, JR., Chief Judge:

Defendant-appellant WhenU.com, Inc. ("WhenU") is an internet marketing company that uses a proprietary software called "SaveNow" to monitor a computer user's internet activity in order to provide the computer user ("C-user") with advertising, in the form of "pop-up ads," that is relevant to that activity. Plaintiff-appellee 1-800 Contacts, Inc. ("1-800") is a distributor that sells contact lenses and related products by mail, telephone, and internet website. At the time 1-800 filed this action in the United States District Court for the Southern District of New York (Deborah A. Batts, District Judge), it owned a registered trademark in the service mark "WE DELIVER. YOU SAVE." and had filed applications with the United States Patent and Trademark Office on July 8, 1999, to register the service mark "1-800CONTACTS", and on October 2, 2000, to register the service mark of "1-800CONTACTS" in a specific color-blocked design logo.\(^2\)

\(^2\)1-800 obtained registration for this service mark on January 21, 2003.

\(^3\)This service mark was described as follows:

Applicant claims the colors yellow, blue and white as part of the mark. The box behind the word CONTACTS is yellow. The border around the yellow
1-800 filed a complaint alleging, *inter alia*, that WhenU was infringing 1-800's trademarks, in violation of the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a)(1), by causing pop-up ads of 1-800's competitors to appear on a C-user's desktop when the C-user has accessed 1-800's website. In an Opinion entered January 7, 2004, the district court granted 1-800's motion for a preliminary injunction as it related to 1-800's trademark claims, and enjoined WhenU from using or otherwise displaying 1-800's trademarks, or anything confusingly similar to such trademarks, in connection with WhenU's contextually relevant advertising. 1-800 Contacts, 309 F. Supp. 2d 467 (S.D.N.Y. 2003). WhenU has filed this

---

In addition to the trademark claims, 1-800 asserts claims for (1) unfair competition, false designation of origin, trademark dilution, and cybersquatting, in violation of § 43 of the Lanham Act, 15 U.S.C. § 1125; (2) copyright infringement and contributory copyright infringement, in violation of the Federal Copyright Act, 17 U.S.C. §§ 101, et seq.,; and (3) state law claims for trademark dilution and injury to business reputation, in violation of N.Y. Gen. Bus. L. § 360-1; and (4) common law claims for unfair competition and tortious interference with prospective economic advantage.

Several claims name Vision Direct, Inc., one of the 1-800 competitors whose advertisements were featured in WhenU's pop-up ads, as either defendant or co-defendant with WhenU.

The district court denied part of 1-800's motion, which related to 1-800's copyright claims.
interlocutory appeal.6

We hold that, as a matter of law, WhenU does not “use” 1-800’s trademarks within the meaning of the Lanham Act, 15 U.S.C. § 1127, when it (1) includes 1-800’s website address, which is almost identical to 1-800’s trademark, in an unpublished directory of terms that trigger delivery of WhenU’s contextually relevant advertising to C-users; or (2) causes separate, branded pop-up ads to appear on a C-user’s computer screen either above, below, or along the bottom edge of the 1-800 website window. Accordingly, we reverse the district court’s entry of a preliminary injunction and remand with instructions to (1) dismiss with prejudice 1-800’s trademark infringement claims against WhenU, and (2) proceed with 1-800’s remaining claims.

BACKGROUND

I. The Internet and Windows

By way of introduction to this case we incorporate the district court’s helpful tutorial on the internet and the Microsoft Windows operating environment as it pertains to this litigation:

6‘Vision Direct, Inc., also appealed the district court’s decision and was a party to this consolidated appeal. See Docket No. 04-0446(CON). Following oral argument, however, 1-800 and Vision Direct filed a stipulation of dismissal with respect to all of 1-800’s claims against Vision Direct. Accordingly, we do not address those claims or Vision Direct’s arguments on appeal. Id.
The Internet is a global network of millions of interconnected computers. . . . [A C-user] can access . . . information that is stored on the Internet in repositories called "servers." Much of the information stored in servers on the Internet can be viewed . . . in the form of "webpages," which are collections of pictures and information, retrieved from the Internet and assembled on the [C-user]'s computer screen. "Websites" are collection[s] of related webpages that are organized and linked together to allow a [C-user] to move from webpage to webpage easily. . . .

[A C-user] generally connects to the Internet using an internet service provider ("ISP")\textsuperscript{10} . . . , which allows the [C-user]'s computer to communicate with the Internet. Once a connection to the Internet has been established . . . , a [C-user] may "browse" or "surf" the Internet by using a software program called an Internet browser ("browser"). Microsoft Internet Explorer is one example of a browser program.\textsuperscript{11} . . .

\textsuperscript{10} Examples of ISPs include Earthlink, Verizon, NetZero, America Online.

\textsuperscript{11} Other examples of browser programs include Netscape Navigator, Opera, and Mozilla; in addition, many residential ISPs like Earthlink and America Online provide their own proprietary browsers.

To retrieve information from the Internet, a [C-user] may type [a specific] address[, called a domain name,.\textsuperscript{13} of a website into the [address line of a] web browser . . . .

\textsuperscript{13} . . . . Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489, 492-93 (2d Cir. 2000) [providing detailed explanation of domain names].

. . . .

[Alternatively,.] . . . a [C-user] can use [a "search engine"] to find information [by] . . . typ[ing] in a word or words describing what is
sought, and the search engine will identify websites
and webpages that contain those words.

1-800 Contacts, 309 F. Supp. 2d at 474-75 (internal citations
and some footnotes omitted).

The district court further explained that

[m]any [C-users] access the Internet with computers
that use the Microsoft Windows operating system
("Windows"). Windows allows a [C-user] to work in
numerous software applications simultaneously. In
Windows, the background screen is called the
"desktop." When a software program is launched, a
"window" appears on the desktop, within which the
functions of that program are displayed and
operate. A [C-user] may open multiple windows
simultaneously, allowing the [C-user] to launch and
use more than one software application at the same
time. Individual windows may be moved around the
desktop, and because the computer screen is
two-dimensional, one window may obscure another
window, thus appearing to be "in front of" another
window.

Id. at 475 (internal citations omitted). Some programs on a
C-user’s computer, such as a calendar or e-mail application,
may cause windows to open on the C-user’s desktop
independently of any contemporaneous action by the C-user.

See Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d
734, 743 ¶ 53 (E.D. Mich. 2003); see generally id. at 740-43
(providing in-depth description of how software applications
and web browsers operate in the Windows environment, and
noting that Windows is currently used on approximately 95% of
personal computers).
II. The Challenged Conduct

The specific conduct at issue in this case has been described in detail by the district court, see 1-800 Contacts, 309 F. Supp. 2d at 476-78, as well as other courts that have addressed similar claims against WhenU, see Wells Fargo, 293 F. Supp. 2d at 738-40, 743-46; U-Haul Int’l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723, 725-26 (E.D. Va. 2003). Accordingly, we recite only those facts relevant to this appeal.

WhenU provides a proprietary software called “SaveNow” without charge to individual C-users, usually as part of a bundle of software that the C-user voluntarily downloads from the internet. “Once installed, the SaveNow software requires no action by the [C-user] to activate its operations; instead, the SaveNow software responds to a [C-user]’s ‘in-the-moment’ activities by generating pop-up advertisement windows” that are relevant to those specific activities. 1-800 Contacts, 309 F. Supp. 2d at 477. To deliver contextually relevant advertising to C-users, the SaveNow software employs an internal directory comprising “approximately 32,000 [website addresses] and [address] fragments, 29,000 search terms and 1,200 keyword algorithms,” Wells Fargo, 293 F. Supp. 2d at 743 ¶ 58, that correlate with particular consumer interests to screen the words a C-user
types into a web browser or search engine or that appear
within the internet sites a C-user visits.

When the SaveNow software recognizes a term, it randomly
selects an advertisement from the corresponding product or
service category to deliver to the C-user’s computer screen
at roughly the same time the website or search result sought
by the C-user appears. As the district court explained,

The SaveNow software generates at least three kinds
of ads—an ad may be a small ‘pop-up’ . . . [that
appears] in the bottom right-hand corner of a [C-
user]’s screen; it may be a ‘pop-under’
advertisement that appears behind the webpage the
[C-user] initially visited; or it may be a
‘panoramic’ ad[] that stretches across the bottom
of the [C-user]’s computer screen.

1-800 Contacts, 309 F. Supp. 2d at 478. Each type of ad
appears in a window that is separate from the particular
website or search-results page the C-user has accessed. Id.
In addition, a label stating “A WhenU Offer--click ? for
info.” appears in the window frame surrounding the ad,
together with a button on the top right of the window frame
marked “?”, which, when clicked by the C-user, displays a new
window containing information about WhenU and its ads,7 as

7Specifically, C-users are informed that

“[t]his offer is brought to you by WhenU.com,
through the SaveNow service. SaveNow alerts you to
offers and services at the moment when they are most
relevant to you. SaveNow does not collect any
personal information or browsing history from its
users. Your privacy is 100 percent protected. The
well as instructions for uninstalling the resident SaveNow software. *Id.* at 478 nn.22 & 23.

Usually there is a "few-second" delay between the moment a user accesses a website, and the point at which a SaveNow pop-up advertisement appears on the [C-user]'s screen.

If a SaveNow user who has accessed the 1-800 Contacts website and has received a WhenU.com pop-up advertisement does not want to view the advertisement or the advertiser's website, the user can click on the visible portion of the [1-800] window . . . , [which will move] the 1-800 Contacts website . . . to the front of the screen display, with the pop-up ad moving behind the website window. Or, . . . the [C-user] can close the pop-up website by clicking on its "X," or close, button. If the user clicks on the pop-up ad, the main browser window (containing the 1-800 Contacts website) will be navigated to the website of the advertiser that was featured inside the pop-up advertisement.

*Id.* at 476-77 (internal citations omitted).

In its complaint, 1-800 alleges that WhenU's conduct infringes 1-800's trademarks, in violation of Sections 32(1) and 43(a) of the Lanham Act, 15 U.S.C. §§ 1114(1), 1125(a), by delivering advertisements of 1-800's competitors (*e.g.*, Vision Direct, Inc.) to C-users who have intentionally accessed 1-800's website. Although somewhat difficult to
discern from the complaint, the allegations that pertain specifically to 1-800’s trademark claims appear to be as follows: (1) WhenU’s pop-up ads appear “on,” “over,” or “on top of” the 1-800 website without 1-800’s authorization, and change its appearance; (2) as a result, the ads impermissibly “appear to be an integral and fully authorized part of [1-800’s] website”; (3) in addition, WhenU’s unauthorized pop-up ads “interfere with and disrupt the carefully designed display of content” on the website, thereby altering and hindering a C-user’s access to 1-800’s website; (4) WhenU is thereby “free-riding” and “trad[ing] upon the goodwill and substantial customer recognition associated with the 1-800 Contacts marks”; and (5) WhenU is using 1-800’s trademarks in a manner that creates a likelihood of confusion.

Following an evidentiary hearing on 1-800’s motion for a preliminary injunction, the district court held that 1-800 had demonstrated a likelihood of success on its trademark infringement claims and issued a preliminary injunction prohibiting WhenU from utilizing 1-800’s trademarks. 8 1-800

8The district court’s order stated, in relevant part:

[WhenU is] preliminarily enjoined from: 1) including the 1-800 Contacts mark, and confusingly similar terms, as elements in the SaveNow software directory, and 2) displaying Plaintiff’s mark “in the . . . advertising of” Defendant Vision Direct’s services, by causing Defendant Vision Direct’s pop-up advertisements to appear when a computer user
Contacts, 309 F. Supp. 2d at 510. WhenU appeals the district
court’s decision.

DISCUSSION

WhenU challenges the district court’s finding that WhenU
"uses" 1-800’s trademarks within the meaning of the Lanham
at 489. In the alternative, WhenU argues that the district
court erred in finding that WhenU’s pop-up ads create a
likelihood of both source confusion and "initial interest
confusion," as to whether WhenU is "somehow associated with
[1-800] or that [1-800] has consented to [WhenU’s] use of the
pop-up ad[s]." Id. at 494; see id. at 503, 504. Because we
agree with WhenU that it does not "use" 1-800’s trademarks,
we need not and do not address the issue of likelihood of
confusion.

I. Legal Standards

A. Preliminary Injunction

To obtain a preliminary injunction,
a party . . . must demonstrate (1) the likelihood
of irreparable injury in the absence of such an

has made a specific choice to access or find
Plaintiff’s website by typing Plaintiff’s mark into
the URL bar of a web browser or into an Internet
search engine. Within 30 days of the date of this
Order, Defendants SHALL effect this injunction.

1-800 Contacts, 309 F. Supp. 2d at 510 (alteration in
original).
injunction, and (2) either (a) likelihood of success on the merits or (b) sufficiently serious questions going to the merits to make them a fair ground for litigation plus a balance of hardships tipping decidedly toward the party requesting the preliminary relief.


Such abuse will be found if a district court rests its decision on a clearly erroneous finding of fact or makes an error of law. Id.

B. Lanham Act

In order to prevail on a trademark infringement claim for registered trademarks, pursuant to 15 U.S.C. § 1114, 9 or

915 U.S.C. § 1114 provides, in relevant part,

(1) Any person who shall, without the consent of the registrant--

(a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive . . .

. . . ,

shall be liable in a civil action by the registrant for the remedies hereinafter provided.
unregistered trademarks, pursuant to 15 U.S.C. § 1125(a)(1),\textsuperscript{10} a plaintiff must establish that (1) it has a valid mark that is entitled to protection under the Lanham Act; and that (2) the defendant used the mark, (3) in commerce, (4) "in connection with the sale . . . or advertising of goods or services," 15 U.S.C. § 1114(1)(a), (5) without the plaintiff's consent. See Time, Inc. v. Petersen Publ'g Co., 173 F.3d 113, 117 (2d Cir. 1999); Genesee Brewing Co., Inc. v. Stroh Brewing Co., 124 F.3d 137, 142 (2d Cir. 1997). In

\textsuperscript{10}15 U.S.C. § 1125 provides, in relevant part,

(a) Civil action

(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which--

(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.
addition, the plaintiff must show that defendant’s use of
that mark "is likely to cause confusion . . . as to the
affiliation, connection, or association of [defendant] with
[plaintiff], or as to the origin, sponsorship, or approval of
[the defendant’s] goods, services, or commercial activities
by [plaintiff]." 15 U.S.C. § 1125(a)(1)(A); see also Estee
Lauder Inc. v. The Gap, Inc., 108 F.3d 1503, 1508-09 (2d Cir.
1997); Gruner + Jahr USA Publ’g v. Meredith Corp., 991 F.2d
1072, 1075 (2d Cir. 1993).

The only issue before us on appeal is whether the
district court abused its discretion when it entered the
preliminary injunction against WhenU; specifically, whether
the district court erred in finding that 1-800 had
demonstrated a likelihood of success on its trademark claims.
As a result, the threshold of error required to reverse the
district court’s decision is higher than it would be were we
reviewing a decision on 1-800’s trademark claims themselves.
That higher threshold is met in this case, however, because
the district court erred as a matter of law in finding that
WhenU “uses” 1-800’s trademark. Because 1-800 cannot
establish an essential element of its trademark claims, not
only must the preliminary injunction be vacated, but 1-800’s
trademark infringement claims must be dismissed as well.

II. “Use” Under the Lanham Act
The Lanham Act defines "use in commerce," in relevant part, as follows:

... For purposes of this Chapter, a mark shall be deemed to be in use in commerce—

(1) on goods when—

(A) it is placed in any manner on the goods or their containers or the displays associated therewith or on the tags or labels affixed thereto, or if the nature of the goods makes such placement impracticable, then on documents associated with the goods or their sale, and

(B) the goods are sold or transported in commerce, and

(2) on services when it is used or displayed in the sale or advertising of services and the services are rendered in commerce ... .


In issuing the preliminary injunction, the district court held that WhenU use[s] [1-800]’s mark in two ways. First, in causing pop-up advertisements for Defendant Vision Direct to appear when SaveNow users have specifically attempted to access [1-800]’s website--on which Plaintiff’s trademark appears--[WhenU is] displaying Plaintiff’s mark “in the ... advertising of” Defendant Vision Direct’s services ... [and, t]hus, ... [is] “using” Plaintiff’s marks that appear on Plaintiff’s website.

Second, Defendant WhenU.com includes Plaintiff’s [website address], <www.1800contacts.com>, [which incorporates 1-800’s trademark,] in the proprietary WhenU.com directory of terms that triggers pop-up advertisements on SaveNow users’ computers. In so doing, Defendant WhenU.com “uses” Plaintiff’s mark ... to
advertise and publicize companies that are in
direct competition with Plaintiff.

1-800 Contacts, 309 F. Supp. 2d at 489.

Prior to the district court's decision, two other courts
had addressed the issue of "use" as it applies to WhenU's
specific activities and reached the opposite conclusion. In
Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734
(E.D. Mich. 2003), the district court denied Wells Fargo's
motion for a preliminary injunction after finding that
WhenU's inclusion of plaintiff Wells Fargo's trademarked
website address in WhenU's proprietary directory of keywords
was not "use" for purposes of the Lanham Act, and that WhenU
did not alter or interfere with Wells Fargo's website in any
manner. Id. at 757-61. The district court in U-Haul
(E.D. Va. 2003), employing a very similar analysis, granted
summary judgment in favor of WhenU after concluding that
WhenU's inclusion of U-Haul's trademarked website address in
the SaveNow directory was not actionable because it was for a
"pure machine-linking function" that was not "use" under the
Lanham Act. Id. at 728 (internal quotation marks omitted).

In the case before us, the district court's
consideration of these two comprehensive decisions on the
precise issue at hand was confined to a footnote in which it
cited the cases, summarized their holdings in parentheticals,
and concluded, without discussion, that it "disagree[d] with, and [was] not bound by these findings." 1-800 Contacts, 309 F. Supp. 2d at 490 n.43. Unlike the district court, we find the thorough analyses set forth in both U-Haul and Wells Fargo to be persuasive and compelling.

A. The SaveNow Directory

The district court held that WhenU's inclusion of 1-800's website address in the SaveNow directory constitutes a prohibited "use" of 1-800's trademark. Id. at 489. We disagree.

At the outset, we note that WhenU does not "use" 1-800's trademark in the manner ordinarily at issue in an infringement claim: it does not "place" 1-800 trademarks on any goods or services in order to pass them off as emanating from or authorized by 1-800. See U-Haul, 279 F. Supp. 2d at 728; cf. L.L. Bean, Inc. v. Drake Publishers, Inc., 811 F.2d 26, 32-34 (1st Cir. 1987); Societe Comptoir de L'Industrie Cotonniere Etablissements Boussac v. Alexander's Dep't Stores, Inc., 299 F.2d 33, 37 (2d Cir. 1962). The fact is that WhenU does not reproduce or display 1-800's trademarks at all, nor does it cause the trademarks to be displayed to a C-user. Rather, WhenU reproduces 1-800's website address, <<www.1800contacts.com>>>, which is similar, but not identical, to 1-800's 1-800CONTACTS trademark. See 1-800
Contacts, 309 F. Supp. 2d at 478-79.

The district court found that the differences between 1-800’s trademarks and the website address utilized by WhenU were insignificant because they were limited to the addition of the “www.” and “.com” and the omission of the hyphen and a space. See id. We conclude that, to the contrary, the differences between the marks are quite significant because they transform 1-800’s trademark -- which is entitled to protection under the Lanham Act -- into a word combination that functions more or less like a public key to 1-800’s website.

Moreover, it is plain that WhenU is using 1-800’s website address precisely because it is a website address, rather than because it bears any resemblance to 1-800’s trademark, because the only place WhenU reproduces the address is in the SaveNow directory. Although the directory resides in the C-user’s computer, it is inaccessible to both the C-user and the general public, see id., at 476 (noting that directory is scrambled to preclude access). Thus, the appearance of 1-800’s website address in the directory does not create a possibility of visual confusion with 1-800’s mark. More important, a WhenU pop-up ad cannot be triggered by a C-user’s input of the 1-800 trademark or the appearance of that trademark on a webpage accessed by the C-user.
Rather, in order for WhenU to capitalize on the fame and recognition of 1-800's trademark — the improper motivation both 1-800 and the district court ascribe to WhenU — it would have needed to put the actual trademark on the list.\textsuperscript{11}

In contrast to some of its competitors, moreover, WhenU does not disclose the proprietary contents of the SaveNow directory to its advertising clients nor does it permit these clients to request or purchase specified keywords to add to the directory. \textit{See GEICO v. Google, Inc.}, 330 F. Supp. 2d 700, 703-04 (E.D. Va. 2004) (distinguishing WhenU's conduct from Gator's practice of selling "keywords" to its advertising clients), \textit{claim dism'd}, Order, Dec. 15, 2004 (dismissing Lanham Act claim following bench trial on finding no likelihood of confusion); \textit{see also U-Haul}, 273 F. Supp. 2d at 728 (discussing other practices).\textsuperscript{12}

A company's internal utilization of a trademark in a way

\textsuperscript{11}This observation, however, is not intended to suggest that inclusion of a trademark in the directory would necessarily be an infringing "use." We express no view on this distinct issue.

\textsuperscript{12}We think it noteworthy that prior to filing its lawsuit against WhenU, 1-800 entered into agreements with WhenU competitors Gator and Yahoo! to have its own pop-up and banner ads delivered to C-users in response to the C-users' input of particular website addresses and keywords that were specified by 1-800. Included in the list 1-800 provided to Gator, for instance, were the website addresses for several of 1-800's competitors, including defendant-appellee Vision Direct, Coastal Contacts, and Lens Express.
that does not communicate it to the public is analogous to a
individual’s private thoughts about a trademark. Such
conduct simply does not violate the Lanham Act, which is
concerned with the use of trademarks in connection with the
sale of goods or services in a manner likely to lead to
consumer confusion as to the source of such goods or
services. See 15 U.S.C. § 1127; see also Louis Altman, 4
Callmann on Unfair Competition, Trademarks and Monopolies
not sell, but merely uses internally within his own company,
the trademarked product of another, is not a trademark
infringer or unfair competitor by virtue of such use.").

Accordingly, we conclude that WhenU’s inclusion of the
1-800 website address in its SaveNow directory does not
infringe on 1-800’s trademark.

B. The Pop-up Advertisements

The primary issue to be resolved by this appeal is
whether the placement of pop-up ads on a C-user’s screen
contemporaneously with either the 1-800 website or a list of
search results obtained by the C-user’s input of the 1-800
website address constitutes “use” under the Lanham Act, 15
U.S.C. §§ 1114(1), 1125(a). The district court reasoned that
WhenU, by “causing pop-up advertisements for Defendant Vision
Direct to appear when SaveNow users have specifically
attempted to access [1-800]’s website, . . . [is] displaying [1-800]’s mark in the . . . advertising of . . . Vision Direct’s services.” 1-800 Contacts, 309 F. Supp. 2d at 489.

The fatal flaw with this holding is that WhenU’s pop-up ads do not display the 1-800 trademark. The district court’s holding, however, appears to have been based on the court’s acceptance of 1-800’s claim that WhenU’s pop-up ads appear “on” and affect 1-800’s website. See, e.g., id. at 479 (stating that WhenU has “no relationship with the companies on whose websites the pop-up advertisements appear”) (emphasis omitted) (emphasis added). As we explained above, the WhenU pop-up ads appear in a separate window that is prominently branded with the WhenU mark; they have has absolutely no tangible effect on the appearance or functionality of the 1-800 website.

More important, the appearance of WhenU’s pop-up ad is not contingent upon or related to 1-800’s trademark, the trademark’s appearance on 1-800’s website, or the mark’s similarity to 1-800’s website address. Rather, the contemporaneous display of the ads and trademarks is the result of the happenstance that 1-800 chose to use a mark similar to its trademark as the address to its web page and to place its trademark on its website. The pop-up ad, which is triggered by the C-user’s input of 1-800’s website
address, would appear even if 1-800’s trademarks were not
displayed on its website. A pop-up ad could also appear if
the C-user typed the 1-800 website address, not as an
address, but as a search term in the browser’s search engine,
and then accessed 1-800’s website by using the hyperlink that
appeared in the list of search results.¹³

In addition, 1-800’s website address is not the only
term in the SaveNow directory that could trigger a Vision
Direct ad to “pop up” on 1-800’s website. For example, an ad
could be triggered by a C-user’s search for “contacts” or
“eye care,” both terms contained in the directory, and then
clicked on the listed hyperlink to 1-800’s website.

Exemplifying the conceptual difficulty that inheres in
this issue, the district court’s decision suggests that the
crux of WhenU’s wrongdoing -- and the primary basis for the
district court’s finding of “use” -- is WhenU’s alleged
effort to capitalize on a C-user’s specific attempt to access

¹³The Second Circuit has defined the term “search engine”
operationally:

A search engine will find all web pages on the
Internet with a particular word or phrase. Given
the current state of search engine technology, that
search will often produce a list of hundreds of web
sites through which the [C-user] must sort in order
to find what he or she is looking for.

Sporty’s Farm L.L.C. v. Sportsman’s Market, Inc., 202 F.3d
489, 493 (2d Cir. 2000).
the 1-800 website. As the court explained it,

WhenU.com is doing far more than merely "displaying" Plaintiff's mark. WhenU's advertisements are delivered to a SaveNow user when the user directly accesses Plaintiff's website--thus allowing Defendant Vision Direct to profit from the goodwill and reputation in Plaintiff's website that led the user to access Plaintiff's website in the first place.

1-800 Contacts, 309 F. Supp. 2d at 490. Absent improper use of 1-800's trademark, however, such conduct does not violate the Lanham Act. See Traffix Devices, Inc. v. Mktg. Displays, Inc., 532 U.S. 23, 29 (2001); Kellogg Co. v. Nat'l Biscuit Co., 305 U.S. 111, 122 (1938) (holding that Kellogg's sharing in the goodwill of the unprotected "Shredded Wheat" market was "not unfair"); see also William P. Kratzke, Normative Economic Analysis of Trademark Law, 21 Memphis St. U. L. Rev. 199, 223 (1991) (criticizing importation into trademark law of "unjust enrichment" and "free riding" theories based on a trademark holder's goodwill). Indeed, it is routine for vendors to seek specific "product placement" in retail stores precisely to capitalize on their competitors' name recognition. For example, a drug store typically places its own store-brand generic products next to the trademarked products they emulate in order to induce a customer who has specifically sought out the trademarked product to consider the store's less-expensive alternative. WhenU employs this same marketing strategy by informing C-users who have sought
out a specific trademarked product about available coupons, discounts, or alternative products that may be of interest to them.

1-800 disputes this analogy by arguing that unlike a drugstore, only the 1-800 website is displayed when the pop-up ad appears. This response, however, ignores the fact that a C-user who has installed the SaveNow software receives WhenU pop-up ads in a myriad of contexts, the vast majority of which are unlikely to have anything to do with 1-800 or the C-user’s input of the 1-800 website address.\(^\text{14}\)

The cases relied on by 1-800 do not alter our analysis. As explained in detail by the court in U-Haul, they are all readily distinguishable because WhenU’s conduct does not involve any of the activities those courts found to constitute “use.” U-Haul, 279 F. Supp. at 728-29 (collecting cases). Significantly, WhenU’s activities do not alter or affect 1-800’s website in any way. Nor do they divert or misdirect C-users away from 1-800’s website, or alter in any way the results a C-user will obtain when searching with the

\(^{14}\)Indeed, although we do not address the district court’s finding of a likelihood of confusion, we note that 1-800’s claim that C-users will likely be confused into thinking that 1-800 has sponsored its competitor’s pop-up ads is fairly incredulous given that C-users who have downloaded the SaveNow software receive numerous WhenU pop-up ads -- each displaying the WhenU brand -- in varying contexts and for a broad range of products.
Compare Playboy Enters., Inc. v. Netscape Communications Corp., 354 F.3d 1020, 1024 (9th Cir. 2004) (holding that infringement could be based on defendant’s insertion of unidentified banner ads on C-user’s search-results page); Brookfield Communications v. West Coast Entm’t Corp., 174 F.3d 1036 (9th Cir. 1999) (holding that defendant’s use of trademarks in “metatags,” invisible text within websites that search engines use for ranking results, constituted a “use in commerce” under the Lanham Act); see generally Bihari v. Gross, 119 F. Supp. 2d 309 (S.D.N.Y. 2000) (discussing Brookfield and similar cases).\

In addition, unlike several other internet advertising companies, WhenU does not “sell” keyword trademarks to its customers or otherwise manipulate which category-related advertisement will pop up in response to any particular terms on the internal directory. See, e.g., GEICO, 330 F. Supp. 2d at 703-04 (finding that Google’s sale to advertisers of right to use specific trademarks as “keywords” to trigger their ads constituted “use in commerce”). In other words, WhenU does not link trademarks to any particular competitor’s ads, and a

---

15We note that in distinguishing cases such as Brookfield, Playboy and Bihari, we do not necessarily endorse their holdings. See Playboy, 354 F.3d at 1034-36 (Berzon, C.J., concurring, noting disagreement with holding in Brookfield).
customer cannot pay to have its pop-up ad appear on any
specific website or in connection with any particular
trademark. See id. at 704 (distinguishing WhenU's conduct on
this basis). Instead, the SaveNow directory terms trigger
categorical associations (e.g., www.1800Contacts.com might
trigger the category of "eye care"), at which point, the
software will randomly select one of the pop-up ads contained
in the eye-care category to send to the C-user's desktop.

Perhaps because ultimately 1-800 is unable to explain
precisely how WhenU "uses" its trademark, it resorts to
bootstrapping a finding of "use" by alleging other elements
of a trademark claim. For example, 1-800 invariably refers
to WhenU's pop-up ads as "unauthorized" in an effort, it
would seem, to establish by sheer force of repetition the
element of unauthorized use of a trademark. Not
surprisingly, 1-800 cites no legal authority for the
proposition that advertisements, software applications, or
any other visual image that can appear on a C-user’s computer
screen must be authorized by the owner of any website that
will appear contemporaneously with that image. The fact is
that WhenU does not need 1-800’s authorization to display a
separate window containing an ad any more than Corel would
need authorization from Microsoft to display its WordPerfect
word-processor in a window contemporaneously with a Word
word-processing window. Moreover, contrary to 1-800's repeated admonitions, WhenU's pop-up ads are authorized -- if unwittingly -- by the C-user who has downloaded the SaveNow software.

1-800 also argues that WhenU's conduct is "use" because it is likely to confuse C-users as to the source of the ad. It buttresses this claim with a survey it submitted to the district court that purportedly demonstrates, inter alia, that (1) a majority of C-users believe that pop-up ads that appear on websites are sponsored by those websites, and (2) numerous C-users are unaware that they have downloaded the SaveNow software. 1-800 also relies on several cases in which the court seemingly based a finding of trademark "use" on the confusion such "use" was likely to cause. See, e.g., Bihari, 119 F. Supp. 2d at 318 (holding that defendant's use of trademarks in metatags constituted a "use in commerce" under the Lanham Act in part because the hyperlinks "effectively act[ed] as a conduit, steering potential customers away from Bihari Interiors and toward its competitors"); GEICO, 330 F. Supp. 2d at 703-04 (finding that Google's sale to advertisers of right to have specific trademarks trigger their ads was "use in commerce" because it created likelihood of confusion that Google had the trademark holder's authority to do so). Again, this rationale puts the
cart before the horse. Not only are "use," "in commerce," and "likelihood of confusion" three distinct elements of a trademark infringement claim, but "use" must be decided as a threshold matter because, while any number of activities may be "in commerce" or create a likelihood of confusion, no such activity is actionable under the Lanham Act absent the "use" of a trademark. 15 U.S.C. § 1114; see People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 364 (4th Cir. 2001). Because 1-800 has failed to establish such "use," its trademark infringement claims fail.

III. 1-800's Remaining Claims

In issuing the preliminary injunction, the district court expressly confined its findings in support of the injunction to 1-800's trademark infringement. Accordingly, 1-800's remaining claims, as to which we express no view, will be the subject of further proceedings on remand.

CONCLUSION

For the foregoing reasons, we reverse the district court's entry of a preliminary injunction and remand with instructions to (1) dismiss with prejudice 1-800's trademark infringement claims against WhenU, and (2) proceed with 1-800's remaining claims.
SPYWARE CONTROL ACT REVISIONS
2005 GENERAL SESSION
STATE OF UTAH

Chief Sponsor: Stephen H. Urquhart
Senate Sponsor: Curtis S. Bramble

LONG TITLE
General Description:
This bill amends the Spyware Control Act.

Highlighted Provisions:
This bill:
• defines terms;
• prohibits certain uses of pop-up advertisements;
• prohibits the purchase of pop-up advertisements that violate the chapter if the purchaser has actual notice of the violation;
• provides for the permissive removal of certain software; and
• defines the scope of actions and penalties authorized by the chapter.

Monies Appropriated in this Bill:
None

Other Special Clauses:
None

Utah Code Sections Affected:

AMENDS:
13-40-102, as enacted by Chapter 363, Laws of Utah 2004
13-40-201, as enacted by Chapter 363, Laws of Utah 2004
13-40-301, as enacted by Chapter 363, Laws of Utah 2004
13-40-302, as enacted by Chapter 363, Laws of Utah 2004

ENACTS:
13-40-202, Utah Code Annotated 1953
Be it enacted by the Legislature of the state of Utah:

Section 1. Section 13-40-102 is amended to read:


As used in this chapter:

[(a) "Context based triggering mechanism" means a software based trigger or program
residing on a consumer's computer that displays an advertisement according to:]

[(a) the current Internet website accessed by a user; or]

[(b) the contents or characteristics of the current Internet website accessed by a user.]

(1) "Cookie" means a text file:

(a) that is placed on a computer by:

(i) an interactive computer service;

(ii) an Internet website; or

(iii) a third party acting on behalf of:

(A) an interactive computer service; or

(B) an Internet website; and

(b) the function of which is to record information that can be read or recognized when
the user of the computer later accesses a particular:

(i) Internet website;

(ii) online location; or

(iii) online service.

(2) "Division" means the Division of Consumer Protection in the Department of
Commerce.

(3) "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:

(a) an Internet or online service provider; or

(b) a service or system providing access to the Internet, including a system operated by a
library or educational institution.

[(3) (4) "Internet" is as defined in the Internet Tax Freedom Act, Pub. L. No. 105-277.

[(4) Except as provided in Subsection (5), "spyware" means software residing on a computer that:

[(a) monitors the computer's usage;]

[(b) (i) sends information about the computer's usage to a remote computer or server; or]

[(ii) displays or causes to be displayed an advertisement in response to the computer's usage if the advertisement:]

[(A) does not clearly identify the full legal name of the entity responsible for delivering the advertisement;]

[(B) uses a federally registered trademark as a trigger for the display of the advertisement by a person other than:]

[(i) the trademark owner;]

[(II) an authorized agent or licensee of the trademark owner; or]

[(III) a recognized Internet search engine;]

[(C) uses a triggering mechanism to display the advertisement according to the Internet websites accessed by a user; or]

[(D) uses a context-based triggering mechanism to display the advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website; and]

[(c) does not:]

[(i) obtain the consent of the user, at the time of, or after installation of the software but before the software does any of the actions described in Subsection (4)(b);]

[(A) to a license agreement;]

[(f) presented in full; and]

[(II) written in plain language;]

[(B) to a notice of the collection of each specific type of information to be transmitted as a result of the software installation;]
[(E) to a clear and representative full-size example of each type of advertisement that may be delivered;]

[(D) to a truthful statement of the frequency with which each type of advertisement may be delivered; and]

[(E) for each type of advertisement delivered by the software, a clear description of a method by which a user may distinguish the advertisement by its appearance from an advertisement generated by other software services; and]

[(ii) provide a method:]

[(A) by which a user may quickly and easily disable and remove the software from the user's computer;]

[(B) that does not have other effects on the non-affiliated parts of the user's computer; and]

[(C) that uses obvious, standard, usual, and ordinary methods for removal of computer software;]

[(5) Notwithstanding Subsection (4), "spyware" does not include:]

[(a) software designed and installed solely to diagnose or resolve technical difficulties;]

[(b) software or data that solely report to an Internet website information previously stored by the Internet website on the user's computer, including:]

[(i) cookies;]

[(ii) HTML-code; or]

[(iii) Java Scripts; or]

[(e) an operating system;]

[(6) "Usage" means:]

[(a) the Internet websites accessed by a user;]

[(b) the contents or characteristics of the Internet websites accessed by a user;]

[(c) a user's personal information, including:]

[(i) a first and last name of a user, whether:]

[(A) given at birth or adoption;]
[B]—assumed; or

[C]—legally changed;

(ii) any of the following with respect to a user’s home or other physical address:

(A) the street name;

(B) the name of the city or town; or

(C) the zip code;

(iii) an electronic mail address;

(iv) a telephone number;

(v) a Social Security number;

(vi) any personal identification number;

(vii) a credit card number;

(viii) any access code associated with a credit card;

(ix) a date of birth, birth certificate number, or place of birth; or

(x) a password or access code; or

(d) a user’s submission to forms or Internet websites.

(5) "Internet or online service provider" means an interactive computer service that provides software or other material that enables a person to:

(a) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content;

(b) select or analyze content; or

(c) allow or disallow content.

(6) "Mark" means a registered trademark, registered service mark, or registered domain name in an Internet website address that is owned, licensed, or lawfully used by a person doing business in this state.

(7) (a) Except as provided in Subsection (7)(b), "spyware" means software on the computer of a user who resides in this state that:

(i) collects information about an Internet website at the time the Internet website is being viewed in this state, unless the Internet website is the Internet website of the person who provides
the software; and

(ii) uses the information described in Subsection (7)(a)(i) contemporaneously to display pop-up advertising on the computer.

(b) "Spyware" does not include:

(i) an Internet website;

(ii) a service operated by an Internet or online service provider accessed by a user;

(iii) software designed and installed primarily to:

(A) prevent, diagnose, or resolve technical difficulties;

(B) detect or prevent fraudulent activities; or

(C) protect the security of the user's computer from unauthorized access or alteration;

(iv) software or data that reports information to an Internet website previously stored by the Internet website on the user's computer, including cookies;

(v) software that provides the user with the capability to search the Internet; or

(vi) software installed with the consent of a user whose primary purpose is to prevent access to certain Internet content.

(8) "Pop-up advertising" means material:

(a) offering for sale or advertising the availability or quality of a commercial property, good, or service; and

(b) that is displayed:

(i) separate from an Internet website;

(ii) as a result of a user accessing an Internet website;

(iii) in a manner that covers paid advertising or other content on an Internet website in a way that interferes with the user's ability to view the advertising or other content that the user attempted to originally access; and

(iv) without the authority of the operator of the Internet website.

[f7] (f) "User" means[±] the owner or authorized user of a computer.

[(a) a computer owner; or]

[(b) a person who accesses an Internet website;]
Section 2. Section 13-40-201 is amended to read:

13-40-201. Prohibited conduct.

(1) A person may not[·] display a pop-up advertisement by means of spyware if the pop-up advertisement:

[(a) install spyware on another person's computer;]
[(b) cause spyware to be installed on another person's computer; or]
[(c) use a context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website;]

[(2) It is not a defense to a violation of this section that a user may remove or hide an advertisement.]

(a) (i) is displayed in response to a specific mark; or
(ii) is displayed in response to a specific Internet website address;
(b) constitutes infringement of a registered trademark under federal or state law; and
(c) is purchased or acquired by a person other than:
(i) the mark owner;
(ii) a licensee of the mark;
(iii) an authorized agent of the owner of the mark;
(iv) an authorized user of the mark;
(v) a person advertising the lawful sale, lease, or transfer of products bearing the mark through a secondary marketplace for the sale of goods or services; or
(vi) a person engaged in a fair or otherwise permissible use of a trademark or service mark under applicable trademark law.

(2) (a) A person using spyware to display a pop-up advertisement under Subsection (1) is not guilty of violating this chapter if:

(i) the person requests information about the user's state of residence before sending the spyware or displaying a pop-up advertisement to the user after May 2, 2005; and
(ii) the user indicates a residence outside this state.
(b) A person purchasing or acquiring advertising under Subsection 13-40-301(5) is not guilty of violating this chapter if the person reasonably determines that the person delivering a pop-up advertisement by use of spyware under Subsection (1) has complied with Subsection (2)(a).

(c) A person requesting information about a user's state of residence under Subsection (2)(a) may not prompt, ask, or otherwise encourage a user to indicate a residence outside this state.

(d) No action may be brought under this chapter for the use of a mark or Internet website address that constitutes a fair or otherwise permissible use of the mark or Internet website address under federal or state law.

Section 3. Section 13-40-202 is enacted to read:


If a provider of computer software or an interactive computer service provides prior notice to a user with whom the provider has an established business relationship, that provider is not liable under the law of this state, or a political subdivision of this state, for identifying, removing, or disabling, preventing installation of a program on the user's computer that is used to, or that the provider reasonably or in good faith believes will likely be used to:

(1) violate a provision of this chapter; or

(2) to engage in surreptitious collection of information concerning the user's use of the computer without the consent of the owner of the computer, except that no notice is required for:

(a) preventing the installation of a program; or

(b) in the case of an enterprise network, removing, disabling, or preventing the installation of a program on the computer of an employee.

Section 4. Section 13-40-301 is amended to read:

13-40-301. Private action.

(1) An action for a violation of this chapter may be brought against a person who violates Section 13-40-201 by:

[1] violates this chapter; or]
[(ii) causes a violation of this chapter; and]
[(b) by any of the following who are adversely affected by a violation of this chapter:]
[(i) an Internet website owner or registrant;]
[(ii) a trademark or copyright owner; or]
[(iii) an authorized advertiser on an Internet website.]
(a) the attorney general; or
(b) a mark owner who:
(i) does business in this state; and
(ii) is directly and adversely affected by a violation of this chapter.
(2) In an action under Subsection (1), a person may:
(a) obtain an injunction against committing any further violation of this chapter; and
(b) subject to Subsection (3), recover the greater of:
(i) actual damages; or
(ii) [$10,000] up to $500 for each separate [violation of this chapter] occurrence resulting in the display of an advertisement prohibited by Section 13-40-201.
(3) In an action under Subsection (1), a court may:
(a) increase the damages up to three times the damages allowed by Subsection (2)(b) if the court finds that the defendant willfully or knowingly violated this chapter; and
(b) award costs and reasonable attorney fees to a prevailing party.
(4) For purposes of this section, a separate violation occurs for each individual occurrence that results in the display of an advertisement described in Subsection 13-40-102[(4)(b)(ii)](8).
(5) Except as provided in Subsection 13-40-201(2)(b), an action for a violation of this chapter may be brought against a person who purchases or acquires advertising described in Subsection 13-40-201(1) if:
(a) the person against whom the action is brought receives actual notice from a mark owner of an alleged violation of Section 13-40-201;
(b) the notice required under Subsection (5)(a) contains a detailed explanation of the
alleged violation; and

(c) the person against whom the action is brought fails to take reasonable steps to stop
the violation of Subsection 13-40-201(1) described in the notice provided under Subsection
(5)(a).

(6) (a) At the time of commencement of an action for a violation of Subsection
13-40-201(1), the person filing the action shall serve a copy of any summons and complaint upon
any person against whom an action is brought under Subsection (5).

(b) A person against whom an action may be brought under Subsection (5) may intervene
in an action for a violation of Subsection 13-40-201(1) in accordance with Rule 24(c) of the Utah
Rules of Civil Procedure or Rule 24(c) of the Federal Rules of Civil Procedure.

Section 5. Section 13-40-302 is amended to read:

13-40-302. Limitations on actions.

(1) A person may not bring an action for a violation of this chapter against [an Internet
service provider for the routine transmission of] a person other than:

[(a) security information; or]

[(b) information that contains an advertisement violating this chapter.]

(a) a person who displays a pop-up advertisement by means of spyware in violation of
Subsection 13-40-301(5); or

(b) a person who purchases or acquires an advertisement in violation of Subsection
13-40-201(2).

(2) A person may not bring a class action under this chapter.

(3) This chapter does not preclude any person accused of violating this chapter from
asserting any fair use or other defense that is available to persons alleged to have engaged in
trademark infringement.
Will the adware industry beat Spitzer?

By Eric Goldman

Story last modified Tue Aug 02 04:00:00 PDT 2005

New York Attorney General Elliott Spitzer's recent enforcement action against adware vendor Intermix Media has opened up a new front in the battle against this type of software.

Though Intermix claims to have settled the matter for $7.5 million, any disposition leaves open a number of issues regarding Spitzer's ultimate plan for a possible sweep against the entire adware industry.

In particular, Spitzer has repeatedly threatened advertisers who run ads with adware vendors. These threats have created a conundrum for advertisers. On one hand, adware offers advertisers a cost-effective way to reach consumers who derive value from the advertisements. On the other hand, no advertiser wants to get on Spitzer's hit list. Thus, if Spitzer's threat is real, many advertisers will simply forgo adware advertising.

But amid the commotion, a critical, substantive question remains ignored: What legal doctrine holds advertisers liable for advertising via adware? We have yet to hear a coherent theory from Spitzer—or anyone else—explaining how this liability arises.

In fact, advertiser liability for adware vendors' actions would represent a novel and unprecedented application of current law. In other words, to hold advertisers liable, Spitzer will need to create new law.

We can better understand the radical nature of these assertions through some analogies to other advertising contexts. Imagine The New York Times runs a libelous story or illegally obtains consumer subscriptions through deceptive trade practices. Or imagine a Yellow Pages vendor illegally trespasses by throwing copies of its book onto homeowners' land.

Are advertisers liable in these circumstances? Generally, the answer is emphatically no. Advertisers have no more responsibility for the media partner's actions than any other customer or vendor. Indeed, such expansive liability might generate First Amendment concerns.

An exception is if an advertiser has sufficient knowledge of, and control over, the media partner's bad practices, which could create liability under venerable agency or conspiracy doctrines. However, the requisite level of knowledge and control is high—far higher than most

Advertiser liability for adware vendors' actions would represent a novel and unprecedented application of current law.

advertisers ever have.

Indeed, many advertisers use intermediate vendors (such as ad agencies or affiliate marketers) to manage ad placement, meaning that the advertisers themselves are often fairly removed from the media partner’s behavior.

In response, Spitzer’s office has intimated that advertisers should know that their ad dollars are finding their way to adware vendors, and further should know that adware vendors are acting illegally.

This logic is extremely unpersuasive. In fact, many adware vendors fully or substantially comply with existing law, so advertisers should hardly assume the worst. Further, even if advertisers know who might get their ad dollars, this is a far cry from the knowledge and control necessary to hold the advertiser liable for someone else’s actions.

In the spam context, Congress statutorily created a new type of advertiser liability in the 2003 Can-Spam law. Congress or state legislatures could choose to adopt a similar law for adware advertisers.

Until then, adware advertiser liability remains purely speculative. Nevertheless, the specter appears to serve Spitzer’s apparent modus operandi of attempting to starve the few truly illegal actors by cutting off their access to customers. Unfortunately, these threats veer disconcertingly close to vigilantism. Using hypothetical law to spook an industry goes far beyond a prosecutor’s role of enforcing existing law and verges into the realm normally reserved for our elected legislators.

Meanwhile, there is a collateral cost to this vigilantism. Legitimate advertisers may choose not to use legitimate adware vendors to deliver socially beneficial advertising to consumers. We would not tolerate scare-mongering in other media, like newspapers, radio or television, and we should not tolerate it in the adware context either.

Spitzer’s threats against the entire adware industry may garner popular support for him for leading the charge against “spyware,” but the threats are based on unprecedented legal theories with broad negative policy implications. We should not allow our current antipathy toward adware to blind us to the radical nature of holding customers liable for what their vendors do.

Copyright ©1995-2005 CNET Networks, Inc. All rights reserved.