Cyberspace Law (Law 793)
Eric Goldman
Fall 2007

1. **Sessions.** The course meets Mondays and Wednesdays 9:00-10:15 am in Room 110 from August 20 to November 28, except September 3 (Labor Day) and October 8 (Academic Recess).

2. **Grading.**

   **Attendance**

   In-class material and discussions are crucial to this course, so I expect you to attend every class. However, because our lives are unpredictable, you have five "free passes" for unexcused absences (no need to notify me in advance). I will excuse absences only for very good cause. Your sixth unexcused absence may trigger a significant penalty to your final course grade. At my option, I may drop you from the course or give you an F upon a seventh unexcused absence.

   **Final Exam**

   Except for any adjustments due to unexcused absences, the final exam will constitute 100% of the course grade. I am considering making the final exam a take-home exam, probably consisting of two or three essay questions with a maximum word count. If so, I would probably distribute the exam on December 5 with a due date of December 7.

   I strongly encourage you to review my past exams to understand my exam style. You can find past exams and sample answers at my website (note the law may have changed in the interim).

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

4. **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.

5. **On-campus Cyberlaw Events This Semester.** Mark your calendars!

   - Sept. 17: Blogging, Scholarship, and the Bench and Bar
   - Oct. 2: Trust and Privacy in Online Transactions
   - Oct. 23: Update on DMCA and Viacom v. Google Case
   - Nov. 1: Prof. Jonathan Zittrain of the Oxford Internet Institute and Harvard Law School
6. **Readings.**

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

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLU v. Reno (CDA I District Ct. Facts Only)</td>
<td>5</td>
</tr>
<tr>
<td>Noah v. AOL (E.D. Va.)</td>
<td>21</td>
</tr>
</tbody>
</table>

Optional: if you'd like to know more about the Internet's technical operations, you might check out the Animated Internet website.

**Jurisdiction**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toys 'R' Us v. Step Two (3d Cir.)</td>
<td>32</td>
</tr>
</tbody>
</table>

**Contracts**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specht v. Netscape Communications (2d Cir.)</td>
<td>46</td>
</tr>
<tr>
<td>Register.com v. Verio (2d Cir.) (except Trespass to Chattels Section)</td>
<td>80</td>
</tr>
</tbody>
</table>

**Trespass/CFAA**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>18 USC §1030</td>
<td>101</td>
</tr>
<tr>
<td>Intel v. Hamidi (Cal. Sup. Ct.)</td>
<td>107</td>
</tr>
<tr>
<td>Register.com v. Verio (Trespass to Chattels Section)</td>
<td>99</td>
</tr>
</tbody>
</table>

**Copyright**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright Office Circular 1</td>
<td>148</td>
</tr>
<tr>
<td>20th Century v. Cablevision</td>
<td>155</td>
</tr>
<tr>
<td>Field v. Google</td>
<td>171</td>
</tr>
</tbody>
</table>

**Subtopic: File Sharing**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 USC §506(a)</td>
<td>185</td>
</tr>
<tr>
<td>BMG v. Gonzalez (7th Cir.)</td>
<td>187</td>
</tr>
<tr>
<td>MGM Studios v. Grokster (Sup. Ct.)</td>
<td>195</td>
</tr>
</tbody>
</table>

**Subtopic: Secondary Liability**

<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 USC §512</td>
<td>219</td>
</tr>
<tr>
<td>Perfect 10 v. ccBill (9th Cir. as amended)</td>
<td>230</td>
</tr>
<tr>
<td>Perfect 10 v. Amazon (9th Cir.)</td>
<td>251</td>
</tr>
<tr>
<td>Perfect 10 v. Visa (9th Cir.)</td>
<td>295</td>
</tr>
</tbody>
</table>
Trademarks and Domain Names

Trademark FAQs ................................................................. 346
Helpful Hints to Knowing Your Trademark Terms ........................................... 348
15 USC §§1125 & 1129 (Infringement, Dilution and ACPA) ....................... 350
15 USC §1114 (Trademark Safe Harbors) ............................................. 360
Domain Name Dispute Resolution Policy and rules ................................... 364

Subtopic: Domain Names and Metatags
Lamparello v. Falwell (4th Cir.) ............................................................ 383
Promatek v. Equitrac (7th Cir.) Original Order and Revision .............. 402
Lockheed Martin v. Network Solutions (9th Cir.) ............................... 412

Subtopic: Search Engines
Keyword Law slides ............................................................................. 417
Playboy v. Netscape (9th Cir. 2004) ....................................................... 422
FragranceNet.com v. FragranceX.com ............................................... 445

Pornography
Helpful Hints to Knowing Your Porn Terms ........................................... 457
Reno v. ACLU (Sup. Ct. 1997) ................................................................. 458
Ashcroft v. ACLU (Sup. Ct. 2004) ......................................................... 478

Defamation and Information Torts
47 USC §230 (Immunization for Interactive Computer Services) ............... 510
Zeran v. America Online (4th Cir.) ......................................................... 513
Fair Housing Council v. Roommates.com (9th Cir.) ............................... 526

Privacy
16 CFR Part 312 (Regulations Implementing COPPA) ....................... 548
In re. Pharmatrak (1st Cir.) ................................................................. 554

Blogs and Social Networks
Social Networking Sites and the Law handout ........................................ 582
Blog Law slides .................................................................................... 584
Doe v. MySpace .................................................................................... 589

Spam
Where’s the Beef? Dissecting Spam’s Purported Harms ....................... 603
CAN-SPAM Act of 2003 ...................................................................... 618
16 CFR Part 316 (CAN-SPAM implementing regulations) .............. 639
MySpace v. TheGlobe.com ................................................................. 646
Omega World Travel v. Mummagraphics (4th Cir.) ........................................ 657

Adware/Spyware

Spyware: Background and Policy Issues for Congress (July 17, 2006 version) .................. 674

7. CONTACT INFORMATION.

Eric Goldman
Santa Clara University School of Law, Bergin 206
500 El Camino Real
Santa Clara, CA 95053
Phone: 408-554-4369
Email: egoldman@scu.edu

In all emails to me related to this course, please put the word “cyberlaw” in the subject line to 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.

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

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

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

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

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

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

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

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

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

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

18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including the members of plaintiff Commercial Internet Exchange Association -- are commercial entities offering Internet access for a monthly or hourly fee. Some Internet service providers, however, are non-profit organizations that offer free or very low cost access to the Internet. For example, the International Internet Association offers free modem access to the Internet upon request. Also, a number of trade or other non-profit associations offer Internet access as a service to members.
19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States.

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

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

Methods to Communicate Over the Internet

22. Once one has access to the Internet, there are a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:
   1. one-to-one messaging (such as "e-mail"),
   2. one-to-many messaging (such as "listserv"),
   3. distributed message databases (such as "USENET newsgroups"),
   4. real time communication (such as "Internet Relay Chat"),
   5. real time remote computer utilization (such as "telnet"), and
   6. remote information retrieval (such as "ftp", "gopher," and the "World Wide Web").

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

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

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

25. Distributed message databases. Similar in function to listservs -- but quite different in how communications are transmitted -- are distributed message databases such as "USENET newsgroups." User-sponsored newsgroups are among the most popular and widespread applications of Internet services, and cover all imaginable topics of interest to users. Like listservs, newsgroups are open discussions and exchanges on particular topics. Users, however, need not subscribe to the discussion mailing list in advance, but can instead access the database at any time. Some USENET newsgroups are "moderated" but most are open access. For the moderated newsgroups, 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:
o THE NATURE OF CYBERSPACEx
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.
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. Microsystems is also offering its PICS client test program for Windows free of charge. The client program can be used by developers of PICS rating services to test their services and products.

**SurfWatch**

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

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

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

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

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

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

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

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

**Content on the Internet**

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

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

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

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

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

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

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

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

**Sexually Explicit Material On the Internet**

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

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

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

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

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

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

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

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

Obstacles to Age Verification on the Internet

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

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

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

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

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

95. Unlike other forms of communication on the Internet, there is technology by which an operator of a World Wide Web server may interrogate a user of a Web site. An HTML document can include a fill-in-the-blank "form" to request information from a visitor to a Web site, and this information can be transmitted back to the Web server and be processed by a computer program, usually a Common Gateway Interface (cgi) script. The Web server could then grant or deny access to the information sought. The cgi script is the means by which a Web site can process a fill-in form and thereby screen visitors by requesting a credit card number or adult password.
96. Content providers who publish on the World Wide Web via one of the large commercial online services, such as America Online or CompuServe, could not use an online age verification system that requires cgi 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 Kirosi Kuromiya testified that it would be impossible for his organization, Critical Path, to review all of its material because it has only one full and one part-time employee.

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

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

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

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

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

The Problems of Offshore Content and Caching

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

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

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

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

Anonymity

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

Plaintiffs' Choices Under the CDA

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

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

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.
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 "Aristotle1" wrote "islam is meaniglessssss thought," "allahsdick cut offffffff," "dumballah bastard," "allah assssshole," "allajis dick is in holy dick place hey." "FUCK ALLAH," etc.


(iii) On November 4, 1998, "Hefedchefe" wrote "SMELLY TOWEL HEADS" and "MUSLIM TOWEL HEADS."

(iv) On July 11, 1999, "Izingher" 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
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. <section> 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
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. 2000(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

(4) 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. 2000(a(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).


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. <section> 12182 (prohibiting discrimination in any place of public accommodation on the basis of disability); <section> 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 Carparks Distribution Center, Inc. v. Automotive Wholesaler's 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 <section> 1218(7) is that a public accommodation is a physical place," because "[e]very term listed in <section> 12181(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 <section> 12181(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 Carparks 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. <section> 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 Carparks 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 Carparks 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. Actna 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 "[t]o expand 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. <section> 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 <section> 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 <section> 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 Zeran, 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.
PRCEDEENTIAL

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. WEISEN
HEATHER C. WILDE
Darby & Darby
805 Third Avenue
New York, NY 10022

Counsel for Appellants

SUSAN H. PARINA
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 Imaginariun 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. § 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 Imaginariun Toy Centers, Inc., which owned and operated a network of "Imaginariun" stores for the sale of educational toys and games. As part of this acquisition, Toys acquired several Imaginariun trademarks, and subsequently filed applications for the registration of additional Imaginariun marks. Prior to Toys' acquisition, the owners of the Imaginariun mark had been marketing a line of educational toys and games since 1985 and had first registered the Imaginariun mark with the United States Patent and Trademark Office in 1989. Toys currently owns thirty-seven freestanding Imaginariun stores in the U.S., of which seven are located in New Jersey. In addition, there are Imaginariun 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 "Imaginariun" in Spain and nine other countries. It first registered the Imaginariun mark in Spain in 1991, and opened its first Imaginariun store in the Spanish city of Zaragoza in November 1992. Step Two began expanding its chain of Imaginariun stores by means of a franchise system in 1994. It has registered the Imaginariun mark in several other countries where its stores are located. There are now 165 Step Two Imaginariun 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 Imaginariun 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,
Pelix 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 web site featuring
merchandise sold at Imaginarium stores. In 1996, Step Two
registered the domain name <imaginarium.ca>, 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 web site 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 web sites are
maintained by Imaginarium Net, S.A., 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 web sites, 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 web
sites provide a contact phone number within Spain that

1. Step Two maintains that goods have been available for purchase via
its web site 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 PsNet 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
PsNet Europe to maintain these domain names, and does not send any
payments to NSI. (JA 314.)

3. The web sites at <imaginariumnet.com> and <imaginariumnet.net>
were not used to sell merchandise. Discovery may be necessary to
determine whether Step Two has changed its web sites 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.4 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.) Toys, however, adduced evidence of two sales to residents of New Jersey conducted via Step Two’s Imaginarium web sites. These purchases were initiated by Toys. 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 Toys. 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 Imaginariat, 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
(quoting Burger King Corp., 471 U.S. at 475). Second, jurisdiction exists only if its exercise "comports with traditional notions of fair play and substantial justice," i.e., the defendant "should reasonably anticipate being haled into court" in that forum. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

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.

7

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 Con 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 "purposely 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.5

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) PSPS, 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 756, 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[,] and 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 412; 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 1025, 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 plaintiffs' "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 web site, 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 on [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 facilitateStep 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) P&S, 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.8

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

8. In its brief on appeal, Step Two contends that Toys should not be allowed discovery because there is simply no basis for believing that there are any other contacts to find and, moreover, seeking discovery about other websites-generated contacts would be futile as Step Two does not keep track of billing addresses or the physical location of its email correspondents. At oral argument, however, counsel for Toys suggested there are means by which an individual’s residence can be determined from a credit card number. Toys also suggests, in its brief on appeal, that the residence of on-line purchasers may be determined from the phone number that purchasers are required to input. These possibilities can be explored through discovery.

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:

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
Decided: October 1, 2002

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

__________________________________________

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.

__________________________________________

Before: McLAUGHLIN, LEVAL, and SOTOMAYOR, Circuit Judges.

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.


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,² 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 “applied 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://www.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 installation3 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\(^3\) 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\(^*\) and that “all disputes relating to this Agreement
(excepting 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

\(^3\) 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 terms

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.²

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

² 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).
DISCUSSION

I. Standard of Review and Applicable Law

A district court's denial of a motion to compel arbitration is reviewed de novo. Collins & Aikman Prods. Co. v. Bldg. Sys., Inc., 58 F.3d 16, 19 (2d Cir. 1995). The determination of whether parties have contractually bound themselves to arbitrate a dispute—a determination involving interpretation of state law—is a legal conclusion also subject to de novo review. Chelsea Square Textiles, Inc. v. Bombay Dyeing & Mfg. Co., Ltd., 189 F.3d 289, 295 (2d Cir. 1999); see also Shann v. Dunk, 84 F.3d 73, 77 (2d Cir. 1996) ("The central issue—whether based on the factual findings, a binding contract existed—is a question of law that we review de novo."). The findings upon which that conclusion is based, however, are factual and thus may not be overturned unless clearly erroneous. Chelsea Square Textiles, 189 F.3d at 295.

If a court finds that the parties agreed to arbitrate, it should then consider whether the dispute falls within the scope of the arbitration agreement. Genesco, Inc. v. T. Kakiuchi & Co., Ltd., 815 F.2d 840, 844 (2d Cir. 1987). A district court's determination of the scope of an arbitration agreement is reviewed de novo. Oldroyd v. Elmira Sav. Bank, FSB, 134 F.3d 72, 76 (2d Cir. 1998). In addition, whether a party may be compelled to arbitrate as a result of direct benefits that he or she allegedly received under a contract entered into by others is an issue of arbitrability that is reviewed de novo. Cf. Smith/Enron Cogeneration Ltd P'ship, Inc. v. Smith Cogeneration Int'l, Inc., 198 F.3d 88, 95 (2d Cir. 1999) ("[W]hether an entity is a party to the arbitration agreement . . . is included within the broader issue of whether the parties agreed to arbitrate.").

The FAA provides that a "written provision in any . . . contract evidencing a
transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract.” 11 9 U.S.C. § 2. It is well settled that a court may not compel arbitration until it has resolved “the question of the very existence” of the contract embodying the arbitration clause. Interocian Shipping Co. v. Nat’l Shipping & Trading Corp., 462 F.2d 673, 676 (2d Cir. 1972). “[A]rbitration is a matter of contract and a party cannot be required to submit to arbitration any dispute which he has not agreed so to submit.” AT & T Techs., Inc. v. Communications Workers of Am., 475 U.S. 643, 648 (1986) (quotation marks omitted). Unless the parties clearly provide otherwise, “the question of arbitrability—whether an agreement creates a duty for the parties to arbitrate the particular grievance—is undeniably an issue for judicial determination.” Id. at 649.

The district court properly concluded that in deciding whether parties agreed to arbitrate a certain matter, a court should generally apply state-law principles to the issue of contract formation. Mohler v. Terminix Int’l Co., 205 F.3d 44, 48 (2d Cir. 2000); see also Perry v. Thomas, 482 U.S. 483, 492 n.9 (1987) (“[S]tate law, whether of legislative or judicial origin, is applicable [to the determination of whether the parties agreed to arbitrate] if that law arose to

11 The parties do not dispute, nor could they, that the software license agreement at issue “involv[ed] commerce” within the meaning of 9 U.S.C. § 2, see Allied-Bruce Terminix Cos., Inc. v. Dobson, 513 U.S. 265, 273-74 (1995) (construing the broad phrase “involving commerce” to be the functional equivalent of “affecting commerce”), or that the agreement is a “written provision” despite being provided to users in a downloadable electronic form. The latter point has been settled by the Electronic Signatures in Global and National Commerce Act (“E-Sign Act”), Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. §§ 7001 et seq.), which provides that “a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.” Id. § 7001(a)(1); see also Cal. Civ. Code § 1633.7(b) (“A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.”).
govern issues concerning the validity, revocability, and enforceability of contracts generally."). Therefore, state law governs the question of whether the parties in the present case entered into an agreement to arbitrate disputes relating to the SmartDownload license agreement. The district court further held that California law governs the question of contract formation here; the parties do not appeal that determination.

II. 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. "It 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."). Mutual

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, *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."); iLAN 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 ("When 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

been adopted by two states, Maryland and Virginia. *See Md. Code Ann. Com. Law §§ 22-101 et seq.; Va. Code Ann. §§ 59.1-501.1 et seq. 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. 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
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.\textsuperscript{16} See, e.g., \textit{Hotmail Corp. v. Van}\$\textsuperscript{8} \textit{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); \textit{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); \textit{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”); \textit{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. \textit{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

\textsuperscript{16} Defendants place great importance on \textit{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. \textit{Id.} at 248. But \textit{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.  

...the reference to them would be called to the attention of an ordinary reasonable person." *Id.* § 211 cmt. 3. The commentary also approves of prominent hypertext links that draw attention to the existence of a standard agreement and allow users to view the terms of the license. *Id.*

We hasten to point out that UCITA, which has been enacted into law only in Maryland and Virginia, does not govern the parties' transactions in the present case, but we nevertheless find that UCITA's provisions offer insight into the evolving online "circumstances" that defendants argue placed plaintiffs on inquiry notice of the existence of the SmartDownload license terms. UCITA has been controversial as a result of the perceived breadth of some of its provisions. Compare Margaret Jane Radin, *Humans Computers, and Binding Commitment*, 75 Ind. L.J. 1125, 1141 (2000) (arguing that "UCITA's definition of manifestation of assent stretches the ordinary concept of consent"), *with* Joseph H. Sommer, *Against Cyberlaw*, 15 Berkeley Tech. L.J. 1145, 1187 (2000) ("There are no new legal developments [in UCITA's assent provisions]. The revolution—if any—occurred with [Karl] Llewellyn's old Article 2, which abandoned most formalisms of contract formation, and sought a contract wherever it could be found."). Nonetheless, UCITA's notice and assent provisions seem to be consistent with well-established principles governing contract formation and enforcement. See Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. Rev. 429, 491 (2002) ("[W]e contend that UCITA maintains the contextual, balanced approach to standard terms that can be found in the paper world.").

---

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 Assoc., Inc. v. Jameson, 102 F.3d 60, 65 (2d Cir. 1996) (quotation marks omitted).

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

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 those 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 Shimbun, Inc. v. Comtline 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 disclaimer 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
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 "Once 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
UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2000


Docket No. 00-9596

REGISTER.COM, INC.,

Plaintiff-Appellee,

-v.-

VERIO, INC.,

Defendant-Appellant.

Before: LEVAL, Circuit Judge, and J. F. KEENAN, District Judge.*

Appeal by defendant Verio, Inc. from preliminary injunction granted by the United States District Court for the Southern District of New York (Jones, J.) on motion of plaintiff Register.com, Inc., a registrar of Internet domain names. The order enjoined the defendant from using the plaintiff's mark in communications with prospective customers, accessing plaintiff's computers by use of software programs performing multiple automated, successive queries, and using contact information relating to recent registrants of Internet domain names ("WHOIS information") obtained from plaintiff's computers for mass solicitation. AFFIRMED.

WILLIAM F. PATRY, New York, NY (Kenneth A. Plevan, Scott D. Brown, Paul M. Fakler, on the brief), for Appellee.

* The Honorable John F. Keenan, United States District Judge for the Southern District of New York, sitting by designation. The Honorable Fred I. Parker was a member of the panel but died on August 12, 2003. Judge Parker would have voted to reverse the district court's order. This appeal is being decided by the two remaining members of the panel, who are in agreement. See Local Rule § 0.14(b).
Michael A. Jacobs, San Francisco, CA,
(James E. Hough, Mark David McPherson, on the
brief) for Appellant.

Leval, Circuit Judge:

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 § IL.F.1.

Section IL.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 relics) 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 § ILS.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.” 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 . . . advertising 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. Register 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 § ILS.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:

[E]nforcement 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 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 § I.F.5.

\[^3\] 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 § I.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
U.S. Code collection

TITLE 18 > PART I > CHAPTER 47 > § 1030
§ 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
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;

(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—

(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

(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)(iii), 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 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 Guillery 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 Kieske 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
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. 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.” (Thifty-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. c, 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 dispossession) 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\textsuperscript{4} from a company’s publicly accessible Web site is a trespass on the

\begin{footnote}
\textsuperscript{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,
\end{footnote}

(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

(Footnote continued from previous page.)

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 *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*,

15
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. c, 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. supra 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.
continue to mark out anticommons 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 Censte, 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 & Brown opinions 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 ‘[c]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.

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 UFLJTPL 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. ... [4] 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
intermeddling with or use of or damages to the personal property.”

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 “bootstrapp[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

\footnotesize{\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 overwhelms Internet
service providers. Corporate tech staff’s 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. . . . [\textsuperscript{1}] ‘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 <http://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},
L.A. Times (Apr. 21, 2003) p. B13, col. 5 [“Spam now costs American businesses
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,”4 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.\footnote{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.}

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. (\textit{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. . . .”]; \textit{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: “[t]he 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 \textit{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”]; \textit{Cyber Promotions, Inc. v. America Online, Inc.}}
(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
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.

*NOTE: Sound recordings are defined in the law as "works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work." Common examples include recordings of music, drama, or lectures. A sound recording is
Copyright Basics

not the same as a phonorecord. A phonorecord is the physical object in which works of authorship are embodied. The word “phonorecord” includes cassette tapes, CDs, LPs, 45 r.p.m. disks, as well as other formats.

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 38a, Highlights of Copyright Amendments Contained in the Uruguay Round Agreements Act (URAA- BATT), 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  
6. motion pictures and other audiovisual works  
7. sound recordings  
8. 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 388 and see the "Notice of Copyright" section on page 4 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 or 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 of 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 be 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 38a.

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."

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;

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: © 2006 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: © 2006 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 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 the work will defeat a claim of 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: © 2006 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 © 2006 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 was 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 is generally computed in the same way as for works created on or after January 1, 1978: the life-plus-70 or 95-year term applies to them as well. The law provides that in no case would 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.
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 as 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.

*NOTE: 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, go to the U.S. Customs and Border Protection website at www.cbp.gov/xp/cgov/import. Click on "Intellectual Property Rights."

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 SE
Washington, DC 20559-6000

1 A properly completed application form.

2 A nonrefundable filing fee* 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 at all possible, when sending multiple works, place all applications, deposits, and fees in the same package. If it is not possible to fit everything in one package, number each package (e.g., 1 of 3; 2 of 4) to facilitate processing and, where possible, attach applications to the appropriate deposits.

*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 408 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:
In March 2006, Cablevision Systems Corporation ("Cablevision") announced that it would be rolling out a "new Remote-Storage DVR System" (the "RS-DVR"). The RS-DVR is intended for Cablevision customers who do not have a digital video recorder ("DVR") in their homes. The RS-DVR would permit these customers to record programs on central servers at Cablevision's facilities and play the programs back for viewing at home.
Cablevision has not obtained permission from plaintiffs, the owners of the copyrighted programs, to reproduce and transmit the programs through its proposed RS-DVR. It contends that a license is not required because the customer, not Cablevision, chooses the content and records the programs for personal viewing. It argues that, under Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), a company cannot be liable for infringement merely because it supplies Betamax recorders, video cassette recorders ("VCRs"), or DVRs to consumers to record television programs for in-home, personal viewing, and it further contends that its RS-DVR is no different from these traditional devices.

In these related cases, plaintiffs sue Cablevision and its parent, CSC Holdings, Inc. ("CSC"), for copyright infringement, seeking a declaratory judgment that Cablevision's RS-DVR would violate their copyrights and an injunction enjoining defendants from rolling out the RS-DVR without copyright licenses. Defendants counterclaim for a declaratory judgment holding that the RS-DVR would not infringe on plaintiffs' copyrights. The parties' cross-motions for summary judgment are before the Court.

Plaintiffs' motions are granted and defendants' motion is denied, for I conclude that Cablevision, and not just its customers, would be engaging in unauthorized reproductions and transmissions of plaintiffs' copyrighted programs under the RS-DVR. Indeed, the RS-DVR is not a stand-alone machine that
sits on top of a television. Rather, it is a complex system that involves an ongoing relationship between Cablevision and its customers, payment of monthly fees by the customers to Cablevision, ownership of the equipment remaining with Cablevision, the use of numerous computers and other equipment located in Cablevision's private facilities, and the ongoing maintenance of the system by Cablevision personnel. Accordingly, judgment will be entered in favor of plaintiffs.

STATEMENT OF THE CASE

A. The Facts

As the parties agree, the facts are largely undisputed. (Tr. 9, 194)¹

1. The Parties

Plaintiffs, counterclaim-defendants, and third-party defendants are The Cartoon Network LP, LLLP; Cable News Network LP, LLLP; Turner Broadcasting System, Inc.; Turner Network Sales, Inc.; Turner Classic Movies, L.P., LLLP; Turner Network Television LP, LLLP; Twentieth Century Fox Film Corporation; Universal City Studios Productions LLLP; Paramount Pictures Corporation; Disney Enterprises, Inc.; CBS Broadcasting Companies, Inc.; and NBC Studios, Inc. (collectively, "plaintiffs"). Plaintiffs own the copyrights to numerous copyrighted entertainment programs, including movies, television

¹ "Tr." refers to the transcript of the hearing and oral argument on October 31 and November 1, 2006.
The nonmoving party may not rest upon mere conclusory allegations or denials, but must set forth "concrete particulars" showing that a trial is needed. *Nat'l Union Fire Ins. Co. v. Deloach*, 708 F. Supp. 1371, 1379 (S.D.N.Y. 1989) (quoting *R.G. Group, Inc. v. Horn & Hardart Co.*, 751 F.2d 69, 77 (2d Cir. 1984) (internal quotations omitted)). Accordingly, it is insufficient for a party opposing summary judgment "merely to assert a conclusion without supplying supporting arguments or facts." *BellSouth Telecomms., Inc. v. W.R. Grace & Co.*, 77 F.3d 603, 615 (2d Cir. 1996) (internal quotations omitted).

A court faced with cross-motions for summary judgment need not "grant judgment as a matter of law for one side or the other," but "must evaluate each party's motion on its own merits, taking care in each instance to draw all reasonable inferences against the party whose motion is under consideration." *Henslein, Inc. v. United States*, 996 F.2d 1455, 1461 (2d Cir. 1993) (quoting *Schwabenbauer v. Bd. of Ed. of Olean*, 667 F.2d 305, 313-14 (2d Cir. 1981) (internal citations omitted)).

**B. Copyright Infringement**

The Copyright Act of 1976 (the "Copyright Act"), 17 U.S.C. § 101 et seq., confers upon copyright owners the exclusive rights to, among other things, "reproduce the copyrighted work in copies" and "in the case of . . . audiovisual works, to perform the copyrighted work publicly." *Id.* §§ 106(1) and (4) (2002).

"To establish a claim of copyright infringement, a plaintiff must establish (1) ownership of a valid copyright and (2) unauthorized

Here, it is undisputed that plaintiffs own valid copyrights for the television programming at issue. The only question before the Court is whether Cablevision is "copying" plaintiffs' copyrighted programming or otherwise violating plaintiffs' rights under the Copyright Act.

Plaintiffs allege that Cablevision, through its RS-DVR, directly infringes upon their copyrights in two ways: one, Cablevision makes unauthorized copies of plaintiffs' programming, in violation of plaintiffs' right to reproduce their work; and two, Cablevision makes unauthorized transmissions of plaintiffs' programming, in violation of plaintiffs' exclusive right to publicly perform their work. I address each argument in turn.

1. **Is Cablevision Making Unauthorized Copies?**

   According to plaintiffs, Cablevision makes multiple unauthorized copies of programming in two respects: (1) a complete copy of a program selected for recording is stored indefinitely on the customer's allotted hard drive space on the Arroyo server at Cablevision's facility; and (2) portions of programming are stored temporarily in buffer memory on Cablevision's servers.
i. Arroyo Server Copies

Cablevision does not deny that these copies are made in the operation of the RS-DVR, but, as the parties agree, the question is who makes the copies. Cablevision sees itself as entirely passive in the RS-DVR's recording process -- it is the customer, Cablevision contends, who is "doing" the copying. To Cablevision, the RS-DVR is a machine, just like a VCR, STS-DVR, or a photocopier. Relying on Sony and other cases, Cablevision argues that it cannot be liable for copyright infringement for merely providing customers with the machinery to make copies. At most, it contends, its role with respect to the RS-DVR establishes indirect infringement, but plaintiffs have waived such a claim. (See June 7, 2006 Order). Plaintiffs, on the other hand, allege direct infringement -- that is, they claim that it is Cablevision that is "doing" the copying here. Plaintiffs characterize the RS-DVR as a service -- one that requires the continuing and active involvement of Cablevision.

I agree with plaintiffs. The RS-DVR is clearly a service, and I hold that, in providing this service, it is Cablevision that does the copying.

In Sony, programming owners sued Sony and others for copyright infringement based on defendants' marketing and sale of Betamax VCRs. The record showed that consumers primarily used VCRs for home "time-shifting" -- the practice of recording a program to view it at a later time, then erasing it. The Supreme
Court held that time-shifting is "fair use"⁷ and does not violate the Copyright Act. 464 U.S. at 456. The Court held that Sony's manufacture of Betamax VCRs therefore did not constitute contributory infringement.

Cablevision's reliance on Sony is misguided. First, Cablevision has waived any arguments based on fair use. (See June 7, 2006 Order). Second, apart from their time-shifting functions, the RS-DVR and the VCR have little in common, and the relationship between Cablevision and potential RS-DVR customers is significantly different from the relationship between Sony and VCR users.

⁷ The "fair use" defense, set forth in § 107 of the Copyright Act, provides in relevant part:

[T]he fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching . . . , scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

A VCR is a stand-alone piece of equipment. A consumer purchases the VCR and owns it outright. The consumer can then pick the VCR up, transport it, connect it to someone else's television and, assuming both devices are in working order, record programming. The RS-DVR does not have that stand-alone quality. An RS-DVR customer would not be able to disconnect his or her home set-top box, connect it elsewhere, and record programming. This is because the RS-DVR is not a single piece of equipment; it consists of a multitude of devices and processes. Unlike a VCR, the simple push of a button by the RS-DVR customer does not produce a recording. The pushing of the "record" button on the remote control merely sends a request to Cablevision's head-end to set the recording process in motion. The various computers and devices owned and operated by Cablevision and located at its head-end are needed to produce a recording.

Indeed, ownership of the RS-DVR set-top box remains with Cablevision and the RS-DVR requires a continuing relationship between Cablevision and its customers. In Sony, "[t]he only contact between Sony and the users of the Betamax . . . occurred at the moment of the sale." 464 U.S. at 438. In stark contrast, Cablevision would not only supply a set-top box for the customer's home, but it would also decide which programming channels to make available for recording and provide that content, and it would house, operate, and maintain the rest of the equipment that makes the RS-DVR's recording process possible. Cablevision has physical control of the equipment at
its head-end, and its personnel must monitor the programming streams at the head-end and ensure that the servers are working properly. (Tr. 52-54, 75-76). Cablevision determines how much memory to allot to each customer and reserves storage capacity for each on a hard drive at its facility, and customers may very well be offered the option of acquiring additional capacity -- for a fee. On the other hand, once Sony sells a VCR to a customer, Sony need not do anything further for the VCR to record.

The ongoing participation by Cablevision in the recording process also sets the RS-DVR apart from the STS-DVR. Cablevision claims that with both, the customer is "doing" the copying, and it points to the fact that no programmer . . . has ever sued Cablevision or any other cable operator in connection with its providing set-top storage DVRs to its customers (Defs. Mem. at 16). By extension, the RS-DVR, it argues, presents no copyright infringement.

This argument is unavailing. The fact that plaintiffs and other programming owners have not sued cable operators over the legality of STS-DVRs does not insulate the RS-DVR from such a challenge. Cablevision has not asserted any affirmative defenses to that effect, nor have plaintiffs conceded the legality of STS-DVRs. In any event, Cablevision's attempt to analogize the RS-DVR to the STS-DVR fails. The RS-DVR may have the look and feel of an STS-DVR (seeDefs. Ex. 101), but "under the hood" the two types of DVRs are vastly different. For example, to
effectuate the RS-DVR, Cablevision must reconfigure the linear channel programming signals received at its head-end by splitting the APS into a second stream, reformatting it through clamping, and routing it to the Arroyo servers. The STS-DVR does not require these activities. The STS-DVR can record directly to the hard drive located within the set-top box itself; it does not need the complex computer network and constant monitoring by Cablevision personnel necessary for the RS-DVR to record and store programming.

The RS-DVR, contrary to defendants' suggestions, is more akin to VOD than to a VCR, STS-DVR, or other time-shifting device. In fact, the RS-DVR is based on a modified VOD platform. (Hartson Report ¶ 114; Tr. 82). With both systems, Cablevision decides what content to make available to customers for on-demand viewing. The programming available for viewing is stored outside the customer's home at Cablevision's head-end. Both utilize a "session resource manager," such as the eSRM used by the RS-DVR, to set up a temporary pathway to deliver programming in encrypted form to the customer for playback; decryption information is transmitted in both systems to the customer's set-top box. (Hartson Report ¶ 120). The number of available pathways for programming delivery in both systems is limited; if there are none available, the customer gets an error message or busy signal. (Id.). Thus, in its architecture and delivery method, the RS-DVR bears striking resemblance to VOD -- a service that Cablevision provides pursuant to licenses negotiated with

- 26 -
programming owners. (See Tr. 84-85).

Defendants cite a host of cases to buttress their argument that the RS-DVR is not a service like VOD, but a machine that allows customers to engage in copying. None of these cases is helpful to defendants. For example, defendants cite two cases for the proposition that a company that makes copiers available to the public on its premises is not subject to liability for direct infringement unless the company's employees do the copying themselves. See Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522 (S.D.N.Y. 1991); Princeton Univ. Press v. Michigan Document Servs., Inc., 99 F.3d 1381 (6th Cir. 1996). In both cases college professors provided copyrighted material to a copy center, which assembled the material into "coursepacks" and sold them to students without paying royalties or obtaining permission from the copyright holders, and in both cases the copy center was found directly liable for infringement.

Here, Cablevision would have a similarly active role. Cablevision, through its RS-DVR, would not merely house copying machinery on its premises for customers to engage in copying. Rather, Cablevision would be "doing" the copying, notwithstanding that the copying would be done at the customer's behest, and Cablevision would provide the content being copied. These cases and others cited by defendants are thus inapposite. See also RCA Records v. All-Fast Sys., Inc., 594 F. Supp. 335, 338 (S.D.N.Y. 1984) (holding retail copy service that operated cassette copying
machine used to copy copyrighted sound recordings liable for
direct infringement, even though copies were made at request of
customers).

Cablevision also relies, to no avail, on Religious
1361 (N.D. Cal. 1995), and subsequent cases brought against
Internet service providers ("ISPs") for copyright infringement
committed by their customers. In Netcom, an individual posted
copyrighted material in a message on a computer bulletin board
service ("BBS"). By operation of the ISP's software, the posting
to the BBS automatically resulted in the copying of the message
to the ISP's computers, where the copies were stored briefly.
The court declined to find the ISP liable for direct infringement
based on these copies, concluding that it is virtually impossible
for an ISP to filter out infringing data. This conclusion was
premised on the unique attributes of the Internet, for "the court
[did] not find workable a theory of infringement that would hold
the entire Internet liable for activities that cannot reasonably
be deterred. Billions of bits of data flow through the Internet
and are necessarily stored on servers throughout the network."
Id. at 1372.

Cablevision, however, is not similarly situated to an
ISP. Cablevision is not confronted with the free flow of
information that takes place on the Internet, which makes it
difficult for ISPs to control the content they carry.
Cablevision has unfettered discretion in selecting the
programming that it would make available for recording through
the RS-DVR and is the driving force behind the RS-DVR's recording
and playback functions. Indeed, at one point Cablevision
considered limiting the RS-DVR to just twelve or fifty channels
before deciding on including all 170 channels. This situation is
a far cry from the ISP's role as a passive conduit in Netcom.
Furthermore, the copies made to the ISP's computers in Netcom
were incidental to the ISP's providing Internet access. The
copies that would be made through the RS-DVR, in contrast, are
instrumental to the RS-DVR's operation. Defendants' reliance on
Netcom and its progeny is therefore misplaced.

On the record before the Court, a reasonable factfinder
could only conclude that the copying at issue -- the copying of
programming to the RS-DVR's Arroyo servers -- would be done not
by the customer but by Cablevision, albeit at the customer's
request. This copying would, as a matter of law, constitute
copyright infringement.

ii. Buffer "Copies"

Defendants deny that the portions of programming
temporarily stored in buffer memory during the RS-DVR's operation
are "copies" for purposes of the Copyright Act. Under the
Copyright Act, "copies" are defined as:

[M]aterial objects... in which a work is
fixed by any method now known or later
developed, and from which the work can be
perceived, reproduced, or otherwise
communicated, either directly or with the aid
of a machine or device. The term "copies"
includes the material object . . . in which the work is first fixed.


The buffer copies here, defendants contend, cannot be considered infringing copies because they are "not fixed" and are "otherwise de minimis." (Defs. Mem. at 29). The Copyright Act, however, provides that a work is "fixed" if it "is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." Id. Here, as discussed, the portions of programming residing in buffer memory are used to make permanent copies of entire programs on the Arroyo servers. Clearly, the buffer copies are capable of being reproduced. Furthermore, the buffer copies, in the aggregate, comprise the whole of plaintiffs' programming. For instance, while it is true that only three frames of each program carried on the linear channels are resident in the primary ingest buffer at any given time, ultimately, however, the entire programming content for each channel will pass through the primary ingest buffer. The aggregate effect of the buffering that takes place in the operation of the RS-DVR can hardly be called de minimis.

Furthermore, numerous courts have held that the transmission of information through a computer's random access memory or RAM, as is the case with the buffering here, creates a "copy" for purposes of the Copyright Act. See, e.g., Stenograph L.L.C. v. Bossard Assoc., Inc., 144 F.3d 96, 100 (D.C. Cir. 1998) (loading of software into RAM is "copying"); Triad Sys. Corp. v.
Southeastern Express Co., 64 F.3d 1330, 1335 (9th Cir. 1995)
(same); MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519
(9th Cir. 1993) (same); Marobie-FL., Inc. v. Nat'l Ass'n of Fire
(downloading of file from website constitutes "copying" by host
computer, where portions of file pass through RAM before being
immediately transmitted over Internet).

Indeed, the United States Copyright Office, in its
August 2001 report on the Digital Millennium Copyright Act⁸
("DMCA Report"),⁹ has indicated that buffer copies are "copies"
within the meaning of the Copyright Act. Specifically, the
Copyright Office concluded that temporary copies of a work in RAM
are generally "fixed" and thus constitute "copies" within the
scope of the copyright owner's right of reproduction, so long as
they exist for a sufficient amount of time to be capable of being
copied, perceived or communicated. (DMCA Report at xxii, 110-
11).

Because I conclude that Cablevision, through operation
of its proposed RS-DVR, would "copy" plaintiffs' programming both
in the Arroyo servers and in buffer memory, in violation of
plaintiffs' exclusive right of reproduction under the Copyright
Act, summary judgment is granted in favor of plaintiffs in this

---

⁸ The DMCA was enacted into law in October 1998 to bring
copyright law in line with the digital age. See S. Rep. No. 105-

⁹ See U.S. Copyright Office, DMCA Section 104 Report, at
reports/studies/dmca/dmca_study.html.
respect. Cablevision is hereby enjoined from so copying plaintiffs' copyrighted works, unless it obtains a license to do so.

2. **Is Cablevision Making Unauthorized Transmissions?**

   As discussed, for the RS-DVR to work, the programming stream that Cablevision receives at its head-end must be split into a second stream, reformatted, and routed to the Arroyo server system. When a customer requests playback of a recorded program, the program must be retrieved from the Arroyo server and transmitted to the customer. This transmission, plaintiffs contend, is an unauthorized public performance by Cablevision of their copyrighted works.

   To "perform" a work, as defined in the Copyright Act, is "to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible." 17 U.S.C. § 101. Cablevision does not contest that the streaming of recorded programming in response to a customer's request is a performance. It again suggests, however, that it is passive in this process -- that it is the customer, not Cablevision, that is "doing" the performing. I reject this suggestion, for the same reasons that I reject the argument that the customer is "doing" the copying involved in the RS-DVR. Cablevision actively participates in the playback process. The customer's use of the remote control to select a recorded program for viewing does not,
UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

BLAKE A. FIELD,                  )
Plaintiff,                       )
vs.                              )
GOOGLE INC.,                     )
Defendant.                       )
AND RELATED COUNTERCLAIMS.

FINDINGS OF FACT
AND CONCLUSIONS OF LAW

ORDER
FINDINGS OF FACT AND CONCLUSIONS OF LAW

This is an action for copyright infringement brought by plaintiff Blake Field ("Field") against Google Inc. ("Google"). Field contends that by allowing Internet users to access copies of 51 of his copyrighted works stored by Google in an online repository, Google violated Field’s exclusive rights to reproduce copies and distribute copies of those works. On December 19, 2005, the Court heard argument on the parties’ cross-motions for summary judgment.

Based upon the papers submitted by the parties and the arguments of counsel, the Court finds that Google is entitled to judgment as a matter of law based on the undisputed facts. For the reasons set forth below, the Court will grant Google’s motion for summary judgment: (1) that it has not directly infringed the copyrighted works at issue; (2) that Google held an implied license to reproduce and distribute copies of the copyrighted works at issue; (3) that Field is estopped from asserting a copyright infringement claim against Google with respect to the works at issue in this action; and (4) that Google’s use of the works is a fair use under 17 U.S.C. § 107.

The Court will further grant a partial summary judgment that Field’s claim for damages is precluded by operation of the “system cache” safe harbor of Section 512(b) of the Digital Millennium Copyright Act ("DMCA"). Finally, the Court will deny Field’s cross-motion for summary judgment seeking a finding of infringement and seeking to dismiss the Google defenses set forth above.

STATEMENT OF PROCEDURAL HISTORY & UNDISPUTED FACTS

Procedural History

1. On April 6, 2004, Plaintiff Field, an author and an attorney who is a member of the State Bar of Nevada, filed a complaint against Google asserting a single claim for copyright infringement based on Google’s alleged copying and distribution of his copyrighted work entitled Good Tea. Field himself had previously published this work on his personal Web site, www.blakeswritings.com.

2. On May 25, 2004, Field filed an Amended Complaint, alleging that Google infringed the copyrights to an additional fifty of Field’s works, which likewise had been published on his personal website. Field did not seek actual damages, but instead requested
$2,550,000 in statutory damages ($50,000 for each of fifty-one registered copyrighted works) along with injunctive relief.

3. On September 27, 2005, Field filed a motion for summary judgment that Google infringed the copyrighted works at issue and that Google’s defenses based on fair use, implied license, estoppel and the Digital Millennium Copyright Act (“DMCA”) should be dismissed as a matter of law. Google filed a motion for summary judgment based on non-infringement, implied license, estoppel and fair use (Docket No. 51).

4. On December 19, 2005, the Court held a hearing on the parties’ cross-motions for summary judgment. At the hearing, Google made an oral cross-motion for partial summary judgment in its favor based upon Section 512(b) of the DMCA.

5. After considering the arguments of counsel, the Court granted Google’s motion for summary judgment on each of the grounds it set forth, granted Google’s oral cross-motion based on the DMCA and denied Field’s motion for summary judgment.

Undisputed Facts

Google, the Google Cache, and “Cached” Links.

6. Google maintains one of the world’s largest and most popular Internet search engines, accessible, among other places, on the World Wide Web at www.google.com. See Brougher Decl. ¶2. Internet search engines like Google’s allow Internet users to sift through the massive amount of information available on the Internet to find specific information that is of particular interest to them. See id. ¶3; see also Levine Report ¶13.¹

7. There are billions of Web pages accessible on the Internet. It would be impossible for Google to locate and index or catalog them manually. See Brougher Decl. ¶3-4; see also Levine Report ¶13-14. Accordingly, Google, like other search engines, uses an automated program (called the “Googlebot”) to continuously crawl across the Internet, to locate and analyze available Web pages, and to catalog those Web pages into Google’s searchable Web index. See Brougher Decl. ¶4-5; see also Levine Report ¶14.

¹ The Levine Report is attached to the Levine Declaration as Exhibit 1.
8. As part of this process, Google makes and analyzes a copy of each Web page that it finds, and stores the HTML code from those pages in a temporary repository called a cache. See Levine Report ¶14; Brougher Decl. ¶5. Once Google indexes and stores a Web page in the cache, it can include that page, as appropriate, in the search results it displays to users in response to their queries. See Brougher Decl. ¶5.

9. When Google displays Web pages in its search results, the first item appearing in each result is the title of a Web page which, if clicked by the user, will take the user to the online location of that page. The title is followed by a short “snippet” from the Web page in smaller font. Following the snippet, Google typically provides the full URL for the page. Then, in the same smaller font, Google often displays another link labeled “Cached.” See Brougher Decl. ¶10.2

10. When clicked, the “Cached” link directs an Internet user to the archival copy of a Web page stored in Google’s system cache, rather than to the original Web site for that page. See Brougher Decl. ¶8. By clicking on the “Cached” link for a page, a user can view the “snapshot” of that page, as it appeared the last time the site was visited and analyzed by the Googlebot. See id.

11. The page a user retrieves from Google after clicking on a “Cached” link contains a conspicuous disclaimer at the top explaining that it is only a snapshot of the page from Google’s cache, not the original page, and that the page from the cache may not be current. See Brougher Decl. ¶11-12 & Ex. 2 (“Google’s cache is the snapshot that we took of the page as we crawled the Web. The page may have changed since that time.”). The disclaimer also includes two separate hyperlinks to the original, current page. See id.

12. Google has provided “Cached” links with its search results since 1998. See Brougher Decl. ¶7. Until this action, Google had never before been sued for providing “Cached”

2 The three most popular search engines – Google, Yahoo!, and MSN – all display “Cached” links with their search results, and operate them identically. See Brougher Decl. ¶17; Google, Yahoo!, and MSN collectively account for more than 80% of all Web searches. See Brougher Decl. ¶17.
links. See Macgillivray Decl. ¶3. The “Cached” link, and the consequences that flow when a
user clicks on it, is the subject of Field’s lawsuit.

The Purposes Served By Google’s “Cached” Links

13. Google enables users to access its copy of Web pages through “Cached” links for
several reasons.

14. Archival Copies. Google’s “Cached” links allow users to view pages that the user
cannot, for whatever reason, access directly. A Web page can become inaccessible to Internet
users because of transmission problems, because nations or service providers seek to censor
certain information, because too many users are trying to access the same page at the same time,
or because the page has been removed from its original location. See Levine Report ¶¶17-19. In
each case, users who request access to the material from the inaccessible site are still able to
access an archival copy of the page via the “Cached” link in Google’s search results. See Levine
Report ¶¶17-19; see also Brougher Decl. ¶14. Google’s users, including those in academia,
describe this functionality as highly valuable. See Levine Decl. ¶4 & Exs. 2-5. This feature
also benefits Web site publishers because it allows users to access their sites when the sites are
otherwise unavailable and has allowed Web site owners to recover copies of their own sites that
might otherwise have been lost due to computer problems. See Levine Report ¶¶16-19; see also
Levine Decl., Ex. 7 at 2.

15. Web Page Comparisons. Google’s archival functionality is also of considerable
importance to those who wish to determine how a particular Web page has been altered over
time. By examining Google’s copy of the page, people can identify subtle but potentially
significant differences between the current version of a page, and the page as it existed when last
visited by the Googlebot. See Levine Report ¶20; see also Brougher Decl. ¶15; Levine Decl.,
Exs. 10, 11.

For example, the State of Indiana instructs its judges about this capability. See Levine
Decl., Ex. 5 at 2 (article entitled “Maximizing Web Searches With Google,” available at
http://www.in.gov/judiciary/center/ed/library/judcon-03/google.pdf, explains that “Clicking
‘Cached’ will simply give you an older version of the result page, which represents what the
page looked like the last time the Google engine indexed the page. This service exists in case a
website’s server becomes unavailable.”).
16. **Identification of Search Query Terms.** Google’s “Cached” links also allow users to immediately determine why a particular page was deemed responsive to their search query, by highlighting the terms from the user’s query as they appear on the page. *See Levine Report ¶17; see also Brougher Decl. ¶16.* In some cases, if a user clicks on Google’s link to an original Web page, he may be unable to determine how the page relates to his inquiry. That is particularly true for text-intensive pages where the user’s search term may be very difficult to find. *See Levine Report ¶17; see also Levine Decl., Ex. 13 at 1.* In some cases it may be impossible for a user to find the information on a page that is responsive to a given search where a site owner has altered the text on the original page and removed the relevant language. *See Levine Report ¶17; see also Brougher Decl. ¶16.* By allowing access to copies of Web pages through “Cached” links, Google enables users to more quickly determine whether and where a user’s search query appears, and thus whether the page is germane to their inquiry.

17. **Given the breadth of the Internet, it is not possible for Google (or other search engines) to personally contact every Web site owner to determine whether the owner wants the pages in its site listed in search results or accessible through “Cached” links. See Brougher Decl. ¶18; see also Levine Report ¶25.**

18. **The Internet industry has developed a set of widely recognized and well-publicized industry standard protocols by which Web site owners can automatically communicate their preferences to search engines such as Google. See Levine Report ¶¶25, 29, 35 (listing sources that document these standards); Brougher Decl. ¶¶18-21. Google provides instructions for Web site owners to communicate their preferences to Google at**

http://www.google.com/remove.html. *See Levine Report ¶¶30, 35; Brougher Decl. ¶¶18-21; O’Callaghan Decl. Ex. 5; see also id. Exs. 4, 6.*

19. **A principal way for Web site owners to communicate with Google’s robot is by placing specific instructions in “meta-tags” within the computer code (called HTML) that comprises a given page. When the Googlebot visits a page, it reads through this code. If it encounters meta-tags, it follows the instructions provided. Thus, for example, a site owner can place the following meta-tag within a page to tell Google’s robot not to analyze the page or**
include it in Google’s Web index and search results: “<META NAME="ROBOTS"
CONTENT="NOINDEX, NOFOLLOW">” See Brougher Decl. ¶20; see also Levine Report ¶33.4

20. Using meta-tags, a Web site owner can also tell Google’s robot that it can include
a given page in Google’s index, but that it should not provide a “Cached” link to that page in
Google’s search results. To do so, the Web site owner uses a “no-archive” meta-tag “<META
NAME="ROBOTS" CONTENT="NOARCHIVE">” See Brougher Decl. ¶21; see also Levine Report ¶35. The “no-archive” meta-tag has been a widely recognized industry standard for
years. See Levine Report ¶35.

21. If a Web site owner includes the “no-archive” meta-tag on a page, then Google
does not provide a “Cached” link when it lists that page in its search results. See Brougher Decl.
¶21-22.5

22. Web site owners can also communicate with search engines’ robots by placing a
“robots.txt” file on their Web site. See Brougher Decl. ¶19; see also Levine Report ¶29. For
example, if the Web site owner does not want robots to crawl the owner’s Web site, the owner
can create a robots.txt file with the following text: “User-agent: * Disallow: /”. See Brougher
Decl. ¶19; see also Levine Report ¶29. The above text tells the robots that they should not
crawl the owner’s Web site. See Brougher Decl. ¶19; see also Levine Report ¶29.6 If Google’s
robot encounters a robots.txt file with the above text, then it will not crawl the Web site, and
there will be no entry for that Web page in Google’s search results and no cached link. See

4 A Web site owner can add the “no-archive” meta-tag to a Web page in a matter of seconds.
See Brougher Decl. ¶21. Web site owners can also use a Google-specific “no-archive” meta-tag
to tell Google that it cannot provide “Cached” links, while allowing other search engines (e.g.,
Yahoo! and MSN) to do so. See id.; see also Levine Report ¶35.

5 A Web site owner can also request that Google not display “Cached” links for given pages
by using Google’s automatic URL removal procedure. See Brougher Decl. ¶23. Google’s Web
site provides step-by-step instructions on using this procedure. See id.; see also O’Callaghan
Decl. Ex. 5 (attaching a printout of http://www.google.com/remove.html). Further, Web site
owners can contact Google directly to make such a request. Google honors such requests. See
Brougher Decl. ¶24.

6 By contrast, a Web site owner can invite robots to visit a site without restriction by
Brougher Decl. ¶19. The Internet industry has widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994. See Levine Report ¶29.

**Plaintiff Blake Field and His Copyright Claim**

23. Plaintiff Blake Field has regularly used Google’s search engine over the past several years and was familiar with the manner in which it operates. See Field Dep. at 103:15-20.\(^7\)

24. Field has long been aware that Google automatically provides “Cached” links for pages that are included in its index and search results unless instructed otherwise. See id. at 74:8-22, 109:22-110:6. Field decided to manufacture a claim for copyright infringement against Google in the hopes of making money from Google’s standard practice. See id. at 79:8-15, 141:15-24.

25. Field admits he knew that any Web site owner could instruct Google not to provide a “Cached” link to a given Web page by using the “no-archive” meta-tag (as discussed above). See Field Dep. at 74:8-22, 81:13-17. Field also knew that Google provided a process to allow Web site owners to remove pages from Google’s system cache. See id. at 81:18-21, 83:4-11, 84:15-21; O’Callaghan Decl. Ex. 3 at 1-2 (Pl.’s Resp. to Req. for Admis. Nos. 1, 4). With this knowledge, Field set out to get his copyrighted works included in Google’s index, and to have Google provide “Cached” links to Web pages containing those works.

26. Over a three-day period in January 2004, Field created the 51 works at issue in this lawsuit. See O’Callaghan Decl. Ex. 2 (Pl.’s Resp. to Interrog. No. 5).

27. Field registered copyrights for each of these works separately on January 16, 2004. See First Am. Compl. ¶7. Field then created a Web site at www.blakeswritings.com and published his works on pages where they were accessible, for free, to the world starting in late January 2004. See Field Dep. at 45:2-4, 94:10-19.

28. Field created a robots.txt file for his site and set the permissions within this file to allow all robots to visit and index all of the pages on the site. See Field Dep. at 46:10-16; Levine.

\(^7\) Excerpts from the Field Deposition are attached to the O’Callaghan Declaration as Exhibit 1.
Report ¶31. Field created the robots.txt file because he wanted search engines to visit his site and include the site within their search results. See Field Dep. at 46:2-4, 17-23.

29. Field knew that if he used the “no-archive” meta-tag on the pages of his site, Google would not provide “Cached” links for the pages containing his works. See Field Dep. at 81:13-17; O’Callaghan Decl. Ex. 3 at 2 (Resp. to Req. for Admis. No. 4). Field consciously chose not to use the “no-archive” meta-tag on his Web site. See Field Dep. at 83:25-84:3.

30. As Field expected, the Googlebot visited his site and indexed its pages, making the pages available in Google search results. When the pages containing Field’s copyrighted works were displayed in Google’s search results, they were automatically displayed with “Cached” links, as Field intended they would be.

31. According to Google’s records, an individual or individuals clicked on the “Cached” links for each of the pages containing Field’s works, and retrieved copies of each of the those pages from Google’s system cache.

32. When Google learned that Field had filed (but not served) his complaint, Google promptly removed the “Cached” links to all of the pages of his site. See MacGillivray Decl. ¶2; see also Countercls. ¶22; Ans. to Countercls. ¶22. Google also wrote to Field explaining that Google had no desire to provide “Cached” links to Field’s pages if Field did not want them to appear. See O’Callaghan Decl. Ex. 7.

CONCLUSIONS OF LAW

Legal Standard for Summary Judgment

A court must grant summary judgment if the pleadings and supporting documents, when viewed in the light most favorable to the non-moving party, “show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c). An issue as to a material fact is only “genuine” if the evidence regarding the disputed fact is “such that a reasonable jury could return a verdict for the nonmoving party,” and a dispute is “material” only if it could affect the outcome of the suit under governing law.


Discussion

I. Direct Infringement of the Copyrighted Works

Google has filed a motion for summary judgment that by operating its cache and presenting "Cached" links to works within it, Google does not directly infringe Field's copyrighted works. Field has filed a cross-motion for summary judgment for a finding of direct infringement. The Court grants Google's motion and denies Field's motion.⁸

To demonstrate copyright infringement, "the plaintiff must show ownership of the copyright and copying by the defendant." *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 817 (9th Cir. 2003); *see also* 17 U.S.C. § 501. A plaintiff must also show volitional conduct on the part of the defendant in order to support a finding of direct copyright infringement. *See Religious Tech. Ctr v. Netcom On-Line COMM'n Servs., Inc.*, 907 F. Supp. 1361, 1369-70 (N.D. Cal. 1995) (direct infringement requires a volitional act by defendant; automated copying by machines occasioned by others not sufficient); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004) ("Agreeing with the analysis in Netcom, we hold that the automatic copying, storage, and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement under §§ 501 and 106 of the Copyright Act.").

The parties do not dispute that Field owns the copyrighted works subject to this action. The parties do dispute whether by allowing access to copyrighted works through "Cached" links Google engages in volitional "copying" or "distribution" under the Copyright Act sufficient to establish a prima facie case for copyright infringement.

Field does not allege that Google committed infringement when its "Googlebot," like an ordinary Internet user, made the initial copies of the Web pages containing his copyrighted works and stores those copies in the Google cache. *See* Field Dep. at 143:13-144-1; 98:18-25. Instead, Field alleges that Google directly infringed his copyrights when a Google user clicked on a "Cached" link to the Web pages containing Field's copyrighted works and downloaded a copy of those pages from Google's computers. *See id.; see also* First Am. Compl. ¶¶ 29-32.

⁸ Field did not contend that Google was liable for indirect infringement (contributory or vicarious liability).
According to Field, Google itself is creating and distributing copies of his works. But when a user requests a Web page contained in the Google cache by clicking on a “Cached” link, it is the user, not Google, who creates and downloads a copy of the cached Web page. Google is passive in this process. Google’s computers respond automatically to the user’s request. Without the user’s request, the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur. The automated, non-volitional conduct by Google in response to a user’s request does not constitute direct infringement under the Copyright Act. See, e.g., Religious Tech. Ctr., 907 F. Supp. at 1369-70 (direct infringement requires a volitional act by defendant; automated copying by machines occasioned by others not sufficient); CoStar Group, 373 F.3d at 555; Sega Enters. Ltd v. MAPHIA, 948 F. Supp. 923, 931-32 (N.D. Cal. 1996).

Summary judgment of non-infringement in Google’s favor is thus appropriate.

II. Google’s Defenses

Google and Field have filed cross-motions for summary judgment with respect to various defenses Google has asserted to Field’s charge of direct copyright infringement. Assuming that by allowing users to access Field’s copyrighted works through its “Cached” links Google is engaged in direct copyright infringement, the Court finds that Google has established four defenses to Field’s copyright infringement claim.

A. Implied License

A license is a defense to a claim of copyright infringement. See Effects Assocs., Inc. v. Cohen, 908 F.2d 555, 558-59 (9th Cir. 1990). A copyright owner may grant a nonexclusive license expressly or impliedly through conduct. See id. (citing 3 Melville B. Nimmer & David Nimmer, Nimmer On Copyright § 10.03[A] (1989) (hereinafter “Nimmer”)); see also Quinn v. City of Detroit, 23 F. Supp. 2d 741, 749 (E.D. Mich. 1998). An implied license can be found where the copyright holder engages in conduct “from which [the] other [party] may properly infer that the owner consents to his use.” See, e.g., De Forest Radio Tel. & Tel. Co. v. United States, 273 U.S. 236, 241 (1927) (setting forth requirements for an implied license defense to a charge of patent infringement). Consent to use the copyrighted work need not be manifested verbally and may be inferred based on silence where the copyright holder knows of the use and
("consent given in the form of mere permission or lack of objection is also equivalent to a
nonexclusive license"); Quinn, 23 F. Supp. at 753.

According to the undisputed testimony of Google’s Internet expert, Dr. John Levine,
Web site publishers typically communicate their permissions to Internet search engines (such as
Google) using "meta-tags." A Web site publisher can instruct a search engine not to cache the
publisher’s Web site by using a "no-archive" meta-tag. According to Dr. Levine, the "no-
archive" meta-tag is a highly publicized and well-known industry standard. Levine Report
¶ 33-37. Field concedes he was aware of these industry standard mechanisms, and knew that
the presence of a "no archive" meta-tag on the pages of his Web site would have informed
Google not to display "Cached" links to his pages. Despite this knowledge, Field chose not to
include the no-archive meta-tag on the pages of his site. He did so, knowing that Google would
interpret the absence of the meta-tag as permission to allow access to the pages via "Cached"
links. Thus, with knowledge of how Google would use the copyrighted works he placed on
those pages, and with knowledge that he could prevent such use, Field instead made a conscious
decision to permit it. His conduct is reasonably interpreted as the grant of a license to Google for
that use. See, e.g., Keane, 968 F. Supp. at 947 (copyright owner’s knowledge of defendant’s use
coupled with owner’s silence constituted an implied license); See also Levine Report ¶37
(providing the undisputed expert opinion that Google reasonably interpreted absence of meta-
tags as permission to present "Cached" links to the pages of Field’s site). Accordingly, the Court
grants Google’s motion that it is entitled to the defense of implied license, and denies Field’s
cross-motion that the defense is inapplicable.

B. Estoppel

A plaintiff is estopped from asserting a copyright claim “if he has aided the defendant in
infringing or otherwise induced it to infringe or has committed covert acts such as holding out .
. by silence or inaction.” See Quinn, 23 F. Supp. 2d at 753 (internal quotation marks omitted,
citing 4 Nimmer § 13.07 (1990)). To prevail on its estoppel defense, Google must prove the
following four elements:
1. Field knew of Google’s allegedly infringing conduct;
2. Field intended that Google rely upon his conduct or acted so that Google had a
   right to believe it was so intended;
3. Google was ignorant of the true facts; and
4. Google detrimentally relied on Field’s conduct.


Here, all four elements have been established as a matter of law.

First, Field knew of Google’s allegedly infringing conduct well before any supposed
infringement of his works took place. Field concedes that he knew that Google would
automatically allow access to his works through “Cached” links when he posted them on the
Internet unless he instructed otherwise. Field also knew that if an Internet user clicked on the
“Cached” links to his web pages, the user would immediately download a copy of those pages
from Google’s system cache. Field was aware of steps he could take to ensure that his web site
would not be archived and not included in Google’s cache. There is no dispute that Field was
aware of the conduct that he challenges in this lawsuit.

Second, Field remained silent regarding his unstated desire not to have “Cached” links
provided to his Web site, and he intended for Google to rely on this silence. Field could have
informed Google not to provide “Cached” links by using a “no archive” meta-tag or by
employing certain commands in robots.txt file. Instead, Field chose to remain silent knowing
that Google would automatically interpret that silence as permission to display “Cached” links.
Field’s silence, particularly given his knowledge of the consequences of that silence, satisfies the
second estoppel factor.

Third, Google was not aware that Field did not wish to have Google provide “Cached”
links to his works. Macgillivray Decl. ¶2.

Fourth, Google detrimentally relied on Field’s silence. It is undisputed that if Google had
known of Field’s preference, it would not have presented “Cached” links to Field’s pages. See
Macgillivray Decl. ¶2; see also O’Callaghan Decl. Ex. 7. Google honors copyright holder’s
requests that it not display “Cached” links to their pages. Brougher Decl. ¶18. Google’s reliance
on Field's silence was to its detriment. Had Field communicated his preferences to Google, the
parties would have avoided the present lawsuit entirely. See Hadady Corp. v. Dean Witter
prejudice to defendant).

Because the Court finds that all four estoppel factors are present based on the undisputed
facts, the Court grants Google's motion for summary judgment on the defense of estoppel and
denies Field's cross-motion.

C. Fair Use

"Fair use" of a copyrighted work "is not an infringement of copyright" under the
Copyright Act. 17 U.S.C. § 107. The fair use doctrine "creates a limited privilege in those other
than the owner of a copyright to use the copyrighted material in a reasonable manner without the
owner's consent," Fisher v. Dees, 794 F.2d 432, 435 (9th Cir. 1986), and "permits courts to
avoid rigid application of the copyright statute when, on occasion, it would stifle the very
creativity which that law is designed to foster." Dr. Seuss Enters., L.P. v. Penguin Books USA,
Inc., 109 F.3d 1394, 1399 (9th Cir. 1997) (internal quotation marks omitted).

In analyzing whether a particular use qualifies as a "fair use," the Copyright Act directs a
Court to analyze at least four factors:

(1) the purpose and character of the use, including whether such use is of a
commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted
work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted
work. 17 U.S.C. § 107. The Court must "balance these factors in light of the objectives of
copyright law, rather than view them as definitive or determinative tests." See Kelly, 336 F.3d at
818.

While no one factor is dispositive, courts traditionally have given the most weight to the

Federal Criminal Intellectual Property Statutes

17 U.S.C. § 506

Effective April 27, 2006; current as of March 1, 2007

(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

http://www.cybercrime.gov/17usc506.htm
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 or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.

(c) Fraudulent Copyright Notice.—Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500.

(d) Fraudulent Removal of Copyright Notice.—Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500.

(e) False Representation.—Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.

(f) Rights of Attribution and Integrity.—Nothing in this section applies to infringement of the rights conferred by section 106A(a).
In the

United States Court of Appeals
For the Seventh Circuit

No. 05-1314

BMG MUSIC, et al.,

v.

CECILIA GONZALEZ,

Plaintiffs-Appellees,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 03 C 6276—Blanche M. Manning, Judge.

ARGUED OCTOBER 27, 2005—DECIDED DECEMBER 9, 2005

Before Easterbrook, Evans, and Williams, Circuit Judges.

Easterbrook, Circuit Judge. Last June the Supreme Court held in MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005), that a distributed file-sharing system is engaged in contributory copyright infringement when its principal object is the dissemination of copyrighted material. The foundation of this holding is a belief that people who post or download music files are primary infringers. In re Aimster Copyright Litigation, 334 F.3d 643, 645 (7th Cir. 2003), which anticipated Grokster, made the same assumption. In this appeal Cecilia Gonzalez, who downloaded copyrighted music through the KaZaA file-sharing network, denies the premise of Grokster and
Aimster. She contends that her activities were fair use rather than infringement. The district court disagreed and granted summary judgment for the copyright proprietors (to which we refer collectively as BMG Music). 2005 U.S. Dist. LEXIS 910 (N.D. Ill. Jan. 7, 2005). The court enjoined Gonzalez from further infringement and awarded $22,500 in damages under 17 U.S.C. §504(c).

A “fair use” of copyrighted material is not infringement. Gonzalez insists that she was engaged in fair use under the terms of 17 U.S.C. §107—or at least that a material dispute entitles her to a trial. It is undisputed, however, that she downloaded more than 1,370 copyrighted songs during a few weeks and kept them on her computer until she was caught. Her position is that she was just sampling music to determine what she liked enough to buy at retail. Because this suit was resolved on summary judgment, we must assume that Gonzalez is telling the truth when she says that she owned compact discs containing some of the songs before she downloaded them and that she purchased others later. She concedes, however, that she has never owned legitimate copies of 30 songs that she downloaded. (How many of the remainder she owned is disputed.)

Instead of erasing songs that she decided not to buy, she retained them. It is these 30 songs about which there is no dispute concerning ownership that formed the basis of the damages award. This is not a form of time-shifting, along the lines of Sony Corp. of America v. Universal Studios, Inc., 464 U.S. 417 (1984) (Betamax). A copy downloaded, played, and retained on one’s hard drive for future use is a direct substitute for a purchased copy—and without the benefit of the license fee paid to the broadcaster. The premise of Betamax is that the broadcast was licensed for one transmission and thus one viewing. Betamax held that shifting the time of this single viewing is fair use. The files that Gonzalez obtained, by contrast, were posted in violation of copyright law; there was

Section 107 provides that when considering a defense of fair use the court must take into account “(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.” Gonzalez was not engaged in a nonprofit use; she downloaded (and kept) whole copyrighted songs (for which, as with poetry, copying of more than a couplet or two is deemed excessive); and she did this despite the fact that these works often are sold per song as well as per album. This leads her to concentrate on the fourth consideration: “the effect of the use upon the potential market for or value of the copyrighted work.”

As she tells the tale, downloading on a try-before-you-buy basis is good advertising for copyright proprietors, expanding the value of their inventory. The Supreme Court thought otherwise in Grokster, with considerable empirical support. As file sharing has increased over the last four years, the sales of recorded music have dropped by approximately 30%. Perhaps other economic factors contributed, but the events likely are related. Music downloaded for free from the Internet is a close substitute for purchased music; many people are bound to keep the downloaded files without buying originals. That is exactly what Gonzalez did for at least 30 songs. It is no surprise, therefore, that the only appellate decision on point has held that downloading copyrighted songs cannot be defended as fair use, whether or not the recipient plans to buy songs she likes well enough.
to spring for. See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1014-19 (9th Cir. 2001). See also *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000) (holding that downloads are not fair use even if the downloader already owns one purchased copy).

Although BMG Music sought damages for only the 30 songs that Gonzalez concedes she has never purchased, all 1,000+ of her downloads violated the statute. All created copies of an entire work. All undermined the means by which authors seek to profit. Gonzalez proceeds as if the authors' only interest were in selling compact discs containing collections of works. Not so; there is also a market in ways to introduce potential consumers to music.

Think of radio. Authors and publishers collect royalties on the broadcast of recorded music, even though these broadcasts may boost sales. See *Broadcast Music, Inc. v. Columbia Broadcasting System, Inc.*, 441 U.S. 1 (1979) (discussing the licenses available from performing rights societies for radio and television broadcasts). Downloads from peer-to-peer networks such as KaZaA compete with licensed broadcasts and hence undermine the income available to authors. This is true even if a particular person never buys recorded media. Cf. *United States v. Slater*, 348 F.3d 666 (7th Cir. 2003). Many radio stations stream their content over the Internet, paying a fee for the right to do so. Gonzalez could have listened to this streaming music to sample songs for purchase; had she done so, the authors would have received royalties from the broadcasters (and reduced the risk that files saved to disk would diminish the urge to pay for the music in the end).

Licensed Internet sellers, such as the iTunes Music Store, offer samples—but again they pay authors a fee for the right to do so, and the teasers are just a portion of the original. Other intermediaries (not only Yahoo! Music Unlimited and Real Rhapsody but also the revived Napster,
with a new business model) offer licensed access to large collections of music; customers may rent the whole library by the month or year, sample them all, and purchase any songs they want to keep. New technologies, such as SNOCAP, enable authorized trials over peer-to-peer systems. See Saul Hansell, *Putting the N fores Genie Back in the Bottle*, New York Times (Nov. 20, 2005); see also http://www.snocap.com.

Authorized previews share the feature of evanescence: if a listener decides not to buy (or stops paying the rental fee), no copy remains behind. With all of these means available to consumers who want to choose where to spend their money, downloading full copies of copyrighted material without compensation to authors cannot be deemed "fair use." Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying "fair use" if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute. Nor can she defend by observing that other persons were greater offenders; Gonzalez's theme that she obtained "only 30" (or "only 1,300") copyrighted songs is no more relevant than a thief's contention that he shoplifted "only 30" compact discs, planning to listen to them at home and pay later for any he liked.

BMG Music elected to seek statutory damages under 17 U.S.C. §504(c)(1) instead of proving actual injury. This section provides that the author's entitlement, per infringed work, is "a sum of not less than $750 or more than $30,000 as the court considers just." But if an "infringer sustains the burden of proving, and the court finds, that such infringer was not aware and had no reason to believe that his or her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages
to a sum of not less than $200.” 17 U.S.C. §504(c)(2). Gonzales asked the district court to reduce the award under this proviso, but the judge concluded that §402(d) bars any reduction in the minimum award. This subsection provides: “If a notice of copyright in the form and position specified by this section appears on the published phonorecord or phonorecords 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.” It is undisputed that BMG Music gave copyright notice as required—“on the surface of the phonorecord, or on the phonorecord label or container” (§402(c)). It is likewise undisputed that Gonzales had “access” to records and compact disks bearing the proper notice. She downloaded data rather than discs, and the data lacked copyright notices, but the statutory question is whether “access” to legitimate works was available rather than whether infringers earlier in the chain attached copyright notices to the pirated works. Gonzales readily could have learned, had she inquired, that the music was under copyright.

If BMG Music had requested more than $750 per work, then Gonzales would have been entitled to a trial. See Feltner v. Columbia Pictures Television, Inc., 523 U.S. 340 (1998). What number between $750 and $30,000 is “just” recompense is a question for the jury, unless both sides agree to decision by the court. But BMG Music was content with $750 per song, which the district judge awarded on summary judgment. Gonzales contends that this was improper: Feltner, she contends, holds that a jury must decide whether even the statutory minimum award will be allowed.

Feltner holds that a claim for statutory damages under §504(c) is a suit at law to which the seventh amendment applies. This does not mean, however, that a jury must resolve every dispute. When there are no disputes of
material fact, the court may enter summary judgment without transgressing the Constitution. See Fidelity &
Deposit Co. v. United States, 187 U.S. 315 (1902). See also
Galloway v. United States, 319 U.S. 372 (1943); Gasoline
While acknowledging this proposition, Gonzalez insists that
copyright cases are different. She relies entirely on a single
passage from Feltner: “The right to a jury trial includes the
right to have a jury determine the amount of statutory
damages, if any, awarded to the copyright owner.” 528 U.S.
at 353 (emphasis in original). Gonzalez maintains that by
adding “if any” the Court allowed a jury to send an author
home empty handed, even if the statute makes $750 the
minimum. In other words, she contends that Feltner creates
a system of jury nullification unique to copyright litigation.

The Justices did not purport to give defendants in
copyright cases the right to ask jurors to return verdicts in
the teeth of the law. The sentence we have quoted is a
general description of the jury’s role, which the Court
drew from seventeenth-century English jurisprudence.
That’s hardly a plausible source for a rule unique to
American copyright law. In Feltner neither side had
sought summary judgment. We read Feltner as establishing
no more (and no less) than that cases under §504(c) are
normal civil actions subject to the normal allocation
of functions between judge and jury. When there is a
material dispute of fact to be resolved or discretion to be
exercised in selecting a financial award, then either
side is entitled to a jury; if there is no material dispute
and a rule of law eliminates discretion in selecting the
remedy, then summary judgment is permissible. See
Segrets, Inc. v. Gillman Knitwear Co., 207 F.3d 56, 65 n.7
(1st Cir. 2000).

Gonzalez says that the ninth circuit understood Feltner
differently on remand, but that’s mistaken. A jury trial was
held—for there were material factual disputes—and the
jury returned a verdict of $31.68 million in statutory damages (or $72,000 per infringed work, an award made possible by the jury's conclusion that infringement had been willful). The defendant, rung its Pyrrhic victory in the Supreme Court (the judge's original award, which the Court vacated, had been $8.8 million), maintained that §504(c) is unconstitutional, and that only actual damages may be awarded, because §504(c) does not provide for a jury trial. The court of appeals rejected that contention, noting that after the Supreme Court's decision a jury trial had been held. See Columbia Pictures Industries, Inc. v. Krypton Broadcasting of Birmingham, Inc., 259 F.3d 1186, 1192-93 (9th Cir. 2001). Whether a jury resolves the dispute because of statutory language or because of the seventh amendment is all the same to the litigants. It is not possible to find, in a decision affirming a jury's verdict, a rule of law that a jury is required even when there are no factual disputes to resolve and no discretion to exercise.

As for the injunction: Gonzalez contends that this should be vacated because she has learned her lesson, has dropped her broadband access to the Internet, and is unlikely to download copyrighted material again. A private party's discontinuation of unlawful conduct does not make the dispute moot, however. An injunction remains appropriate to ensure that the misconduct does not recur as soon as the case ends. See United States v. W.T. Grant Co., 345 U.S. 629 (1953). The district court did not abuse its discretion in awarding prospective relief.

AFFIRMED
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.\(^3\) 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-

\(^3\)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

4There 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.

5By 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 file sharing 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.

Grokster 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.

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

---

6The Grokster 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 “[it 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
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 (ellipsis in original). 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-to and inserted digital codes into its Web site so that computer users using Web search engines to look for “Napster” or “[f]ree filesharing” would be directed to the Grokster Web site, where they could download the Grokster software. Id., at 992–993. And Grokster’s name is an apparent derivative of Napster.

The 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 Gershin 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 436, 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 inducement 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(e); *Aro Mfg. Co. v. Convertible Top Replacement Co.*, 377 U. S. 476, 485 (1964) (notingcodification 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 Heckin 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


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
Opinion of the Court

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

\(^{10}\) Nor 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 co-operate in an infringement when sale to such user is invoked by advertisement" of the infringing use); *Thompson-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.*
Opinion of the Court

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, more 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
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-
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.

Concurrence omitted
TITLE 17 > CHAPTER 5 > § 512
§ 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) 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) does not have actual knowledge that the material or activity is infringing;

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

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

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

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

(e) Limitation on Liability of Nonprofit Educational Institutions.—

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

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

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

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

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

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

(1) that material or activity is infringing, or

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

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

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

(1) No liability for taking down generally.— Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception.— Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the
service provider that is removed, or to which access is disabled by the
service provider, pursuant to a notice provided under subsection (c)
(1)(C), unless the service provider—

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

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

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

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

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

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

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

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

(4) Limitation on other liability.— A service provider’s compliance
with paragraph (2) shall not subject the service provider to liability for
copyright infringement with respect to the material identified in the
notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer.—

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

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

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

(B) a proposed subpoena; and

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

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

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

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

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

(I) Conditions for Eligibility.—

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

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

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

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

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

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

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

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

(1) Scope of relief.—

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

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

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

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

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

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

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

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

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

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

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

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

(3) Notice and ex parte orders.— Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider’s communications network.

(k) Definitions.—

(1) Service provider.—

(A) As used in subsection (a), the term “service provider” means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term “service provider” means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary relief.— As used in this section, the term “monetary relief” means damages, costs, attorneys’ fees, and any other form of monetary payment.

(l) Other Defenses Not Affected.— The failure of a service provider’s conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider’s conduct is not infringing under this title or any other

http://www4.law.cornell.edu/uscode/html/uscode17/usc_sec_17_00000512----000-.html

8/3/2007
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 (l); 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.

LII has no control over and does not endorse any external Internet site that contains links to or references LII.

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

PERFECT 10, INC., a California corporation,

Plaintiff-Appellant,

v.

CCBILL LLC, a corporation;
CAVE CREEK WHOLESALE INTERNET
EXCHANGE, a corporation d/b/a
CWIE LLC,

Defendants-Appellees,

and

NETPASS SYSTEMS INC., a corporation,

Defendant.

No. 04-57143
D.C. No.
CV-02-07624-LGB

PERFECT 10, INC., a California corporation,

Plaintiff-Appellee,

v.

CCBILL LLC, a corporation;
CAVE CREEK WHOLESALE INTERNET
EXCHANGE, a corporation d/b/a
CWIE LLC,

Defendants-Appellants,

and

NETPASS SYSTEMS INC., a corporation,

Defendant.

No. 04-57207
D.C. No.
CV-02-07624-LGB
ORDER
AMENDING OPINION AND
AMENDED OPINION

6535
OPINION

MILAN D. SMITH, JR., Circuit Judge:

Perfect 10, the publisher of an adult entertainment magazine and the owner of the subscription website perfect10.com, alleges that CCBill and CWIE violated copyright, trademark, and state unfair competition, false advertising and right of publicity laws by providing services to websites that posted images stolen from Perfect 10's magazine and website. Perfect 10 appeals the district court's finding that CCBill and CWIE qualified for certain statutory safe harbors from copyright infringement liability under the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512, and that CCBill and CWIE were immune from liability for state law unfair competition and false advertising claims based on the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1). CCBill and CWIE cross-appeal, arguing that the district court erred in holding that the CDA does not provide immunity against Perfect 10's right of publicity claims and in denying their requests for costs and attorney's fees under the Copyright Act.

We have jurisdiction pursuant to 28 U.S.C. § 1291. We affirm in part, reverse in part, and remand.

BACKGROUND

Perfect 10 is the publisher of the eponymous adult entertainment magazine and the owner of the website, perfect10.com. Perfect10.com is a subscription site where consumers pay a membership fee in order to gain access to
content on the website. Perfect 10 has created approximately 5,000 images of models for display in its website and magazine. Many of the models in these images have signed releases assigning their rights of publicity to Perfect 10. Perfect 10 also holds registered U.S. copyrights for these images and owns several related, registered trademark and service marks.

CWIE provides webhosting and related Internet connectivity services to the owners of various websites. For a fee, CWIE provides “ping, power, and pipe,” services to their clients by ensuring the “box” or server is on, ensuring power is provided to the server and connecting the client’s service or website to the Internet via a data center connection. CCBill allows consumers to use credit cards or checks to pay for subscriptions or memberships to e-commerce venues.

Beginning August 10, 2001, Perfect 10 sent letters and emails to CCBill and CWIE stating that CCBill and CWIE clients were infringing Perfect 10 copyrights. Perfect 10 directed these communications to Thomas A. Fisher, the designated agent to receive notices of infringement. Fisher is also the Executive Vice-President of both CCBill and CWIE. Representatives of celebrities who are not parties to this lawsuit also sent notices of infringement to CCBill and CWIE. On September 30, 2002, Perfect 10 filed the present action alleging copyright and trademark violations, state law claims of violation of right of publicity, unfair competition, false and misleading advertising, as well as RICO claims.

STANDARDS OF REVIEW

We review a district court’s grant of summary judgment de novo. Rossi v. Motion Picture Ass’n of Am. Inc., 391 F.3d 1000, 1002 (9th Cir. 2004). “Viewing the evidence in the light most favorable to the nonmoving party, we must determine whether there are any genuine issues of material fact and whether the district court correctly applied the relevant sub-
stative law." *Leever v. Carson City*, 360 F.3d 1014, 1017 (9th Cir. 2004). The district court’s interpretations of the Copyright Act are also reviewed de novo. *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004).

We review a district court’s decision to grant or deny attorney’s fees under the Copyright Act for abuse of discretion. *Columbia Pictures Television, Inc. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1197 (9th Cir. 2001).

**DISCUSSION**

**I. SECTION 512 SAFE HARBORS**

[1] The DMCA established certain safe harbors to “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 1076-77 (citing 17 U.S.C. §§ 512(a)-(d)) (footnotes omitted). These safe harbors limit liability but “do not affect the question of ultimate liability under the various doctrines of direct, vicarious, and contributory liability,” *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002) (citing H.R. Rep. 105-551 (II), at 50 (1998) (“H.R. Rep.”), and “nothing in the language of § 512 indicates that the limitation on liability described therein is exclusive.” *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 552 (4th Cir. 2004).

**A. Reasonably Implemented Policy: § 512(i)(1)(A)**

[2] To be eligible for any of the four safe harbors at §§ 512(a)-(d), a service provider must first meet the threshold conditions set out in § 512(i), including the requirement that the service provider:

---

[H]as 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.

Section 512(i)(1)(A); Ellison, 357 F.3d at 1080.

[3] The statute does not define "reasonably implemented." We hold that a service provider "implements" a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications. Ellison, 357 F.3d at 1080 (working notification system required); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1102-03 (W.D. Wash. 2004) (must adopt procedure for dealing with notifications); In re Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002) (policy not implemented if service provider actively blocks collection of information). The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under "appropriate circumstances," the service provider terminates users who repeatedly or blatantly infringe copyright. See 17 U.S.C. § 512(i); Corbis, 351 F. Supp. 2d at 1102.

I. "Implementation"

Perfect 10 argues that there is a genuine issue of material fact whether CCBill and CWIE prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters. The district court found that there was not, and we agree.

In Ellison, Stephen Robertson posted copies of Harlan Ellison's copyrighted short stories on Internet newsgroups avail-
able through USENET servers. 357 F.3d at 1075. Ellison asserted that America Online, Inc. ("AOL") had infringed his copyright by providing access to the USENET servers. Id. Based on evidence that AOL changed its contact email address for copyright infringement notices from copyright@aol.com to aolcopyright@aol.com in the fall of 1999, but neglected to register the change with the U.S. Copyright Office until April 2000, we held that the district court erred in concluding on summary judgment that AOL satisfied the requirements of § 512(i). Id. at 1077. Even though Ellison did not learn of the infringing activity until after AOL had notified the U.S. Copyright Office of the correct email address, we found that "AOL allowed notices of potential copyright infringement to fall into a vacuum and go unheeded; that fact is sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers." Id. at 1080.

Similarly, the Aimster cases hold that a repeat infringer policy is not implemented under § 512(i)(1)(A) if the service provider prevents copyright holders from providing DMCA-compliant notifications. In Aimster, the district court held that Aimster did not reasonably implement its stated repeat infringer policy because "the encryption on Aimster renders it impossible to ascertain which users are transferring which files." 252 F. Supp. 2d at 659. The court found that "[a]dopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an 'implementation' as required by § 512(i)." Id. The Seventh Circuit affirmed, finding that Aimster did not meet the requirement of § 512(i)(1)(A) because, in part, "by teaching its users how to encrypt their unlawful distribution of copyrighted materials [Aimster] disabled itself from doing anything to prevent infringement." In re Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003).

[4] Based on Ellison and the Aimster cases, a substantial failure to record webmasters associated with allegedly
infringing websites may raise a genuine issue of material fact as to the implementation of the service provider’s repeat infringer policy. In this case, however, the record does not reflect such a failure. Perfect 10 references a single page from CCBill and CWIE’s “DMCA Log.” Although this page shows some empty fields in the spreadsheet column labeled “Webmasters [sic] Name,” Perfect 10’s conclusion that the DMCA Log thus “does not reflect any effort to track notices of infringements received by webmaster identity” is not supported by evidence in the record. The remainder of the DMCA Log indicates that the email address and/or name of the webmaster is routinely recorded in CCBill and CWIE’s DMCA Log. CCBill’s interrogatory responses dated December 11, 2003 also contain a chart indicating that CCBill and CWIE largely kept track of the webmaster for each website.

[5] Unlike Ellison and Aimster, where the changed email address and the encryption system ensured that no information about the repeat infringer was collected, it is undisputed that CCBill and CWIE recorded most webmasters. The district court properly concluded that the DMCA Log does not raise a triable issue of fact that CCBill and CWIE did not implement a repeat infringer policy.

2. Reaonableness

[6] A service provider reasonably implements its repeat infringer policy if it terminates users when “appropriate.” See Corbis, 351 F. Supp. 2d at 1104. Section 512(i) itself does not clarify when it is “appropriate” for service providers to act. It only requires that a service provider terminate users who are “repeat infringers.”

[7] To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement. Section 512(c) states that “[a] service provider shall not be liable for monetary relief” if it does not know of infringement. A service provider is also not liable
under § 512(c) if it acts “expeditiously to remove, or disable access to, the material” when it (1) has actual knowledge, (2) is aware of facts or circumstances from which infringing activity is apparent, or (3) has received notification of claimed infringement meeting the requirements of § 512(c)(3). Were we to require service providers to terminate users under circumstances other than those specified in § 512(c), § 512(c)’s grant of immunity would be meaningless. This interpretation of the statute is supported by legislative history. See H.R. Rep., at 61 (Section 512(i) is not intended “to undermine the . . . knowledge standard of [§ 512(c)].”).

Perfect 10 claims that CCBill and CWIE unreasonably implemented their repeat infringer policies by tolerating flagrant and blatant copyright infringement by its users despite notice of infringement from Perfect 10, notice of infringement from copyright holders not a party to this litigation and “red flags” of copyright infringement.

a. **Perfect 10’s Claimed Notice of Infringement**

Perfect 10 argues that CCBill and CWIE implemented their repeat infringer policy in an unreasonable manner because CCBill and CWIE received notices of infringement from Perfect 10, and yet the infringement identified in these notices continued. The district court found that Perfect 10 did not provide notice that substantially complied with the requirements of § 512(c)(3), and thus did not raise a genuine issue of mate-

---

2Section 512(c)(3) reads:

(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.
rial fact as to whether CCBill and CWIE reasonably implemented their repeat infringer policy. We agree.

[8] Compliance is not “substantial” if the notice provided complies with only some of the requirements of § 512(c)(3)(A). Section 512(c)(3)(B)(ii) explains that a service provider will not be deemed to have notice of infringement when “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)” so long as the service provider responds to the inadequate notice and explains the requirements for substantial compliance. The statute thus signals that substantial compliance means substantial compliance with all of § 512(c)(3)’s clauses, not just some of them. See H.R. Rep., at 56 (A communication substantially complies even if it contains technical errors such as

(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.
Perfect 10 claims that it met the requirements of § 512(c)(3) through a combination of three sets of documents. The first set of documents is a 22,185 page bates-stamped production on October 16, 2002 that includes pictures with URLs of Perfect 10 models allegedly posted on CCBill or CWIE client websites. The October 16, 2002 production did not contain a statement under penalty of perjury that the complaining party was authorized to act, as required by § 512(c)(3)(A)(vi). The second set of documents was also not sworn to, and consisted of a spreadsheet emailed to Fisher on July 14, 2003 identifying the Perfect 10 models in the October 16, 2002 production by bates number. On December 2, 2003, Perfect 10 completed interrogatory responses which were signed under penalty of perjury. These responses incorporated the July 14, 2003 spreadsheet by reference.

[9] Taken individually, Perfect 10’s communications do not substantially comply with the requirements of § 512(c)(3). Each communication contains more than mere technical errors; often one or more of the required elements are entirely absent. See Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1100-01 (C.D. Cal. 2004) (“Order”). In order to substantially comply with § 512(c)(3)’s requirements, a notification must do more than identify infringing files. The DMCA requires a complainant to declare, under penalty of perjury, that he is authorized to represent the copyright holder, and that he has a good-faith belief that the use is infringing. This requirement is not superfluous. Accusations of alleged infringement have drastic consequences: A user could have

---

3We do not read the Fourth Circuit’s holding in ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001), as holding that only location information is required for substantial compliance with the terms of § 512(c)(3).
content removed, or may have his access terminated entirely. If the content infringes, justice has been done. But if it does not, speech protected under the First Amendment could be removed. We therefore do not require a service provider to start potentially invasive proceedings if the complainant is unwilling to state under penalty of perjury that he is an authorized representative of the copyright owner, and that he has a good-faith belief that the material is unlicensed.4

Permitting a copyright holder to cobble together adequate notice from separately defective notices also unduly burdens service providers. Indeed, the text of § 512(c)(3) requires that the notice be “a written communication.” (Emphasis added). Again, this requirement is not a mere technicality. It would have taken Fisher substantial time to piece together the relevant information for each instance of claimed infringement. To do so, Fisher would have to first find the relevant line in the spreadsheet indicating ownership information, then comb the 22,185 pages provided by Perfect 10 in order to find the appropriate image, and finally copy into a browser the location printed at the top of the page—a location which was, in some instances, truncated. The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider; Perfect 10’s separate communications are inadequate.

[10] Since Perfect 10 did not provide effective notice, knowledge of infringement may not be imputed to CCBill or

4Perfect 10’s argument that its initial notice substantially complied with the DMCA’s notice requirements because Fisher, the recipient of that notice, admitted that he could have found the infringing photographs on the basis of the October 16, 2002, bates-stamped production, is thus beside the point. Without the predicate certification under penalty of perjury, Fisher would have had no reason to go looking for the photographs.
CWIE based on Perfect 10’s communications. Perfect 10’s attempted notice does not raise a genuine issue of material fact that CCBill and CWIE failed to reasonably implement a repeat infringer policy within the meaning of § 512(i)(1)(A).

b. Non-Party Notices

Perfect 10 also cites to notices of infringement by other copyright holders, and argues that CCBill and CWIE did not reasonably implement their repeat infringer policies because they continued to provide services for websites that infringed non-party copyrights. The district court expressly declined to consider evidence of notices provided by any party other than Perfect 10 on the basis that these notices were irrelevant to Perfect 10’s claims. We disagree.

[11] CCBill and CWIE’s actions towards copyright holders who are not a party to the litigation are relevant in determining whether CCBill and CWIE reasonably implemented their repeat infringer policy. Section 512(i)(1)(A) requires an assessment of the service provider’s “policy,” not how the service provider treated a particular copyright holder. See Ellison, 357 F.3d at 1080 (AOL’s repeat infringer policy was not reasonably implemented because copyright holders other than Ellison could have attempted to notify AOL during the time that AOL’s email address was incorrectly listed.). Thus, CCBill and CWIE’s response to adequate non-party notifications is relevant in determining whether they reasonably implemented their policy against repeat infringers.

[12] A policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement. The district court in this case did not consider any evidence relating to copyright holders other than Perfect 10. We remand for determination of whether CCBill and/or CWIE implemented its repeat infringer policy in an unreasonable manner with respect to any copyright holder other than Perfect 10.
c. Apparent Infringing Activity

[13] In importing the knowledge standards of § 512(c) to the analysis of whether a service provider reasonably implemented its § 512(i) repeat infringer policy, Congress also imported the “red flag” test of § 512(c)(1)(A)(ii). Under this section, a service provider may lose immunity if it fails to take action with regard to infringing material when it is "aware of facts or circumstances from which infringing activity is apparent." § 512(c)(1)(A)(ii). Notice that fails to substantially comply with § 512(c)(3), however, cannot be deemed to impart such awareness. §§ 512(c)(3)(B)(i) & (ii).

Perfect 10 alleges that CCBill and CWIE were aware of a number of “red flags” that signaled apparent infringement. Because CWIE and CCBill provided services to “illegal.net” and “stolencelebritypics.com,” Perfect 10 argues that they must have been aware of apparent infringing activity. We disagree. When a website traffics in pictures that are titillating by nature, describing photographs as “illegal” or “stolen” may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.

Perfect 10 also argues that a disclaimer posted on illegal.net made it apparent that infringing activity had taken place. Perfect 10 alleges no facts showing that CWIE and CCBill were aware of that disclaimer, and, in any event, we disagree that the disclaimer made infringement apparent. The disclaimer in question stated: “The copyrights of these files remain the creator's. I do not claim any rights to these files, other than the right to post them.” Contrary to Perfect 10’s assertion, this disclaimer is not a “red flag” of infringement. The disclaimer specifically states that the webmaster has the right to post the files.

In addition, Perfect 10 argues that password-hacking websites, hosted by CWIE, also obviously infringe. While such
sites may not directly infringe on anyone's copyright, they may well contribute to such infringement. The software provided by Grokster in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), also did not itself infringe, but did enable users to swap infringing files. *Grokster* held that "instructing [users] how to engage in an infringing use" could constitute contributory infringement. *Id.* at 936. Similarly, providing passwords that enable users to illegally access websites with copyrighted content may well amount to contributory infringement.

[14] However, in order for a website to qualify as a "red flag" of infringement, it would need to be apparent that the website instructed or enabled users to infringe another's copyright. See *A&M Records, Inc. v. Napster, Inc.*., 239 F.3d 1004, 1013 n.2 (9th Cir. 2001). We find that the burden of determining whether passwords on a website enabled infringement is not on the service provider. The website could be a hoax, or out of date. The owner of the protected content may have supplied the passwords as a short-term promotion, or as an attempt to collect information from unsuspecting users. The passwords might be provided to help users maintain anonymity without infringing on copyright. There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers. Password-hacking websites are thus not *per se* "red flags" of infringement.

[15] Perfect 10 also alleges that "red flags" raised by third parties identified repeat infringers who were not terminated. Because the district court did not consider potential red flags raised by third parties, we remand to the district court to determine whether third-party notices made CCBill and CWIE aware that it provided services to repeat infringers, and if so, whether they responded appropriately.
B. Standard Technical Measures: § 512(i)(1)(B)

[16] Under § 512(i)(1)(B), a service provider that interferes with "standard technical measures" is not entitled to the safe harbors at §§ 512(a)-(d). "Standard technical measures" refers to a narrow group of technology-based solutions to online copyright infringement:

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.

§ 512(i)(2). Perfect 10 argues that CCBill does not qualify for any safe harbor because it interfered with "standard technical measures" by blocking Perfect 10's access to CCBill affiliated websites in order to prevent Perfect 10 from discovering whether those websites infringed Perfect 10 copyrights.

There are two disputed facts here.

We are unable to determine on this record whether accessing websites is a standard technical measure, which was "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process." § 512(i)(2)(A). We thus remand to the district court to determine whether access to a website
is a "standard technical measure," and if so, whether CCBill interfered with that access.

[17] If allowing access is a standard technical measure, CCBill claims it only blocked Perfect 10's credit card because Perfect 10 had previously reversed charges for subscriptions; Perfect 10 insists it did so in order to prevent Perfect 10 from identifying infringing content. If CCBill is correct, Perfect 10's method of identifying infringement—forcing CCBill to pay the fines and fees associated with chargebacks—may well impose a substantial cost on CCBill. If not, CCBill may well have interfered with Perfect 10's efforts to police the websites in question for possible infringements. Because there are disputed issues of material fact, we remand to the district court for a determination of whether CCBill's refusal to process Perfect 10's transactions interfered with a "standard technical measure" for identifying infringement.

C. Transitory Digital Network Communications: § 512(a)

[18] Section 512(a) provides safe harbor for service providers who act as conduits for infringing content. In order to qualify for the safe harbor of § 512(a), a party must be a service provider under a more restrictive definition than applicable to the other safe harbors provided under § 512:

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.

Section 512 (k)(1)(A). The district court held that CCBill met the requirements of § 512(k)(1)(A) by "provid[ing] a connection to the material on its clients' websites through a system
which it operates in order to provide its clients with billing services." Order at 1102. We reject Perfect 10's argument that CCBill is not eligible for immunity under § 512(a) because it does not itself transmit the infringing material. A service provider is "an entity offering the transmission, routing, or providing of connections for digital online communications." § 512(k)(1)(A). There is no requirement in the statute that the communications must themselves be infringing, and we see no reason to import such a requirement. It would be perverse to hold a service provider immune for transmitting information that was infringing on its face, but find it contributorily liable for transmitting information that did not infringe.

Section 512(a) provides a broad grant of immunity to service providers whose connection with the material is transient. When an individual clicks on an Internet link, his computer sends a request for the information. The company receiving that request sends that request on to another computer, which sends it on to another. After a series of such transmissions, the request arrives at the computer that stores the information. The requested information is then returned in milliseconds, not necessarily along the same path. In passing the information along, each intervening computer makes a short-lived copy of the data. A short time later, the information is displayed on the user's computer.

[19] Those intervening computers provide transient connections among users. The Internet as we know it simply cannot exist if those intervening computers must block indirectly infringing content. We read § 512(a)'s grant of immunity exactly as it is written: Service providers are immune for transmitting all digital online communications, not just those that directly infringe.

[20] CCBill transmits credit card information and proof of payment, both of which are "digital online communications." However, we have little information as to how CCBill sends the payment it receives to its account holders. It is unclear
whether such payment is a digital communication, transmitted without modification to the content of the material, or transmitted often enough that CCBill is only a transient holder. On the record before us, we cannot conclude that CCBill is a service provider under § 512(a). Accordingly, we remand to the district court for further consideration the issue of whether CCBill meets the requirements of § 512(a).

D. Information Location Tools: § 512(d)

After CCBill processes a consumer’s credit card and issues a password granting access to a client website, CCBill displays a hyperlink so that the user may access the client website. CCBill argues that it falls under the safe harbor of § 512(d) by displaying this hyperlink at the conclusion of the consumer transaction. We disagree. Section 512(d) reads:

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.

Even if the hyperlink provided by CCBill could be viewed as an “information location tool,” the majority of CCBill’s functions would remain outside of the safe harbor of § 512(d). Section 512(d) provides safe harbor only for “infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity.” (Emphasis added). Perfect 10 does not claim that CCBill infringed its copyrights by providing a hyperlink; rather, Perfect 10 alleges infringement through CCBill’s performance of other business services for these websites. Even if CCBill’s provision of a hyperlink is immune under
§ 512(n), CCBill does not receive blanket immunity for its other services.

E. Information Residing on Systems or Networks at the Direction of Users: § 512(c)

Section 512(c) "limits the liability of qualifying service providers for claims of direct, vicarious, and contributory infringement for 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." H.R. Rep., at 53. A service provider qualifies for safe harbor under § 512(c) if it meets the requirements of § 512(i) and:

(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.

Section 512(c)(1). As discussed above, Perfect 10 did not provide CWIE with knowledge or awareness within the standard
of § 512(c)(1)(A), and Perfect 10 did not provide notice that complies with the requirements of § 512(c)(3).

[21] The remaining question is whether Perfect 10 raises a genuine issue of material fact that CWIE does not qualify for safe harbor under § 512(c) because it fails to meet the requirements of § 512(c)(1)(B), namely, that a service provider not receive a direct financial benefit from the infringing activity if the service provider also has the right and ability to control the infringing activity.

[22] Based on the “well-established rule of construction that where Congress uses terms that have accumulated settled meaning under common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms,” Rossi, 391 F.3d at 1004 n.4 (9th Cir. 2004) (quoting Neder v. United States, 527 U.S. 1, 21 (1999)), we hold that “direct financial benefit” should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability. See, e.g., Ellison, 357 F.3d at 1078 (a vicariously liable copyright infringer “derive[s] a direct financial benefit from the infringement and ha[s] the right and ability to supervise the infringing activity”). Thus, the relevant inquiry is “whether the infringing activity constitutes a draw for subscribers, not just an added benefit.” Id. at 1079. In Ellison, the court held that “no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material” because “[t]he record lacks evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL’s eventual obstruction of the infringement.” Id.

[23] In this case, Perfect 10 provides almost no evidence about the alleged direct financial benefit to CWIE. Perfect 10 only alleges that “CWIE ‘hosts’ websites for a fee.” This allegation is insufficient to show that the infringing activity was “a draw” as required by Ellison. 357 F.3d at 1079. Further-
more, the legislative history expressly states that "receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity.'" H.R. Rep., at 54. Perfect 10 has not raised a genuine issue of material fact that CWIE receives a direct financial benefit from infringing activity. Because CWIE does not receive a direct financial benefit, CWIE meets the requirements of § 512(c).

[24] If the district court finds that CWIE meets the threshold requirements of § 512(i), CWIE is entitled to safe harbor under § 512(c).

II. COMMUNICATIONS DECENCY ACT

[25] The Communications Decency Act states that "[n]o 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," and expressly preempts any state law to the contrary. 47 U.S.C. §§ 230(c)(1), (e)(3). "The majority of federal circuits have interpreted the CDA to establish broad 'federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.'" Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006) (quoting Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997)); see also Carafano v. Metro. splash.com, Inc., 339 F.3d 1185, 1192 (9th Cir. 2003) (citing Batts v. Smith, 333 F.3d 1018, 1026-27 (9th Cir. 2003)).

The immunity created by § 230(c)(1) is limited by § 230(c)(2), which requires the court to "construe Section 230(c)(1) in a manner that would neither 'limit or expand any law pertaining to intellectual property.'" Gucci Am., Inc. v. Hall & Assoc., 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (quoting § 230(c)(2)). As a result, the CDA does not clothe
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

PERFECT 10, INC., a California corporation,

Plaintiff-Appellant,

v.

AMAZON.COM, INC., a corporation;
A9.COM INC., a corporation,

Defendants-Appellees.

No. 06-55405
D.C. No.
CV-05-04753-AHM

PERFECT 10, INC., a California corporation,

Plaintiff-Appellant,

v.

GOOGLE INC., a corporation,

Defendant-Appellee.

No. 06-55406
D.C. No.
CV-04-09484-AHM

PERFECT 10, INC., a California corporation,

Plaintiff-Appellee,

v.

GOOGLE INC., a corporation,

Defendant-Appellant.

No. 06-55425
D.C. No.
CV-04-09484-AHM

5751
America, and Internet Commerce Coalition in support of Google Inc.


OPINION

IKUTA, Circuit Judge:

In this appeal, we consider a copyright owner’s efforts to stop an Internet search engine from facilitating access to infringing images. Perfect 10, Inc. sued Google Inc., for infringing Perfect 10’s copyrighted photographs of nude models, among other claims. Perfect 10 brought a similar action against Amazon.com and its subsidiary A9.com (collectively, “Amazon.com”). The district court preliminarily enjoined Google from creating and publicly displaying thumbnail versions of Perfect 10’s images, Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828 (C.D. Cal. 2006), but did not enjoin Google from linking to third-party websites that display infringing full-size versions of Perfect 10’s images. Nor did the district court preliminarily enjoin Amazon.com from giving users access to information provided by Google. Perfect 10 and Google both appeal the district court’s order. We have jurisdiction pursuant to 28 U.S.C. § 1292(a)(1).³

³Google argues that we lack jurisdiction over the preliminary injunction to the extent it enforces unregistered copyrights. Registration is generally a jurisdictional prerequisite to a suit for copyright infringement. See 17
The district court handled this complex case in a particularly thoughtful and skillful manner. Nonetheless, the district court erred on certain issues, as we will further explain below. We affirm in part, reverse in part, and remand.

I

Background

Google's computers, along with millions of others, are connected to networks known collectively as the "Internet." "The Internet is a world-wide network of networks . . . all sharing a common communications technology." Religious Tech. Ctr. v. Netcom On-Line Comm'n Servs., Inc., 923 F. Supp. 1231, 1238 n.1 (N.D. Cal. 1995). Computer owners can provide information stored on their computers to other users connected to the Internet through a medium called a webpage. A webpage consists of text interspersed with instructions written in Hypertext Markup Language ("HTML") that is stored in a computer. No images are stored on a webpage; rather, the HTML instructions on the webpage provide an address for where the images are stored, whether in the webpage publisher's computer or some other computer. In general, webpages are publicly available and can be accessed by computers connected to the Internet through the use of a web browser.

U.S.C. § 411. But section 411 does not limit the remedies a court can grant. Rather, the Copyright Act gives courts broad authority to issue injunctive relief. See 17 U.S.C. § 502(a). Once a court has jurisdiction over an action for copyright infringement under section 411, the court may grant injunctive relief to restrain infringement of any copyright, whether registered or unregistered. See, e.g., Olan Mills, Inc. v. Linn Photo Co., 23 F.3d 1345, 1349 (8th Cir. 1994); Pac. & S. Co., Inc. v. Duncan, 744 F.2d 1490, 1499 n.17 (11th Cir. 1984). Because at least some of the Perfect 10 images at issue were registered, the district court did not err in determining that it could issue an order that covers unregistered works. Therefore, we have jurisdiction over the district court's decision and order.
Google operates a search engine, a software program that automatically accesses thousands of websites (collections of webpages) and indexes them within a database stored on Google’s computers. When a Google user accesses the Google website and types in a search query, Google’s software searches its database for websites responsive to that search query. Google then sends relevant information from its index of websites to the user’s computer. Google’s search engines can provide results in the form of text, images, or videos.

The Google search engine that provides responses in the form of images is called “Google Image Search.” In response to a search query, Google Image Search identifies text in its database responsive to the query and then communicates to users the images associated with the relevant text. Google’s software cannot recognize and index the images themselves. Google Image Search provides search results as a webpage of small images called “thumbnails,” which are stored in Google’s servers. The thumbnail images are reduced, lower-resolution versions of full-sized images stored on third-party computers.

When a user clicks on a thumbnail image, the user’s browser program interprets HTML instructions on Google’s webpage. These HTML instructions direct the user’s browser to cause a rectangular area (a “window”) to appear on the user’s computer screen. The window has two separate areas of information. The browser fills the top section of the screen with information from the Google webpage, including the thumbnail image and text. The HTML instructions also give the user’s browser the address of the website publisher’s computer that stores the full-size version of the thumbnail.² By

²The website publisher may not actually store the photographic images used on its webpages in its own computer, but may provide HTML instructions directing the user’s browser to some further computer that stores the image. Because this distinction does not affect our analysis, for convenience, we will assume that the website publisher stores all images used on its webpages in the website publisher’s own computer.
following the HTML instructions to access the third-party webpage, the user’s browser connects to the website publisher’s computer, downloads the full-size image, and makes the image appear at the bottom of the window on the user’s screen. Google does not store the images that fill this lower part of the window and does not communicate the images to the user; Google simply provides HTML instructions directing a user’s browser to access a third-party website. However, the top part of the window (containing the information from the Google webpage) appears to frame and comment on the bottom part of the window. Thus, the user’s window appears to be filled with a single integrated presentation of the full-size image, but it is actually an image from a third-party website framed by information from Google’s website. The process by which the webpage directs a user’s browser to incorporate content from different computers into a single window is referred to as “in-line linking.” *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 816 (9th Cir. 2003). The term “framing” refers to the process by which information from one computer appears to frame and annotate the in-line linked content from another computer. *Perfect 10*, 416 F. Supp. 2d at 833-34.

Google also stores webpage content in its cache.\(^3\) For each cached webpage, Google’s cache contains the text of the webpage as it appeared at the time Google indexed the page, but does not store images from the webpage. *Id.* at 833. Google may provide a link to a cached webpage in response to a

\(^3\)Generally, a “cache” is “a computer memory with very short access time used for storage of frequently or recently used instructions or data.” *United States v. Ziegler*, 474 F.3d 1184, 1186 n.3 (9th Cir. 2007) (quoting *MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY* 171 (11th ed. 2003)). There are two types of caches at issue in this case. A user’s personal computer has an internal cache that saves copies of webpages and images that the user has recently viewed so that the user can more rapidly revisit these webpages and images. Google’s computers also have a cache which serves a variety of purposes. Among other things, Google’s cache saves copies of a large number of webpages so that Google’s search engine can efficiently organize and index these webpages.
user’s search query. However, Google’s cache version of the webpage is not automatically updated when the webpage is revised by its owner. So if the webpage owner updates its webpage to remove the HTML instructions for finding an infringing image, a browser communicating directly with the webpage would not be able to access that image. However, Google’s cache copy of the webpage would still have the old HTML instructions for the infringing image. Unless the owner of the computer changed the HTML address of the infringing image, or otherwise rendered the image unavailable, a browser accessing Google’s cache copy of the website could still access the image where it is stored on the website publisher’s computer. In other words, Google’s cache copy could provide a user’s browser with valid directions to an infringing image even though the updated webpage no longer includes that infringing image.

In addition to its search engine operations, Google generates revenue through a business program called “AdSense.” Under this program, the owner of a website can register with Google to become an AdSense “partner.” The website owner then places HTML instructions on its webpages that signal Google’s server to place advertising on the webpages that is relevant to the webpages’ content. Google’s computer program selects the advertising automatically by means of an algorithm. AdSense participants agree to share the revenues that flow from such advertising with Google.

Google also generated revenues through an agreement with Amazon.com that allowed Amazon.com to in-line link to Google’s search results. Amazon.com gave its users the impression that Amazon.com was providing search results, but Google communicated the search results directly to Amazon.com’s users. Amazon.com routed users’ search queries to Google and automatically transmitted Google’s responses (i.e., HTML instructions for linking to Google’s search results) back to its users.
Perfect 10 markets and sells copyrighted images of nude models. Among other enterprises, it operates a subscription website on the Internet. Subscribers pay a monthly fee to view Perfect 10 images in a "members' area" of the site. Subscribers must use a password to log into the members' area. Google does not include these password-protected images from the members' area in Google's index or database. Perfect 10 has also licensed Fonestarz Media Limited to sell and distribute Perfect 10's reduced-size copyrighted images for download and use on cell phones.

Some website publishers republish Perfect 10's images on the Internet without authorization. Once this occurs, Google's search engine may automatically index the webpages containing these images and provide thumbnail versions of images in response to user inquiries. When a user clicks on the thumbnail image returned by Google's search engine, the user's browser accesses the third-party webpage and in-line links to the full-sized infringing image stored on the website publisher's computer. This image appears, in its original context, on the lower portion of the window on the user's computer screen framed by information from Google's webpage.

Procedural History. In May 2001, Perfect 10 began notifying Google that its thumbnail images and in-line linking to the full-size images infringed Perfect 10's copyright. Perfect 10 continued to send these notices through 2005.

On November 19, 2004, Perfect 10 filed an action against Google that included copyright infringement claims. This was followed by a similar action against Amazon.com on June 29, 2005. On July 1, 2005 and August 24, 2005, Perfect 10 sought a preliminary injunction to prevent Amazon.com and Google, respectively, from "copying, reproducing, distributing, publicly displaying, adapting or otherwise infringing, or contributing to the infringement" of Perfect 10's photographs; linking to websites that provide full-size infringing versions
of Perfect 10's photographs; and infringing Perfect 10's username/password combinations."

The district court consolidated the two actions and heard both preliminary injunction motions on November 7, 2005. The district court issued orders granting in part and denying in part the preliminary injunction against Google and denying the preliminary injunction against Amazon.com. Perfect 10 and Google cross-appealed the partial grant and partial denial of the preliminary injunction motion, and Perfect 10 appealed the denial of the preliminary injunction against Amazon.com. On June 15, 2006, the district court temporarily stayed the preliminary injunction.

II

Standard of Review

We review the district court's grant or denial of a preliminary injunction for an abuse of discretion. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001). The district court must support a preliminary injunction with findings of fact, which we review for clear error. Earth Island Inst. v. U.S. Forest Serv., 442 F.3d 1147, 1156 (9th Cir. 2006). We review the district court's conclusions of law de novo. Napster, 239 F.3d at 1013.

11] Section 502(a) of the Copyright Act authorizes a court to grant injunctive relief "on such terms as it may deem reasonable to prevent or restrain infringement of a copyright." 17 U.S.C. § 502(a). Preliminary injunctive relief is available to a party who demonstrates either: (1) a combination of probable success on the merits and the possibility of irreparable harm; or (2) that serious questions are raised and the balance of hardships tips in its favor. These two formulations represent two points on a sliding scale in which the required degree of irreparable harm increases as the probability of success
Because Perfect 10 has the burden of showing a likelihood of success on the merits, the district court held that Perfect 10 also had the burden of demonstrating a likelihood of overcoming Google's fair use defense under 17 U.S.C. § 107. Perfect 10, 416 F. Supp. 2d at 836-37. We have not previously ruled on this issue, see Napster, 239 F.3d at 1014 n.3 (cataloguing conflicting authority), and we now agree with the district court’s ruling. In order to demonstrate its likely success on the merits, the moving party must necessarily demonstrate it will overcome defenses raised by the non-moving party. This burden is correctly placed on the party seeking to demonstrate entitlement to the extraordinary remedy of a preliminary injunction at an early stage of the litigation, before the defendant has had the opportunity to undertake extensive discovery or develop its defenses. Our conclusion that a party seeking a preliminary injunction in the copyright context bears the burden of showing its likely success in overcoming a fair use defense is consistent with decisions of the Federal Circuit purporting to apply Ninth Circuit law. See Atari Games Corp. v. Nintendo of Am. Inc., 975 F.2d 832, 837 (Fed. Cir. 1992) (“[F]ollowing Ninth Circuit caselaw [for review of a district court’s grant of preliminary injunction], this court must determine whether Nintendo has shown a likelihood of success on its prima facie case of copyright infringement and a likelihood that it will overcome Atari’s copyright misuse defense.”); see also H.H. Robertson, Co. v. United Steel Deck, Inc., 820 F.2d 384, 387-89 (Fed. Cir. 1987) (requiring a patent holder seeking preliminary injunctive relief to overcome the defense that the patent is invalid even though the patent is presumed valid at trial), overruled on other grounds by Markman v. Westview Instruments, Inc., 52 F.3d 967, 977-79 (Fed. Cir. 1995).

However, entitlement for preliminary relief “is determined in the context of the presumptions and burdens that
would inhere at trial on the merits.” *H.H. Robertson*, 820 F.2d at 388. Because the defendant in an infringement action has the burden of proving fair use, see *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 590 (1994), the defendant is responsible for introducing evidence of fair use in responding to a motion for preliminary relief. See *Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1403 (9th Cir. 1997). The plaintiff must then show it is likely to succeed in its challenge to the alleged infringer’s evidence.

Google also raises an affirmative defense under title II of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 512. Congress enacted title II of the DMCA “to provide greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.” *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (internal quotation omitted). Sections 512(a) through (d) limit liability for (respectively): “(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.” *Id.* at 1077. A service provider that qualifies for such protection is not liable for monetary relief and may be subject only to the narrow injunctive relief set forth in section 512(j). 17 U.S.C. § 512(a). In order to obtain preliminary injunctive relief beyond what is allowed by title II of the DMCA, Perfect 10 must also demonstrate a likelihood of overcoming Google’s defenses under title II of the DMCA.

4Perfect 10 argues that we are bound by the language and structure of title II of the DMCA in determining Google’s liability for copyright infringement. We have noted that the DMCA does not change copyright law; rather, “Congress provided that [the DMCA’s] limitations of liability apply if the provider is found to be liable under existing principles of law.” *Ellison*, 357 F.3d at 1077 (emphasis and internal quotation omitted). As a result, “[c]laims against service providers for direct, contributory, or vicarious copyright infringement, therefore, are generally evaluated just as they would be in the non-online world.” *Id.*; see also 17 U.S.C. § 512(f) (“The failure of a service provider’s conduct to qualify for limitation of
III

Direct Infringement

Perfect 10 claims that Google’s search engine program directly infringes two exclusive rights granted to copyright holders: its display rights and its distribution rights. 8 “Plaintiffs must satisfy two requirements to present a prima facie case of direct infringement: (1) they must show ownership of the allegedly infringed material and (2) they must demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders under 17 U.S.C. § 106.” Napster, 239 F.3d at 1013; see 17 U.S.C. § 501(a). Even if a plaintiff satisfies these two requirements and makes a prima facie case of direct infringement, the defendant may avoid liability if it

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.”). Therefore, we must consider Google’s potential liability under the Copyright Act without reference to title II of the DMCA.

817 U.S.C. § 106 states, in pertinent part:

Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

(1) to reproduce the copyrighted work in copies or phonorecords;

(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

(5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly
can establish that its use of the images is a “fair use” as set forth in 17 U.S.C. § 107. See Kelly, 336 F.3d at 817.

Perfect 10’s ownership of at least some of the images at issue is not disputed. See Perfect 10, 416 F. Supp. 2d at 836.

The district court held that Perfect 10 was likely to prevail in its claim that Google violated Perfect 10’s display right with respect to the infringing thumbnails. Id. at 844. However, the district court concluded that Perfect 10 was not likely to prevail on its claim that Google violated either Perfect 10’s display or distribution right with respect to its full-size infringing images. Id. at 844-45. We review these rulings for an abuse of discretion. Napster, 239 F.3d at 1013.

A. Display Right

In considering whether Perfect 10 made a prima facie case of violation of its display right, the district court reasoned that a computer owner that stores an image as electronic information and serves that electronic information directly to the user (“i.e., physically sending ones and zeroes over the Internet to the user’s browser,” Perfect 10, 416 F. Supp. 2d at 839) is displaying the electronic information in violation of a copyright holder’s exclusive display right. Id. at 843-45; see 17 U.S.C. § 106(5). Conversely, the owner of a computer that does not store and serve the electronic information to a user is not displaying that information, even if such owner in-line links to or frames the electronic information. Perfect 10, 416 F. Supp. 2d at 843-45. The district court referred to this test as the “server test.” Id. at 838-39.

Applying the server test, the district court concluded that Perfect 10 was likely to succeed in its claim that Google’s thumbnails constituted direct infringement but was unlikely to succeed in its claim that Google’s in-line linking to full-size infringing images constituted a direct infringement. Id. at 843-45. As explained below, because this analysis comports with
the language of the Copyright Act, we agree with the district court’s resolution of both these issues.

[4] We have not previously addressed the question when a computer displays a copyrighted work for purposes of section 106(5). Section 106(5) states that a copyright owner has the exclusive right “to display the copyrighted work publicly.” The Copyright Act explains that “display” means “to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process . . . .” 17 U.S.C. § 101. Section 101 defines “copies” as “material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.” Id. Finally, the Copyright Act provides that “[a] work is ‘fixed’ in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.” Id.

[5] We must now apply these definitions to the facts of this case. A photographic image is a work that is “‘fixed’ in a tangible medium of expression,” for purposes of the Copyright Act, when embodied (i.e., stored) in a computer’s server (or hard disk, or other storage device). The image stored in the computer is the “copy” of the work for purposes of copyright law. See MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 517-18 (9th Cir. 1993) (a computer makes a “copy” of a software program when it transfers the program from a third party’s computer (or other storage device) into its own memory, because the copy of the program recorded in the computer is “fixed” in a manner that is “sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration” (quoting 17 U.S.C. § 101)). The computer owner shows a copy “by means of a . . . device or process” when the owner
uses the computer to fill the computer screen with the photographic image stored on that computer, or by communicating the stored image electronically to another person’s computer. 17 U.S.C. § 101. In sum, based on the plain language of the statute, a person displays a photographic image by using a computer to fill a computer screen with a copy of the photographic image fixed in the computer’s memory. There is no dispute that Google’s computers store thumbnail versions of Perfect 10’s copyrighted images and communicate copies of those thumbnails to Google’s users. Therefore, Perfect 10 has made a prima facie case that Google’s communication of its stored thumbnail images directly infringes Perfect 10’s display right.

[6] Google does not, however, display a copy of full-size infringing photographic images for purposes of the Copyright Act when Google frames in-line linked images that appear on a user’s computer screen. Because Google’s computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act. In other words, Google does not have any “material objects . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated” and thus cannot communicate a copy. 17 U.S.C. § 101.

[7] Instead of communicating a copy of the image, Google provides HTML instructions that direct a user’s browser to a website publisher’s computer that stores the full-size photographic image. Providing these HTML instructions is not equivalent to showing a copy. First, the HTML instructions are lines of text, not a photographic image. Second, HTML

---

6Because Google initiates and controls the storage and communication of these thumbnail images, we do not address whether an entity that merely passively owns and manages an Internet bulletin board or similar system violates a copyright owner’s display and distribution rights when the users of the bulletin board or similar system post infringing works. Cf. CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004).
instructions do not themselves cause infringing images to appear on the user’s computer screen. The HTML merely gives the address of the image to the user’s browser. The browser then interacts with the computer that stores the infringing image. It is this interaction that causes an infringing image to appear on the user’s computer screen. Google may facilitate the user’s access to infringing images. However, such assistance raises only contributory liability issues, see Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 929-30 (2005), Napster, 239 F.3d at 1019, and does not constitute direct infringement of the copyright owner’s display rights.

Perfect 10 argues that Google displays a copy of the full-size images by framing the full-size images, which gives the impression that Google is showing the image within a single Google webpage. While in-line linking and framing may cause some computer users to believe they are viewing a single Google webpage, the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion. Cf. 15 U.S.C. § 1114(1) (providing that a person who uses a trademark in a manner likely to cause confusion shall be liable in a civil action to the trademark registrant). 7

Nor does our ruling that a computer owner does not display

7Perfect 10 also argues that Google violates Perfect 10’s right to display full-size images because Google’s in-line linking meets the Copyright Act’s definition of “to perform or display a work ‘publicly.’” 17 U.S.C. § 101. This phrase means “to transmit or otherwise communicate a performance or display of the work to . . . the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.” Id. Perfect 10 is mistaken. Google’s activities do not meet this definition because Google transmits or communicates only an address which directs a user’s browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself.
a copy of an image when it communicates only the HTML address of the copy erroneously collapse the display right in section 106(5) into the reproduction right set forth in section 106(1). Nothing in the Copyright Act prevents the various rights protected in section 106 from overlapping. Indeed, under some circumstances, more than one right must be infringed in order for an infringement claim to arise. For example, a “Game Genie” device that allowed a player to alter features of a Nintendo computer game did not infringe Nintendo’s right to prepare derivative works because the Game Genie did not incorporate any portion of the game itself. See Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 964 F.2d 965, 967 (9th Cir. 1992). We held that a copyright holder’s right to create derivative works is not infringed unless the alleged derivative work “incorporate[s] a protected work in some concrete or permanent ‘form.’” Id. In other words, in some contexts, the claimant must be able to claim infringement of its reproduction right in order to claim infringement of its right to prepare derivative works.

[8] Because Google’s cache merely stores the text of webpages, our analysis of whether Google’s search engine program potentially infringes Perfect 10’s display and distribution rights is equally applicable to Google’s cache. Perfect 10 is not likely to succeed in showing that a cached webpage that in-line links to full-size infringing images violates such rights. For purposes of this analysis, it is irrelevant whether cache copies direct a user’s browser to third-party images that are no longer available on the third party’s website, because it is the website publisher’s computer, rather than Google’s computer, that stores and displays the infringing image.

B. Distribution Right

The district court also concluded that Perfect 10 would not likely prevail on its claim that Google directly infringed Perfect 10’s right to distribute its full-size images. Perfect 10,
416 F. Supp. 2d at 844–45. The district court reasoned that distribution requires an “actual dissemination” of a copy. Id. at 844. Because Google did not communicate the full-size images to the user’s computer, Google did not distribute these images. Id.

Again, the district court’s conclusion on this point is consistent with the language of the Copyright Act. Section 106(3) provides that the copyright owner has the exclusive right “to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending.” 17 U.S.C. § 106(3). As noted, “copies” means “material objects . . . in which a work is fixed.” 17 U.S.C. § 101. The Supreme Court has indicated that in the electronic context, copies may be distributed electronically. See N.Y. Times Co. v. Tasini, 533 U.S. 483, 498 (2001) (a computer database program distributed copies of newspaper articles stored in its computerized database by selling copies of those articles through its database service). Google’s search engine communicates HTML instructions that tell a user’s browser where to find full-size images on a website publisher’s computer, but Google does not itself distribute copies of the infringing photographs. It is the website publisher’s computer that distributes copies of the images by transmitting the photographic image electronically to the user’s computer. As in Tasini, the user can then obtain copies by downloading the photo or printing it.

Perfect 10 incorrectly relies on Hotaling v. Church of Jesus Christ of Latter-Day Saints and Napster for the proposition that merely making images “available” violates the copyright owner’s distribution right. Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199 (4th Cir. 1997); Napster, 239 F.3d 1004. Hotaling held that the owner of a collection of works who makes them available to the public may be deemed to have distributed copies of the works. Hotaling, 118 F.3d at 203. Similarly, the distribution rights of the plaintiff copyright owners were infringed by Napster users (private
individuals with collections of music files stored on their home computers) when they used the Napster software to make their collections available to all other Napster users. *Napster*, 239 F.3d at 1011-14.

[9] This “deemed distribution” rule does not apply to Google. Unlike the participants in the Napster system or the library in *Hotaling*, Google does not own a collection of Perfect 10’s full-size images and does not communicate these images to the computers of people using Google’s search engine. Though Google indexes these images, it does not have a collection of stored full-size images it makes available to the public. Google therefore cannot be deemed to distribute copies of these images under the reasoning of *Napster* or *Hotaling*. Accordingly, the district court correctly concluded that Perfect 10 does not have a likelihood of success in proving that Google violates Perfect 10’s distribution rights with respect to full-size images.

C. Fair Use Defense

Although Perfect 10 has succeeded in showing it would prevail in its prima facie case that Google’s thumbnail images infringe Perfect 10’s display rights, Perfect 10 must still show a likelihood that it will prevail against Google’s affirmative defense. Google contends that its use of thumbnails is a fair use of the images and therefore does not constitute an infringement of Perfect 10’s copyright. See 17 U.S.C. § 107.

The fair use defense permits the use of copyrighted works without the copyright owner’s consent under certain situations. The defense encourages and allows the development of new ideas that build on earlier ones, thus providing a necessary counterbalance to the copyright law’s goal of protecting creators’ work product. “From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright’s very purpose . . . .” *Campbell*, 510 U.S. at 575. “The fair use doctrine thus
permits [and requires] courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." Id. at 577 (quoting *Stewart v. Abend*, 495 U.S. 207, 236 (1990)) (alteration in original).

Congress codified the common law of fair use in 17 U.S.C. § 107, which provides:

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

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

2. the nature of the copyrighted work;

3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

4. the effect of the use upon the potential market for or value of the copyrighted work.

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

We must be flexible in applying a fair use analysis; it "is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis. . . . Nor may the four statutory factors be treated in isolation, one from another. All are to be explored, and the results weighed together, in light of the purposes of copyright." Campbell, 510 U.S. at 577-78; see also Kelly, 336 F.3d at 817-18. The purpose of copyright law is "[t]o promote the Progress of Science and useful Arts," U.S. Const. art. I, § 8, cl. 8, and to serve "the welfare of the public." Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 n.10 (quoting H.R. Rep. No. 2222, 60th Cong., 2d Sess. 7 (1909)).

In applying the fair use analysis in this case, we are guided by Kelly v. Arriba Soft Corp., which considered substantially the same use of copyrighted photographic images as is at issue here. See 336 F.3d 811. In Kelly, a photographer brought a direct infringement claim against Arriba, the operator of an Internet search engine. The search engine provided thumbnail versions of the photographer’s images in response to search queries. Id. at 815-16. We held that Arriba’s use of thumbnail images was a fair use primarily based on the transformative nature of a search engine and its benefit to the public. Id. at 818-22. We also concluded that Arriba’s use of the thumbnail images did not harm the photographer’s market for his image. Id. at 821-22.

In this case, the district court determined that Google’s use of thumbnails was not a fair use and distinguished Kelly. Perfect 10, 416 F. Supp. 2d at 845-51. We consider these distinctions in the context of the four-factor fair use analysis, remaining mindful that Perfect 10 has the burden of proving that it will successfully challenge any evidence Google presents to support its affirmative defense.
Purpose and character of the use. The first factor, 17
U.S.C. § 107(1), requires a court to consider “the purpose and
character of the use, including whether such use is of a com-
mercial nature or is for nonprofit educational purposes.” The
central purpose of this inquiry is to determine whether and to
what extent the new work is “transformative.” Campbell, 510
U.S. at 579. A work is “transformative” when the new work
does not “merely supersed[e] the objects of the original cre-
ation” but rather “adds something new, with a further purpose
or different character, altering the first with new expression,
meaning, or message.” Id. (internal quotation and altera-
tion omitted). Conversely, if the new work “supersed[e] the use
of the original,” the use is likely not a fair use. Harper & Row
(1985) (internal quotation omitted) (publishing the “heart” of
an unpublished work and thus supplanting the copyright hold-
er’s first publication right was not a fair use); see also Wall
Data Inc. v. L.A. County Sheriff’s Dep’t, 447 F.3d 769, 778-
82 (9th Cir. 2006) (using a copy to save the cost of buying
additional copies of a computer program was not a fair use).8

8We reject at the outset Perfect 10’s argument that providing access to
infringing websites cannot be deemed transformative and is inherently not
fair use. Perfect 10 relies on Video Pipeline, Inc. v. Buena Vista Home
Entm’t, Inc., 342 F.3d 191 (3d Cir. 2003), and Atari Games, 975 F.2d at
843. But these cases, in essence, simply apply the general rule that a party
claiming fair use must act in a manner generally compatible with princi-
ple[s] of good faith and fair dealing. See Harper & Row, 471 U.S. at 562-
63. For this reason, a company whose business is based on providing
scenes from copyrighted movies without authorization could not claim
that it provided the same public benefit as the search engine in Kelly. See
Video Pipeline, 342 F.3d at 198-200. Similarly, a company whose overrid-
ing desire to replicate a competitor’s computer game led it to obtain a
copy of the competitor’s source code from the Copyright Office under
false pretenses could not claim fair use with respect to its purloined copy.
Atari Games, 975 F.2d at 843.

Unlike the alleged infringers in Video Pipeline and Atari Games, who
intentionally misappropriated the copyright owners’ works for the purpose
of commercial exploitation, Google is operating a comprehensive search
engine that only incidentally indexes infringing websites. This incidental
As noted in Campbell, a "transformative work" is one that alters the original work "with new expression, meaning, or message." Campbell, 510 U.S. at 579. "A use is considered transformative only where a defendant changes a plaintiff's copyrighted work or uses the plaintiff's copyrighted work in a different context such that the plaintiff's work is transformed into a new creation." Wall Data, 447 F.3d at 778.

[11] Google's use of thumbnails is highly transformative. In Kelly, we concluded that Arriba's use of thumbnails was transformative because "Arriba's use of the images serve[d] a different function than Kelly's use—improving access to information on the Internet versus artistic expression." Kelly, 336 F.3d at 819. Although an image may have been created originally to serve an entertainment, aesthetic, or informative function, a search engine transforms the image into a pointer directing a user to a source of information. Just as a "parody has an obvious claim to transformative value" because "it can provide social benefit, by shedding light on an earlier work, and, in the process, creating a new one," Campbell, 510 U.S. at 579, a search engine provides social benefit by incorporating an original work into a new work, namely, an electronic reference tool. Indeed, a search engine may be more transformative than a parody because a search engine provides an entirely new use for the original work, while a parody typically has the same entertainment purpose as the original work. See, e.g., id. at 594-96 (holding that 2 Live Crew's parody of "Oh, Pretty Woman" using the words "hairy woman" or "bald headed woman" was a transformative work, and thus constituted a fair use); Mattel, Inc. v. Walking Mountain Prods., 353 F.3d 792, 796-98, 800-06 (concluding that

impact does not amount to an abuse of the good faith and fair dealing underpinnings of the fair use doctrine. Accordingly, we conclude that Google's inclusion of thumbnail images derived from infringing websites in its Internet-wide search engine activities does not preclude Google from raising a fair use defense.
photos parodying Barbie by depicting “mude Barbie dolls juxtaposed with vintage kitchen appliances” was a fair use). In other words, a search engine puts images “in a different context” so that they are “transformed into a new creation.” \textit{Wall Data}, 447 F.3d at 778.

The fact that Google incorporates the entire Perfect 10 image into the search engine results does not diminish the transformative nature of Google’s use. As the district court correctly noted, \textit{Perfect 10}, 416 F. Supp. 2d at 848-49, we determined in \textit{Kelly} that even making an exact copy of a work may be transformative so long as the copy serves a different function than the original work, \textit{Kelly}, 336 F.3d at 818-19. For example, the First Circuit has held that the republication of photos taken for a modeling portfolio in a newspaper was transformative because the photos served to inform, as well as entertain. \textit{See Nez v. Caribbean Int’l News Corp.}, 235 F.3d 18, 22-23 (1st Cir. 2000). In contrast, duplicating a church’s religious book for use by a different church was not transformative. \textit{See Worldwide Church of God v. Phila. Church of God, Inc.}, 227 F.3d 1110, 1117 (9th Cir. 2000). Nor was a broadcaster’s simple retransmission of a radio broadcast over telephone lines transformative, where the original radio shows were given no “new expression, meaning, or message.” \textit{Infinity Broad. Corp. v. Kirkwood}, 150 F.3d 104, 108 (2d Cir. 1998). Here, Google uses Perfect 10’s images in a new context to serve a different purpose.

The district court nevertheless determined that Google’s use of thumbnail images was less transformative than Arriba’s use of thumbnails in \textit{Kelly} because Google’s use of thumbnails superseded Perfect 10’s right to sell its reduced-size images for use on cell phones. \textit{See Perfect 10}, 416 F. Supp. 2d at 849. The district court stated that “mobile users can download and save the thumbnails displayed by Google Image Search onto their phones,” and concluded “to the extent that users may choose to download free images to their
phone rather than purchase [Perfect 10’s] reduced-size images, Google’s use supersedes [Perfect 10’s].” Id.

Additionally, the district court determined that the commercial nature of Google’s use weighed against its transformative nature. Id. Although Kelly held that the commercial use of the photographer’s images by Arriba’s search engine was less exploitative than typical commercial use, and thus weighed only slightly against a finding of fair use, Kelly, 336 F.3d at 818-20, the district court here distinguished Kelly on the ground that some website owners in the AdSense program had infringing Perfect 10 images on their websites, Perfect 10, 416 F. Supp. 2d at 846-47. The district court held that because Google’s thumbnails “lead users to sites that directly benefit Google’s bottom line,” the AdSense program increased the commercial nature of Google’s use of Perfect 10’s images. Id. at 847.

In conducting our case-specific analysis of fair use in light of the purposes of copyright, Campbell, 510 U.S. at 581, we must weigh Google’s superseding and commercial uses of thumbnail images against Google’s significant transformative use, as well as the extent to which Google’s search engine promotes the purposes of copyright and serves the interests of the public. Although the district court acknowledged the “truisms that search engines such as Google Image Search provide great value to the public,” Perfect 10, 416 F. Supp. 2d at 848-49, the district court did not expressly consider whether this value outweighed the significance of Google’s superseding use or the commercial nature of Google’s use. Id. at 849. The Supreme Court, however, has directed us to be mindful of the extent to which a use promotes the purposes of copyright and serves the interests of the public. See Campbell, 510 U.S. at 579; Harper & Row, 471 U.S. at 556-57; Sony, 464 U.S. at 431-32.

We note that the superseding use in this case is not significant at present: the district court did not find that any down-
loads for mobile phone use had taken place. See Perfect 10, 416 F. Supp. 2d at 849. Moreover, while Google’s use of thumbnails to direct users to AdSense partners containing infringing content adds a commercial dimension that did not exist in Kelly, the district court did not determine that this commercial element was significant. See id. at 848-49. The district court stated that Google’s AdSense programs as a whole contributed “$630 million, or 46% of total revenues” to Google’s bottom line, but noted that this figure did not “break down the much smaller amount attributable to websites that contain infringing content.” Id. at 847 & n.12 (internal quotation omitted).

[12] We conclude that the significantly transformative nature of Google’s search engine, particularly in light of its public benefit, outweighs Google’s superseding and commercial uses of the thumbnails in this case. In reaching this conclusion, we note the importance of analyzing fair use flexibly in light of new circumstances. Sony, 464 U.S. at 431-32; id. at 448 n.31 (“[Section 107] endorses the purpose and general scope of the judicial doctrine of fair use, but there is no disposition to freeze the doctrine in the statute, especially during a period of rapid technological change.”) (quoting H.R. Rep. No. 94-1476, at 65-66 (1976), U.S. Code Cong. & Admin. News 1976, p. 5680)). We are also mindful of the Supreme Court’s direction that “the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use.” Campbell, 510 U.S. at 579.

Accordingly, we disagree with the district court’s conclusion that because Google’s use of the thumbnails could supersede Perfect 10’s cell phone download use and because the use was more commercial than Arriba’s, this fair use factor weighed “slightly” in favor of Perfect 10. Perfect 10, 416 F. Supp. 2d at 849. Instead, we conclude that the transformative nature of Google’s use is more significant than any incidental superseding use or the minor commercial aspects of Google’s
search engine and website. Therefore, the district court erred in determining this factor weighed in favor of Perfect 10.

The nature of the copyrighted work. With respect to the second factor, “the nature of the copyrighted work,” 17 U.S.C. § 107(2), our decision in Kelly is directly on point. There we held that the photographer’s images were “creative in nature” and thus “closer to the core of intended copyright protection than are more fact-based works.” Kelly, 336 F.3d at 820 (internal quotation omitted). However, because the photos appeared on the Internet before Arriba used thumbnail versions in its search engine results, this factor weighed only slightly in favor of the photographer. Id.

[13] Here, the district court found that Perfect 10’s images were creative but also previously published. Perfect 10, 416 F. Supp. 2d at 850. The right of first publication is “the author’s right to control the first public appearance of his expression.” Harper & Row, 471 U.S. at 564. Because this right encompasses “the choices of when, where, and in what form first to publish a work,” id., an author exercises and exhausts this one-time right by publishing the work in any medium. See, e.g., Batjac Prods. Inc. v. GoodTimes Home Video Corp., 160 F.3d 1223, 1235 (9th Cir. 1998) (noting, in the context of the common law right of first publication, that such a right “does not entail multiple first publication rights in every available medium”). Once Perfect 10 has exploited this commercially valuable right of first publication by putting its images on the Internet for paid subscribers, Perfect 10 is no longer entitled to the enhanced protection available for an unpublished work. Accordingly the district court did not err in holding that this factor weighed only slightly in favor of Perfect 10.8 See Perfect 10, 416 F. Supp. 2d at 849-50.

8Google contends that Perfect 10’s photographic images are less creative and less deserving of protection than the images of the American West in Kelly because Perfect 10 boasts of its un-retouched photos showing the natural beauty of its models. Having reviewed the record, we con-
[14] The amount and substantiality of the portion used. The third factor asks whether the amount and substantiality of the portion used in relation to the copyrighted work as a whole . . . are reasonable in relation to the purpose of the copying.” Campbell, 510 U.S. at 586 (internal quotation omitted); see also 17 U.S.C. § 107(3). In Kelly, we held Arriba’s use of the entire photographic image was reasonable in light of the purpose of a search engine. Kelly, 336 F.3d at 821. Specifically, we noted, “[i]t was necessary for Arriba to copy the entire image to allow users to recognize the image and decide whether to pursue more information about the image or the originating [website]. If Arriba only copied part of the image, it would be more difficult to identify it, thereby reducing the usefulness of the visual search engine.” Id. Accordingly, we concluded that this factor did not weigh in favor of either party. Id. Because the same analysis applies to Google’s use of Perfect 10’s image, the district court did not err in finding that this factor favored neither party.

Effect of use on the market. The fourth factor is “the effect of the use upon the potential market for or value of the copyrighted work.” 17 U.S.C. § 107(4). In Kelly, we concluded that Arriba’s use of the thumbnail images did not harm the market for the photographer’s full-size images. See Kelly, 336 F.3d at 821-22. We reasoned that because thumbnails were not a substitute for the full-sized images, they did not harm the photographer’s ability to sell or license his full-sized images. Id. The district court here followed Kelly’s reasoning, holding that Google’s use of thumbnails did not hurt Perfect 10’s market for full-size images. See Perfect 10, 416 F. Supp. 2d at 850-51.

...clude that the district court’s finding that Perfect 10’s photographs “consistently reflect professional, skillful, and sometimes tasteful artistry” is not clearly erroneous. Perfect 10, 416 F. Supp. 2d at 849 n.15. We agree with the district court that there is no basis for concluding that photos of the American West are more deserving of protection than photos of nude models. See id.
Perfect 10 argues that the district court erred because the likelihood of market harm may be presumed if the intended use of an image is for commercial gain. However, this presumption does not arise when a work is transformative because “market substitution is at least less certain, and market harm may not be so readily inferred.” *Campbell*, 510 U.S. at 591. As previously discussed, Google’s use of thumbnails for search engine purposes is highly transformative. Because market harm cannot be presumed, and because Perfect 10 has not introduced evidence that Google’s thumbnails would harm Perfect 10’s existing or potential market for full-size images, we reject this argument.

[15] Perfect 10 also has a market for reduced-size images, an issue not considered in *Kelly*. The district court held that “Google’s use of thumbnails likely does harm the potential market for the downloading of [Perfect 10’s] reduced-size images onto cell phones.” *Perfect 10*, 416 F. Supp. 2d at 851 (emphasis omitted). The district court reasoned that persons who can obtain Perfect 10 images free of charge from Google are less likely to pay for a download, and the availability of Google’s thumbnail images would harm Perfect 10’s market for cell phone downloads. *Id.* As we discussed above, the district court did not make a finding that Google users have downloaded thumbnail images for cell phone use. This potential harm to Perfect 10’s market remains hypothetical. We conclude that this factor favors neither party.

[16] Having undertaken a case-specific analysis of all four factors, we now weigh these factors together “in light of the purposes of copyright.” *Campbell*, 510 U.S. at 578; see also *Kelly*, 336 F.3d at 818 (“We must balance [the section 107] factors in light of the objectives of copyright law, rather than view them as definitive or determinative tests.”). We note that Perfect 10 has the burden of proving that it would defeat Google’s affirmative fair use defense, *see supra* Section II. In this case, Google has put Perfect 10’s thumbnail images (along with millions of other thumbnail images) to a use fun-
damentally different than the use intended by Perfect 10. In doing so, Google has provided a significant benefit to the public. Weighing this significant transformative use against the unproven use of Google's thumbnails for cell phone downloads, and considering the other fair use factors, all in light of the purpose of copyright, we conclude that Google's use of Perfect 10's thumbnails is a fair use. Because the district court here "found facts sufficient to evaluate each of the statutory factors . . . [we] need not remand for further fact-finding." Harper & Row, 471 U.S. at 560 (internal quotation omitted). We conclude that Perfect 10 is unlikely to be able to overcome Google's fair use defense and, accordingly, we vacate the preliminary injunction regarding Google's use of thumbnail images.

IV

Secondary Liability for Copyright Infringement

[17] We now turn to the district court's ruling that Google is unlikely to be secondarily liable for its in-line linking to infringing full-size images under the doctrines of contributory and vicarious infringement.10 The district court ruled that Perfect 10 did not have a likelihood of proving success on the merits of either its contributory infringement or vicarious infringement claims with respect to the full-size images. See Perfect 10, 416 F. Supp. 2d at 856, 858. In reviewing the district court's conclusions, we are guided by the Supreme Court's recent interpretation of secondary liability, namely: "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise

10Because the district court concluded that Perfect 10 was likely to prevail on its direct infringement claim with respect to Google's use of thumbnails, but not with respect to its in-line linking to full-size images, the district court considered Google's potential secondary liability only on the second issue.
a right to stop or limit it." Grokster, 545 U.S. at 930 (internal citations omitted).

Direct Infringement by Third Parties. As a threshold matter, before we examine Perfect 10's claims that Google is secondarily liable, Perfect 10 must establish that there has been direct infringement by third parties. See Napster, 239 F.3d at 1013 n.2 ("Secondary liability for copyright infringement does not exist in the absence of direct infringement by a third party.").

Perfect 10 alleges that third parties directly infringed its images in three ways. First, Perfect 10 claims that third-party websites directly infringed its copyright by reproducing, displaying, and distributing unauthorized copies of Perfect 10's images. Google does not dispute this claim on appeal.

[18] Second, Perfect 10 claims that individual users of Google's search engine directly infringed Perfect 10's copyrights by storing full-size infringing images on their computers. We agree with the district court's conclusion that Perfect 10 failed to provide sufficient evidence to support this claim. See Perfect 10, 416 F. Supp. 2d at 852. There is no evidence in the record directly establishing that users of Google's search engine have stored infringing images on their computers, and the district court did not err in declining to infer the existence of such evidence.

[19] Finally, Perfect 10 contends that users who link to infringing websites automatically make "cache" copies of full size images and thereby directly infringe Perfect 10's reproduction right. The district court rejected this argument, holding that any such reproduction was likely a "fair use." Id. at 852 n.17. The district court reasoned that "[I]ocal caching by the browsers of individual users is noncommercial, transformative, and no more than necessary to achieve the objectives of decreasing network latency and minimizing unnecessary bandwidth usage (essential to the [I]nternet). It has a minimal
impact on the potential market for the original work ...” *Id.* We agree; even assuming such automatic copying could constitute direct infringement, it is a fair use in this context. The copying function performed automatically by a user’s computer to assist in accessing the Internet is a transformative use. Moreover, as noted by the district court, a cache copies no more than is necessary to assist the user in Internet use. It is designed to enhance an individual’s computer use, not to supersede the copyright holders’ exploitation of their works. Such automatic background copying has no more than a minimal effect on Perfect 10’s rights, but a considerable public benefit. Because the four fair use factors weigh in favor of concluding that cache copying constitutes a fair use, Perfect 10 has not carried its burden of showing that users’ cache copies of Perfect 10’s full-size images constitute direct infringement.

Therefore, we must assess Perfect 10’s arguments that Google is secondarily liable in light of the direct infringement that is undisputed by the parties: third-party websites’ reproducing, displaying, and distributing unauthorized copies of Perfect 10’s images on the Internet. *Id.* at 852.

**A. Contributory Infringement**

In order for Perfect 10 to show it will likely succeed in its contributory liability claim against Google, it must establish that Google’s activities meet the definition of contributory liability recently enunciated in *Grokster*. Within the general rule that “[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement,” *Grokster*, 545 U.S. at 930, the Court has defined two categories of contributory liability: “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 sig-
significant noninfringing uses.” *Id.* at 942 (Ginsburg, J., concurring) (quoting *Sony*, 464 U.S. at 442); see also *id.* at 936-37.

Looking at the second category of liability identified by the Supreme Court (distributing products), Google relies on *Sony*, 464 U.S. at 442, to argue that it cannot be held liable for contributory infringement because liability does not arise from the mere sale of a product (even with knowledge that consumers would use the product to infringe) if the product is capable of substantial non-infringing use. Google argues that its search engine service is such a product. Assuming the principle enunciated in *Sony* is applicable to the operation of Google’s search engine, then Google cannot be held liable for contributory infringement *solely* because the design of its search engine facilitates such infringement. *Grokster*, 545 U.S. at 931-32 (discussing *Sony*, 464 U.S. 417). Nor can Google be held liable solely because it did not develop technology that would enable its search engine to automatically avoid infringing images. *See id.* at 939 n.12. However, Perfect 10 has not based its claim of infringement on the design of Google’s search engine and the *Sony* rule does not immunize Google from other sources of contributory liability. *See id.* at 933-34.

[20] We must next consider whether Google could be held liable under the first category of contributory liability identified by the Supreme Court, that is, the liability that may be imposed for intentionally encouraging infringement through specific acts. *Grokster* tells us that contribution to infringement must be intentional for liability to arise. *Grokster*, 545 U.S. at 930. However, *Grokster* also directs us to analyze con-

---

*Google's activities do not meet the ‘inducement’ test explained in *Grokster* because Google has not promoted the use of its search engine specifically to infringe copyrights. *See Grokster*, 545 U.S. at 935-37. However, the Supreme Court in *Grokster* did not suggest that a court must find inducement in order to impose contributory liability under common law principles.*
tributory liability in light of "rules of fault-based liability derived from the common law," id. at 934-35, and common law principles establish that intent may be imputed. "Tort law ordinarily imputes to an actor the intention to cause the natural and probable consequences of his conduct." DeVoto v. Pac. Fid. Life Ins. Co., 618 F.2d 1340, 1347 (9th Cir. 1980); Restatement (Second) of Torts § 8A cmt. b (1965) ("If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result."). When the Supreme Court imported patent law's "staple article of commerce doctrine" into the copyright context, it also adopted these principles of imputed intent. Grokster, 545 U.S. at 932 ("The [staple article of commerce] 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."). Therefore, under Grokster, an actor may be contributorily liable for intentionally encouraging direct infringement if the actor knowingly takes steps that are substantially certain to result in such direct infringement.

Our tests for contributory liability are consistent with the rule set forth in Grokster. We have adopted the general rule set forth in Gershwin Publishing Corp. v. Columbia Artists Management, Inc., namely: "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer," 443 F.2d 1159, 1162 (2d Cir. 1971). See Ellison, 357 F.3d at 1076; Napster, 239 F.3d at 1019; Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

[21] We have further refined this test in the context of cyberspace to determine when contributory liability can be

imposed on a provider of Internet access or services. See Napster, 239 F.3d at 1019-20. In Napster, we considered claims that the operator of an electronic file sharing system was contributorily liable for assisting individual users to swap copyrighted music files stored on their home computers with other users of the system. Napster, 239 F.3d at 1011-13, 1019-22.

We stated that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement." Id. at 1021. Because Napster knew of the availability of infringing music files, assisted users in accessing such files, and failed to block access to such files, we concluded that Napster materially contributed to infringement. Id. at 1022.

The Napster test for contributory liability was modeled on the influential district court decision in Religious Technology Center v. Netcom On-Line Communication Services, Inc. (Netcom), 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995). See Napster, 239 F.3d at 1021. In Netcom, a disgruntled former Scientology minister posted allegedly infringing copies of Scientological works on an electronic bulletin board service. Netcom, 907 F. Supp. at 1365-66. The messages were stored on the bulletin board operator's computer, then automatically copied onto Netcom's computer, and from there copied onto other computers comprising "a worldwide community" of electronic bulletin board systems. Id. at 1366-67 & n.4 (internal quotation omitted). Netcom held that if plaintiffs could prove that Netcom knew or should have known that the minister infringed plaintiffs' copyrights, "Netcom [would] be liable for contributory infringement since its failure to simply cancel [the former minister's] infringing message and thereby stop an infringing copy from being distributed worldwide constitute[d] substantial participation in [the former minister's] public distribution of the message." Id. at 1374.

[22] Although neither Napster nor Netcom expressly required a finding of intent, those cases are consistent with
Grokker because both decisions ruled that a service provider's knowing failure to prevent infringing actions could be the basis for imposing contributory liability. Under such circumstances, intent may be imputed. In addition, Napster and Netcom are consistent with the longstanding requirement that an actor’s contribution to infringement must be material to warrant the imposition of contributory liability. Gershwin, 443 F.2d at 1162. Both Napster and Netcom acknowledge that services or products that facilitate access to websites throughout the world can significantly magnify the effects of otherwise immaterial infringing activities. See Napster, 239 F.3d at 1022; Netcom, 907 F. Supp. at 1375. The Supreme Court has acknowledged that “[t]he argument for imposing indirect liability” is particularly “powerful” when individuals using the defendant’s software could make a huge number of infringing downloads every day. Grokker, 545 U.S. at 929. Moreover, copyright holders cannot protect their rights in a meaningful way unless they can hold providers of such services or products accountable for their actions pursuant to a test such as that enunciated in Napster. See id. at 929-30 ("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."). Accordingly, we hold that a computer system operator can be held contributorily liable if it “has actual knowledge that specific infringing material is available using its system,” Napster, 239 F.3d at 1022, and can “take simple measures to prevent further damage” to copyrighted works, Netcom, 907 F. Supp. at 1375, yet continues to provide access to infringing works.

Here, the district court held that even assuming Google had actual knowledge of infringing material available on its system, Google did not materially contribute to infringing conduct because it did not undertake any substantial promotional or advertising efforts to encourage visits to infringing web-
sites, nor provide a significant revenue stream to the infringing websites. *Perfect 10*, 416 F. Supp. 2d at 854-56. This analysis is erroneous. There is no dispute that Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials. We cannot discount the effect of such a service on copyright owners, even though Google’s assistance is available to all websites, not just infringing ones. Applying our test, Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10’s copyrighted works, and failed to take such steps.

[23] The district court did not resolve the factual disputes over the adequacy of Perfect 10’s notices to Google and Google’s responses to these notices. Moreover, there are factual disputes over whether there are reasonable and feasible means for Google to refrain from providing access to infringing images. Therefore, we must remand this claim to the district court for further consideration whether Perfect 10 would likely succeed in establishing that Google was contributorily liable for in-line linking to full-size infringing images under the test enunciated today. 13

13Perfect 10 claims that Google materially contributed to infringement by linking to websites containing unauthorized passwords, which enabled Google users to access Perfect 10’s website and make infringing copies of images. However, Perfect 10 points to no evidence that users logging onto the Perfect 10 site with unauthorized passwords infringed Perfect 10’s exclusive rights under section 106. In the absence of evidence that Google’s actions led to any direct infringement, this argument does not assist Perfect 10 in establishing that it would prevail on the merits of its contributory liability claim. See *Napster*, 239 F.3d at 1013 n.2 ("Secondary liability for copyright infringement does not exist in the absence of direct infringement by a third party.").
B. Vicarious Infringement

[24] Perfect 10 also challenges the district court's conclusion that it is not likely to prevail on a theory of vicarious liability against Google. *Perfect 10*, 416 F. Supp. 2d at 856-58. *Grokster* states that one "infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." *Grokster*, 545 U.S. at 930. As this formulation indicates, to succeed in imposing vicarious liability, a plaintiff must establish that the defendant exercises the requisite control over the direct infringer and that the defendant derives a direct financial benefit from the direct infringement. See id. *Grokster* further explains the "control" element of the vicarious liability test as the defendant's "right and ability to supervise the direct infringer." Id. at 930 n.9. Thus, under *Grokster*, a defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so.

We evaluate Perfect 10's arguments that Google is vicariously liable in light of the direct infringement that is undisputed by the parties, namely, the third-party websites' reproduction, display, and distribution of unauthorized copies of Perfect 10's images on the Internet. *Perfect 10*, 416 F. Supp. 2d at 852; see *supra* Section IV.A. In order to prevail at this preliminary injunction stage, Perfect 10 must demonstrate a likelihood of success in establishing that Google has the right and ability to stop or limit the infringing activities of third-party websites. In addition, Perfect 10 must establish a likelihood of proving that Google derives a direct financial benefit from such activities. Perfect 10 has not met this burden.

With respect to the "control" element set forth in *Grokster*, Perfect 10 has not demonstrated a likelihood of showing that Google has the legal right to stop or limit the direct infringement of third-party websites. See *Grokster*, 545 U.S. at 930. Unlike *Fonovisa*, where by virtue of a "broad contract" with
its vendors the defendant swap meet operators had the right to stop the vendors from selling counterfeit recordings on its premises, *Fonovisa*, 76 F.3d at 263, Perfect 10 has not shown that Google has contracts with third-party websites that empower Google to stop or limit them from reproducing, displaying, and distributing infringing copies of Perfect 10's images on the Internet. Perfect 10 does point to Google's AdSense agreement, which states that Google reserves "the right to monitor and terminate partnerships with entities that violate others' copyright[s]." *Perfect 10*, 416 F. Supp. 2d at 858. However, Google's right to terminate an AdSense partnership does not give Google the right to stop direct infringement by third-party websites. An infringing third-party website can continue to reproduce, display, and distribute its infringing copies of Perfect 10 images after its participation in the AdSense program has ended.

[25] Nor is Google similarly situated to Napster. Napster users infringed the plaintiffs' reproduction and distribution rights through their use of Napster's proprietary music-file sharing system. *Napster*, 239 F.3d at 1011-14. There, the infringing conduct was the use of Napster's "service to download and upload copyrighted music." *Id.* at 1014 (internal quotation omitted). Because Napster had a closed system requiring user registration, and could terminate its users' accounts and block their access to the Napster system, Napster had the right and ability to prevent its users from engaging in the infringing activity of uploading file names and downloading Napster users' music files through the Napster system.14 *Id.* at 1023-24. By contrast, Google cannot stop any

---

14Napster's system included "Napster's MusicShare software, available free of charge from Napster's Internet site, and Napster's network servers and server-side software." *Napster*, 239 F.3d at 1011. By downloading Napster's MusicShare software to the user's personal computer, and registering with the Napster system, a user could both upload and download music files. *Id.* at 1011-13. If the Napster user uploaded a list of music files stored on the user's personal computer to the Napster system, such
of the third-party websites from reproducing, displaying, and distributing unauthorized copies of Perfect 10's images because that infringing conduct takes place on the third-party websites. Google cannot terminate those third-party websites or block their ability to "host and serve infringing full-size images" on the Internet. *Perfect 10*, 416 F. Supp. 2d at 831.

Moreover, the district court found that Google lacks the practical ability to police the third-party websites' infringing conduct. *Id.* at 857-58. Specifically, the court found that Google's supervisory power is limited because "Google's software lacks the ability to analyze every image on the Internet, compare each image to all the other copyrighted images that exist in the world . . . and determine whether a certain image on the web infringes someone's copyright." *Id.* at 858. The district court also concluded that Perfect 10's suggestions regarding measures Google could implement to prevent its web crawler from indexing infringing websites and to block access to infringing images were not workable. *Id.* at 858 n.25. Rather, the suggestions suffered from both "imprecision and overbreadth." *Id.* We hold that these findings are not clearly erroneous. Without image-recognition technology, Google lacks the practical ability to police the infringing activities of third-party websites. This distinguishes Google from the defendants held liable in *Napster* and *Fonovisa*. See *Napster*, 239 F.3d at 1023-24 (Napster had the ability to identify and police infringing conduct by searching its index for song titles); *Fonovisa*, 76 F.3d at 262 (swap meet operator

music files would be automatically available to other Napster users whenever the user was logged on to the Napster system. *Id.* at 1012. In addition, the Napster user could download music files directly from other users' personal computers. *Id.* We explained the infringing conduct as "Napster users who upload file names to the [Napster] search index for others to copy violate plaintiffs' distribution rights. Napster users who download files [through the Napster system] containing copyrighted music violate plaintiffs' reproduction rights." *Id.* at 1014.
had the ability to identify and police infringing activity by patrolling its premises).

Perfect 10 argues that Google could manage its own operations to avoid indexing websites with infringing content and linking to third-party infringing sites. This is a claim of contributory liability, not vicarious liability. Although "the lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn," Sony, 464 U.S. at 435 n.17 (internal quotation omitted), in general, contributory liability is based on the defendant's failure to stop its own actions which facilitate third-party infringement, while vicarious liability is based on the defendant's failure to cause a third party to stop its directly infringing activities. See, e.g., Ellison, 357 F.3d at 1077-78; Fonovisa, 76 F.3d at 261-64. Google's failure to change its operations to avoid assisting websites to distribute their infringing content may constitute contributory liability, see supra Section IV.A. However, this failure is not the same as declining to exercise a right and ability to make third-party websites stop their direct infringement. We reject Perfect 10's efforts to blur this distinction.

[26] Because we conclude that Perfect 10 has not shown a likelihood of establishing Google's right and ability to stop or limit the directly infringing conduct of third-party websites, we agree with the district court's conclusion that Perfect 10 "has not established a likelihood of proving the [control] prong necessary for vicarious liability." Perfect 10, 416 F. Supp. 2d at 858.16

C. Digital Millennium Copyright Act

Google claims that it qualifies for the limitations on liability set forth in title II of the DMCA, 17 U.S.C. § 512. In particular, section 512(d) limits the liability of a service provider

16Having so concluded, we need not reach Perfect 10's argument that Google received a direct financial benefit.
"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 meets certain criteria. We have held that the limitations on liability contained in 17 U.S.C. § 512 protect secondary infringers as well as direct infringers. *Napster*, 239 F.3d at 1025.

[27] The parties dispute whether Google meets the specified criteria. Perfect 10 claims that it sent qualifying notices to Google and Google did not act expeditiously to remove the infringing material. Google claims that Perfect 10’s notices did not comply with the notice provisions of section 512 and were not adequate to inform Google of the location of the infringing images on the Internet or identify the underlying copyrighted work. Google also claims that it responded to all notices it received by investigating the webpages identified by Perfect 10 and suppressing links to any webpages that Google confirmed were infringing.

Because the district court determined that Perfect 10 was unlikely to succeed on its contributory and vicarious liability claims, it did not reach Google’s arguments under section 512. In revisiting the question of Perfect 10’s likelihood of success on its contributory infringement claims, the district court should also consider whether Perfect 10 would likely succeed in showing that Google was not entitled to the limitations on injunctive relief provided by title II of the DMCA.

V

Amazon.com

Perfect 10 claims that Amazon.com displays and distributes Perfect 10’s copyrighted images and is also secondarily liable for the infringements of third-party websites and Amazon.com users. The district court concluded that Perfect 10
was unlikely to succeed in proving that Amazon.com was a direct infringer, because it merely in-line linked to the thumbnails on Google’s servers and to the full-size images on third-party websites.\footnote{Perfect 10 v. Amazon, No. 05-4753, consolidated with 04-9484 (C.D. Cal. February 21, 2006) (order denying preliminary injunction). In addition, the district court concluded that Perfect 10’s secondary infringement claims against Amazon.com were likely to fail because Amazon.com had no program analogous to AdSense, and thus did not provide any revenues to infringing sites. Id. Finally, the district court determined that Amazon.com’s right and ability to control the infringing conduct of third-party websites was substantially less than Google’s. Id. Therefore, the district court denied Perfect 10’s motion for a preliminary injunction against Amazon.com. Id.}

We agree that Perfect 10 has not shown a likelihood that it would prevail on the merits of its claim that Amazon.com directly infringed its images. Amazon.com communicates to its users only the HTML instructions that direct the users’ browsers to Google’s computers (for thumbnail images) or to a third party’s computer (for full-size infringing images). Therefore, Amazon.com does not display or distribute a copy of the thumbnails or full-size images to its users.

[28] We also agree with the district court’s conclusion that Amazon.com does not have “the right and ability to supervise the infringing activity” of Google or third parties. The district court did not clearly err in concluding that Amazon.com lacked a direct financial interest in such activities. Therefore, Perfect 10’s claim that Amazon.com is vicariously liable for third-party infringement is unlikely to succeed.

\footnote{Amazon.com states that it ended its relationship with Google on April 30, 2006. Perfect 10’s action for preliminary injunction against Amazon.com is not moot, however, because Amazon.com has not established “that the allegedly wrongful behavior cannot reasonably be expected to recur.” F.T.C. v. Affordable Media, LLC, 179 F.3d 1228, 1238 (9th Cir. 1999) (internal quotation omitted).}
However, the district court did not consider whether Amazon.com had "actual knowledge that specific infringing material is available using its system," *Napster*, 239 F.3d at 1022 (emphasis in original), and could have "take[n] simple measures to prevent further damage" to copyrighted works, *Netcom*, 907 F. Supp. at 1375, yet continued to provide access to infringing works. Perfect 10 has presented evidence that it notified Amazon.com that it was facilitating its users' access to infringing material. It is disputed whether the notices gave Amazon.com actual knowledge of specific infringing activities available using its system, and whether Amazon.com could have taken reasonable and feasible steps to refrain from providing access to such images, but failed to do so. Nor did the district court consider whether Amazon.com is entitled to limit its liability under title II of the DMCA. On remand, the district court should consider Amazon.com's potential contributory liability, as well as possible limitations on the scope of injunctive relief, in light of our rulings today.

VI

We conclude that Perfect 10 is unlikely to succeed in overcoming Google's fair use defense, and therefore we reverse the district court's determination that Google's thumbnail versions of Perfect 10's images likely constituted a direct infringement. The district court also erred in its secondary liability analysis because it failed to consider whether Google and Amazon.com knew of infringing activities yet failed to take reasonable and feasible steps to refrain from providing access to infringing images. Therefore we must also reverse the district court's holding that Perfect 10 was unlikely to succeed on the merits of its secondary liability claims. Due to this error, the district court did not consider whether Google and Amazon.com are entitled to the limitations on liability set forth in title II of the DMCA. The question whether Google and Amazon.com are secondarily liable, and whether they can limit that liability pursuant to title II of the DMCA, raise fact-intensive inquiries, potentially requiring further fact finding,
and thus can best be resolved by the district court on remand. We therefore remand this matter to the district court for further proceedings consistent with this decision.

Because the district court will need to reconsider the appropriate scope of injunctive relief after addressing these secondary liability issues, we do not address the parties’ arguments regarding the scope of the injunction issued by the district court. For the same reason, we do not address the parties’ dispute over whether the district court abused its discretion in determining that Perfect 10 satisfied the irreparable harm element of a preliminary injunction.

Therefore, we reverse the district court’s ruling and vacate the preliminary injunction regarding Google’s use of thumbnail versions of Perfect 10’s images. We reverse the district court’s rejection of the claims that Google and Amazon.com are secondarily liable for infringement of Perfect 10’s full-size images. We otherwise affirm the rulings of the district court. We remand this matter for further proceedings consistent with this opinion. Each party shall bear its own costs on appeal. See Fed. R. App. P. 39(a)(4).

AFFIRMED IN PART; REVERSED IN PART; REMANDED.

17Because we vacate the injunction, Google’s motion for stay of the injunction is moot.
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Perfect 10, Inc.,
Plaintiff-Appellant,

v.

Visa International Service
Association; First Data
Corporation; Cardservice
International, Inc.; Humboldt
Bank; Mastercard International,
Inc.,

Defendants-Appellees.

No. 05-15170
D.C. No.
CV-04-00371-JW
OPINION

Appeal from the United States District Court
for the Northern District of California
James Ware, District Judge, Presiding

Argued and Submitted
December 4, 2006—Pasadena, California

Filed July 3, 2007

Before: Stephen Reinhardt, Alex Kozinski, and
Milan D. Smith, Jr., Circuit Judges.

Opinion by Judge Milan D. Smith, Jr.;
Dissent by Judge Kozinski
COUNSEL

Howard E. King (argued) and Stephen D. Rothschild, King, Holmes, Paterno & Berliner, LLP, Los Angeles, California, for the plaintiff-appellant.

Jeffrey N. Mausner, Berman, Mausner & Resser, Los Angeles, California, for the plaintiff-appellant.

Daniel J. Cooper, Los Angeles, California, for the plaintiff-appellant.

Andrew P. Bridges (argued), John C. Nishi, Winston & Strawn LLP, San Francisco, California, for defendant-appellee Mastercard International Incorporated.


OPINION

MILAN D. SMITH, JR., Circuit Judge:

Perfect 10, Inc. (Perfect 10) sued Visa International Service Association, MasterCard International Inc., and several affli-
ated banks and data processing services (collectively, the Defendants), alleging secondary liability under federal copyright and trademark law and liability under California statutory and common law. It sued because Defendants continue to process credit card payments to websites that infringe Perfect 10’s intellectual property rights after being notified by Perfect 10 of infringement by those websites. The district court dismissed all causes of action under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted. We affirm the decision of the district court.

FACTS AND PRIOR PROCEEDINGS

Perfect 10 publishes the magazine “PERFECT10” and operates the subscription website www.perfect10.com, both of which “feature tasteful copyrighted images of the world’s most beautiful natural models.” Appellant’s Opening Brief at 1. Perfect 10 claims copyrights in the photographs published in its magazine and on its website, federal registration of the “PERFECT 10” trademark and blanket publicity rights for many of the models appearing in the photographs. Perfect 10 alleges that numerous websites based in several countries have stolen its proprietary images, altered them, and illegally offered them for sale online.

Instead of suing the direct infringers in this case, Perfect 10 sued Defendants, financial institutions that process certain credit card payments to the allegedly infringing websites. The Visa and MasterCard entities are associations of member banks that issue credit cards to consumers, automatically process payments to merchants authorized to accept their cards, and provide information to the interested parties necessary to settle the resulting debits and credits. Defendants collect fees for their services in these transactions. Perfect 10 alleges that it sent Defendants repeated notices specifically identifying infringing websites and informing Defendants that some of their consumers use their payment cards to purchase infring-
ing images. Defendants admit receiving some of these notices, but they took no action in response to the notices after receiving them.

Perfect 10 separately alleges that it formerly had a merchant account with defendant First Data Corporation (FDC) but that in the Spring of 2001 FDC terminated the account. FDC’s stated reason for the termination is that the percentage of Perfect 10’s customers who later disputed the charges attributed to them (the chargeback rate) exceeded contractual limits. Perfect 10 claims these chargeback rates were temporarily and substantially inflated because Perfect 10 was the “victim of hackers who were subsequently investigated by the Secret Service.” Appellant’s Opening Brief at 13. Perfect 10 claims that FDC was aware of this and was also aware that Perfect 10’s chargeback rate dropped to within association limits once the hacking ceased, but that FDC nevertheless placed Perfect 10 on an industry-wide “black list” of terminated accounts.

Perfect 10 filed suit against Defendants on January 28, 2004 alleging contributory and vicarious copyright and trademark infringement as well as violations of California laws proscribing unfair competition and false advertising, violation of the statutory and common law right of publicity, libel, and intentional interference with prospective economic advantage. Defendants moved to dismiss the initial complaint under FRCP 12(b)(6). The district court granted the motion, dismissing the libel and intentional interference claims with prejudice but granting leave to amend the remaining claims. In its first amended complaint, Perfect 10 essentially repeated the allegations in its original complaint concerning the surviving causes of action and Defendants again moved to dismiss under FRCP 12(b)(6). The district court granted the Defendants’ second motion in full, dismissing all remaining causes of action with prejudice. Perfect 10 appealed to this court.

JURISDICTION

The district court had original jurisdiction over the copyright and trademark claims pursuant to 28 U.S.C. §§ 1331 and
DISCUSSION

SECONDARY LIABILITY UNDER FEDERAL COPYRIGHT AND TRADEMARK LAW

A. Secondary Liability for Copyright Infringement

Perfect 10 alleges that numerous websites based in several countries—and their paying customers—have directly infringed its rights under the Copyright Act, 17 U.S.C. § 101, et. seq.\(^1\) In the present suit, however, Perfect 10 has sued Defendants, not the direct infringers, claiming contributory and vicarious copyright infringement because Defendants process credit card charges incurred by customers to acquire the infringing images.

We evaluate Perfect 10’s claims with an awareness that credit cards serve as the primary engine of electronic commerce and that Congress has determined it to be the “policy of the United States—(1) to promote the continued development of the Internet and other interactive computer services and other interactive media [and] (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.” 47 U.S.C. §§ 230 (b)(1), (2).\(^2\)

\(^1\)While Perfect 10’s complaint does not clearly specify which of Perfect 10’s rights are being infringed, it appears that at least four such rights are potentially at issue: reproduction (17 U.S.C. § 106(1)); derivative works (17 U.S.C. § 106(2)); distribution of copies (17 U.S.C. § 106(3)); and public display (17 U.S.C. § 106(5)).

\(^2\)Congress expressed similar sentiments when it enacted the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512, one of the stated purposes of which was to “facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.” S. Rep. 105-190, at 1-2 (1998).
1. Contributory Copyright Infringement

Contributory copyright infringement is a form of secondary liability with roots in the tort-law concepts of enterprise liability and imputed intent. See Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996); Perfect 10, Inc. v. Amazon.com, Inc. et al., 481 F.3d 1005, 1007 (9th Cir. 2007) (citing Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)). This court and the United States Supreme Court (Supreme Court) have announced various formulations of the same basic test for such liability. We have found that a defendant is a contributory infringer if it (1) has knowledge of a third party’s infringing activity, and (2) “induces, causes, or materially contributes to the infringing conduct.” Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004) (citing Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)). In an Internet context, we have found contributory liability when the defendant “engages in personal conduct that encourages or assists the infringement.” A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001) (internal citations omitted). In Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., the Supreme Court adopted from patent law the concept of “inducement” and found that “[o]ne infringes contributory by intentionally inducing or encouraging direct infringement.” 545 U.S. 913, 930 (2005). Most recently, in a case also brought by Perfect 10, we found that “an actor may be contributiorily liable [under Grokster] for intentionally encouraging direct infringement if the actor knowingly takes steps that are substantially certain to result in such direct infringement.” Amazon.com, 2007 WL 1428632, at *17.

In her concurring opinion in Grokster, Justice Ginsburg identified another strand of contributory liability in the Supreme Court’s jurisprudence, i.e., liability based on “distributing a product distributorse use to infringe copyrights, if the product is not capable of ‘substantial’ or ‘commercially significant’ noninfringing uses.” Grokster, 545 U.S. at 942 (citing Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984)). Even assuming Defendants offer a “product” for these purposes, Perfect 10 does not claim that the “product” of credit card services is incapable of substantial and commercially significant noninfringing uses.
[1] We understand these several criteria to be non-contradictory variations on the same basic test, i.e., that one contributorily infringes when he (1) has knowledge of another's infringement and (2) either (a) materially contributes to or (b) induces that infringement. Viewed in isolation, the language of the tests described is quite broad, but when one reviews the details of the actual “cases and controversies” before the relevant court in each of the test-defining cases and the actual holdings in those cases, it is clear that the factual circumstances in this case are not analogous. To find that Defendants’ activities fall within the scope of such tests would require a radical and inappropriate expansion of existing principles of secondary liability and would violate the public policy of the United States.

a. Knowledge of the Infringing Activity

[2] Because we find that Perfect 10 has not pled facts sufficient to establish that Defendants induce or materially contribute to the infringing activity, Perfect 10’s contributory copyright infringement claim fails and we need not address the Defendants’ knowledge of the infringing activity.4

4We note that an anomaly exists regarding the concept of notice in secondary copyright infringement cases outside a FRCP 12(b)(6) context. Congress addressed the issue of notice in the DMCA, which grants a safe harbor against liability to certain Internet service providers, even those with actual knowledge of infringement, if they have not received statutorily-compliant notice. See Perfect 10 v. CCBill LLC, 481 F.3d 751 (9th Cir. 2007). amended and superceded, ___ F.3d ___, 2007 WL 1557475 (9th Cir. May 31, 2007); 17 U.S.C. § 512(c)(3). Because Defendants are not “service providers” within the scope of the DMCA, they are not eligible for these safe harbors. The result, under Perfect 10’s theories, would therefore be that a service provider with actual knowledge of infringement and the actual ability to remove the infringing material, but which has not received a statutorily compliant notice, is entitled to a safe harbor from liability, while credit card companies with actual knowledge but without the actual ability to remove infringing material, would benefit from no safe harbor. We recognize that the DMCA was not intended to displace the development of secondary liability in the courts; rather, we simply take note of the anomalous result Perfect 10 seeks.
b. Material Contribution, Inducement, or Causation

[3] To state a claim of contributory infringement, Perfect 10 must allege facts showing that Defendants induce, cause, or materially contribute to the infringing conduct. See, e.g., Ellison, 357 F.3d at 1076. Three key cases found defendants contributorily liable under this standard: Fonovisa, 76 F.3d 259; Napster, 239 F.3d 1004; and Grokster, 545 U.S. 913. In Fonovisa, we held a swap meet operator contributorily liable for the sale of pirated works at the swap meet. In Napster, we held the operator of an electronic file sharing system liable when users of that system employed it to exchange massive quantities of copyrighted music. In Grokster, the Supreme Court found liability for the substantially similar act of distributing software that enabled exchange of copyrighted music on a peer-to-peer, rather than a centralized basis. Perfect 10 argues that by continuing to process credit card payments to the infringing websites despite having knowledge of ongoing infringement, Defendants induce, enable and contribute to the infringing activity in the same way the defendants did in Fonovisa, Napster and Grokster. We disagree.

1. Material Contribution

[4] The credit card companies cannot be said to materially contribute to the infringement in this case because they have no direct connection to that infringement. Here, the infringement rests on the reproduction, alteration, display and distribution of Perfect 10’s images over the Internet. Perfect 10 has not alleged that any infringing material passes over Defendants’ payment networks or through their payment processing systems, or that Defendants’ systems are used to alter or display the infringing images. In Fonovisa, the infringing material was physically located in and traded at the defendant’s

---

5Because the Grokster court focused primarily on an “inducement” theory rather than a “material contribution” theory, our primary discussion of Grokster is located below in the “inducement” section of this opinion.
market. Here, it is not. Nor are Defendants' systems used to locate the infringing images. The search engines in *Amazon.com* provided links to specific infringing images, and the services in *Napster* and *Grokster* allowed users to locate and obtain infringing material. Here, in contrast, the services provided by the credit card companies do not help locate and are not used to distribute the infringing images. While *Perfect 10* has alleged that Defendants make it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display and distribution, which can occur without payment. Even if infringing images were not paid for, there would still be infringement. *See Napster*, 239 F.3d at 1014 (Napster users infringed the distribution right by uploading file names to the search index for others to copy, despite the fact that no money changed hands in the transaction).

Our analysis is fully consistent with this court's recent decision in *Perfect 10 v. Amazon.com*, where we found that "Google could be held contributorily liable if it had knowledge that infringing *Perfect 10* images were available using its search engine, could take simple measures to prevent further damage to *Perfect 10*’s copyrighted works, and failed to take such steps." 2007 WL 1428632, at *19. The dissent claims this statement applies squarely to Defendants if we just substitute "payment systems" for "search engine." Dissent at 7866. But this is only true if search engines and payment systems are equivalents for these purposes, and they are not. The salient distinction is that Google’s search engine itself assists in the distribution of infringing content to Internet users, while Defendants’ payment systems do not. The *Amazon.com* court noted that "Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials." *Id.* Defendants do not provide such a service. They in no way assist or enable Internet users to locate infringing material, and they do not distribute it. They do, as alleged, make infringement more profitable, and people are generally more inclined to engage in an activity when it is financially
profitable. However, there is an additional step in the causal chain: Google may materially contribute to infringement by making it fast and easy for third parties to locate and distribute infringing material, whereas Defendants make it easier for infringement to be profitable, which tends to increase financial incentives to infringe, which in turn tends to increase infringement.

[5] The dissent disagrees with our reading of Amazon.com and charges us with wishful thinking, dissent at 7866, and with "draw[ing] a series of ephemeral distinctions," dissent at 7890. We respectfully disagree and assert that our construction of the relevant statutes and case law is completely consistent with existing federal law, is firmly grounded in both commercial and technical reality and conforms to the public policy of the United States. Helping users to locate an image might substantially assist users to download infringing images, but processing payments does not. If users couldn't pay for images with credit cards, infringement could continue on a large scale because other viable funding mechanisms are available. For example, a website might decide to allow users to download some images for free and to make its profits from advertising, or it might develop other payment mechanisms that do not depend on the credit card companies. In either case, the unlicensed use of Perfect 10's copyrighted images would still be infringement. We acknowledge that

---

[6] As discussed in note 11, infra, the dissent's claims that payment processing is "an essential step in the infringement process," dissent at 7867, and that "Defendants are directly involved in every infringing transaction where payment is made by credit card," dissent at 7873, suggests that the dissent believes that the Defendants are directly infringing when they process these payments.

[7] As discussed more fully in the vicarious infringement section, infra, Perfect 10's factual allegations are not to the contrary.

[8] We recognize that Google is not the only search engine available to Internet users, and that users do not necessarily need Google to locate infringing images. The distinction we draw, however, is not specific to
Defendants' payment systems make it easier for such an infringement to be profitable, and that they therefore have the effect of increasing such infringement, but because infringement of Perfect 10's copyrights can occur without using Defendants' payment system, we hold that payment processing by the Defendants as alleged in Perfect 10's First Amended Complaint does not constitute a "material contribution" under the test for contributory infringement of copyrights.∗

Google; it is between location services and payment services. Because location services lead Internet users directly to infringing images and often display them on the website of the service itself, we find that location services are more important and more essential—indeed, more "material"—to infringement than payment services are.

∗Our dissenting colleague assures us that we would not jeopardize Internet commerce by finding Defendants liable because he has "every confidence" that this court will simply find that other providers of essential services may contribute to infringement, but not materially so. Dissent at 7875. We take little comfort in his assurances because the predicate of our colleague's optimistic view of future judicial refinement of his new world of secondary liability is a large number of expensive and drawn-out pieces of litigation that may, or may not, ever be filed. Meanwhile, what would stop a competitor of a web-site from sending bogus notices to a credit card company claiming infringement by its competitor in the hope of putting a competitor out of business, or, at least, requiring it to spend a great deal of money to clear its name? Threatened with significant potential secondary liability on a variety of fronts under the dissent's proposed expansion of existing secondary liability law, perhaps the credit card companies would soon decline to finance purchases that are more legally risky. They, after all, are as moved by Adam Smith's "invisible hand" as the next set of merchants. If that happened, would First Amendment rights of consumers be trampled? Would Perfect 10 itself be adversely impacted because no credit card company would want to take a chance on becoming secondarily liable?

We similarly take little comfort in the dissent's resurrection of the "dance-hall-owner/absentee-landlord" cases as a source of any principled distinction in this area. Dissent at 7874-75. Those tests were developed for a brick-and-mortar world, and, as the Napster and Grokster courts implicitly recognized by paying little attention to them, they do not lend themselves well to application in an electronic commerce context. In deciding this case, we are well-advised to follow the lead of the Supreme Court's and our own court's cases confronting online commerce issues.
Our holding is also fully consistent with and supported by this court's previous holdings in Fonovisa and Napster. While there are some limited similarities between the factual scenarios in Fonovisa and Napster and the facts in this case, the differences in those scenarios are substantial, and, in our view, dispositive. In Fonovisa, we held a flea market proprietor liable as a contributory infringer when it provided the facilities for and benefitted from the sale of pirated works. 76 F.3d 259. The court found that the primary infringers and the swap meet were engaged in a mutual enterprise of infringement and observed that "it would be difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet. These services include, among other things, the provision of space, utilities, parking, advertising, plumbing, and customers." 76 F.3d at 264. But the swap meet owner did more to encourage the enterprise. In 1991, the Fresno County Sheriff raided the swap meet and seized 38,000 counterfeit recordings. Id. at 261. The Sheriff sent a letter to the swap meet operator the following year notifying it that counterfeit sales continued and reminding it that it had agreed to provide the Sheriff with identifying information from each vendor, but had failed to do so. Id. The Fonovisa court found liability because the swap meet operator knowingly provided the "site and facilities" for the infringing activity. Id. at 264.

In Napster, this court found the designer and distributor of a software program liable for contributory infringement. 239 F.3d 1004. Napster was a file-sharing program which, while capable of non-infringing use, was expressly engineered to enable the easy exchange of pirated music and was widely so used. See Napster, 239 F.3d at 1020 n.5 (quoting document authored by Napster co-founder which mentioned "the need to remain ignorant of users' real names and IP addresses 'since they are exchanging pirated music'"). Citing the Fonovisa standard, the Napster court found that Napster materially contributes to the users' direct infringement by
knowingly providing the “site and facilities” for that infringement. 239 F.3d at 1022.

Seeking to draw an analogy to Fonovisa and, by extension, Napster, Perfect 10 pleads that Defendants materially contribute to the infringement by offering services that allow it to happen on a larger scale than would otherwise be possible. Specifically, because the swap meet in Fonovisa created a commercial environment which allowed the frequency of that infringement to increase, and the Napster program increased the frequency of infringement by making it easy, Perfect 10 argues that the Defendants have made available a payment system that allows third-party infringement to be profitable, and, consequently, more widespread than it otherwise might be. This analogy fails.

The swap meet operator in Fonovisa and the administrators of the Napster and Grokster programs increased the level of infringement by providing a centralized place, whether physical or virtual, where infringing works could be collected, sorted, found, and bought, sold, or exchanged. The provision of parking lots, plumbing and other accoutrements in Fonovisa was significant only because this was part of providing the environment and market for counterfeit recording sales to thrive.

Defendants, in contrast, do no such thing. While Perfect 10 has alleged that it is easy to locate images that infringe its copyrights, the Defendants’ payment systems do not cause this. Perfect 10’s images are easy to locate because of the very nature of the Internet—the website format, software allowing

---

In fact, as virtually every interested college student knew—and as the program’s creator expressly admitted—the sole purpose of the Napster program was to provide a forum for easy copyright infringement. See Napster, 239 F.3d at 1020 n.5. Perfect 10 does not contend that Defendants’ payment systems were engineered for infringement in this way, and we decline to radically expand Napster’s cursory treatment of “material contribution” to cover a credit card payment system that was not so designed.
for the easy alteration of images, high-speed connections allowing for the rapid transfer of high-resolution image files, and perhaps most importantly, powerful search engines that can aggregate and display those images in a useful and efficient manner, without charge, and with astounding speed. Defendants play no role in any of these functions.

Perfect 10 asserts otherwise by arguing for an extremely broad conception of the term “site and facilities” that bears no relationship to the holdings in the actual “cases and controversies” decided in *Fonovisa* and *Napster*. Taken literally, Perfect 10’s theory appears to include any tangible or intangible component related to any transaction in which infringing material is bought and sold. But *Fonovisa* and *Napster* do not require or lend themselves to such a construction. The actual display, location, and distribution of infringing images in this case occurs on websites that organize, display, and transmit information over the wires and wireless instruments that make up the Internet. The websites are the “site” of the infringement, not Defendants’ payment networks. Defendants do not create, operate, advertise, or otherwise promote these websites. They do not operate the servers on which they reside. Unlike the *Napster* (and *Grokker*) defendants, they do not provide users the tools to locate infringing material, nor does any infringing material ever reside on or pass through any network or computer Defendants operate. Defendants merely provide a method of payment, not a “site” or “facility” of infringement. Any conception of “site and facilities” that

*Moreover, if the processing of payment for an infringing transaction were as central to the infringement as the dissent believes it to be—see, e.g., dissent at 7867 (payment processing is “an essential step in the infringement process”), dissent at 7873 (“Defendants are directly involved in every infringing transaction where payment is made by credit card”)—it is difficult to see why Defendants would be not be direct infringers of the distribution right. Not even Perfect 10 has gone so far as to allege that theory here—Perfect 10 would undoubtedly be quite surprised to learn, after years of litigation attempting to expand the scope of secondary liability, that Defendants are direct infringers after all.*
encompasses Defendants would also include a number of peripherally-involved third parties, such as computer display companies, storage device companies, and software companies that make the software necessary to alter and view the pictures and even utility companies that provide electricity to the Internet.

Perfect 10 seeks to side-step this reality by alleging that Defendants are still contributory infringers because they could refuse to process payments to the infringing websites and thereby undermine their commercial viability. Even though we must take this factual allegation as true, that Defendants have the power to undermine the commercial viability of infringement does not demonstrate that the Defendants materially contribute to that infringement. As previously noted, the direct infringement here is the reproduction, alteration, display and distribution of Perfect 10’s images over the Internet. Perfect 10 has not alleged that any infringing material passes over Defendants’ payment networks or through their payment processing systems, or that Defendants designed or promoted their payment systems as a means to infringe. While Perfect 10 has alleged that Defendants make it easier for websites to profit from this infringing activity, the infringement stems from the failure to obtain a license to distribute, not the processing of payments.

2. Inducement

[6] In Grokster, the Supreme Court applied the patent law concept of “inducement” to a claim of contributory infringement against a file-sharing program. 545 U.S. 913. The court found 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

---

10 This allegation is considered below under vicarious infringement, but we also address it here in terms of contributory infringement.
parties.” *Id.* at 936-37. Perfect 10 claims that *Grokster* is analogous because Defendants induce customers to use their cards to purchase goods and services, and are therefore guilty of specifically inducing infringement if the cards are used to purchase images from sites that have content stolen from Perfect 10. This is mistaken. Because Perfect 10 alleges no “affirmative steps taken to foster infringement” and no facts suggesting that Defendants promoted their payment system as a means to infringe, its claim is premised on a fundamental misreading of *Grokster* that would render the concept of “inducement” virtually meaningless.

[7] The *Grokster* court announced that the standard for inducement liability is providing a service “with the object of promoting its use to infringe copyright.” *Id.* “[M]ere knowledge of infringing potential or actual infringing uses would not be enough here to subject [a defendant] to liability.” *Id.* at 937. Instead, inducement “presents liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful purpose.” *Id.* Moreover, to establish inducement liability, it is crucial to establish that the distributors “communicated an inducing message to their . . . users,” the classic example of which is an “advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations.” *Id.* The *Grokster* court summarized the “inducement” rule as follows:

In sum, where an article is good for nothing else but infringement, there is no legitimate public interest in its unlicensed availability, and there is no injustice in presuming or imputing an intent to infringe. 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.

545 U.S. at 932-33 (internal citations and quotation marks omitted).

Perfect 10 has not alleged that any of these standards are met or that any of these considerations are present here. Defendants do, of course, market their credit cards as a means to pay for goods and services, online and elsewhere. But it does not follow that Defendants affirmatively promote each product that their cards are used to purchase. The software systems in Napster and Grokster were engineered, disseminated, and promoted explicitly for the purpose of facilitating piracy of copyrighted music and reducing legitimate sales of such music to that extent. Most Napster and Grokster users understood this and primarily used those systems to purloin copyrighted music. Further, the Grokster operators explicitly targeted then-current users of the Napster program by sending them ads for its OpenNap program. Id. at 925-26. In contrast, Perfect 10 does not allege that Defendants created or promote their payment systems as a means to break laws. Perfect 10 simply alleges that Defendants generally promote their cards and payment systems but points to no “clear expression” or “affirmative acts” with any specific intent to foster infringement.

[8] The Amazon.com court recognized this distinction and applied it in a matter fully consistent with our analysis in this case. While the Amazon.com court did not bifurcate its analysis of contributory liability into “material contribution” liability and “inducement” liability, it did recognize that contributory liability “may be predicated on actively encouraging (or inducing) infringement through specific acts.” Amazon.com, 2007 WL 1428632, at *16 (quoting Grokster, 545 U.S. at 942 (Ginsburg, J., concurring)). It also found that Google could be held contributorily liable if it has “actual knowledge that specific infringing material is available using
its system, and can take simple measures to prevent further damage,” but does not. *Id.* at *18* (internal citations and quotation marks omitted). While this test is read more naturally as a test for “material contribution” than as a test for “inducement,” under an “inducement” analysis Defendants are not within its scope. As discussed above, Perfect 10 has not alleged any “specific acts” intended to encourage or induce infringement. And moreover, Defendants are distinguishable under the *Amazon.com* test because, unlike Google, infringing material is not “available using [their] system” of payment processing. *Id.* That system does not “facilitate access to websites,” *id.*; infringers do not use it to copy, alter, distribute or display infringing material; and consumers do not use it to locate, view or download the infringing images. Rather, all parties involved simply use Defendants’ system to process payments for that infringing material.

[9] Finally, we must take as true the allegations that Defendants lend their names and logos to the offending websites and continue to allow their cards to be used to purchase infringing images despite actual knowledge of the infringement—and perhaps even bending their association rules to do so. But we do not and need not, on this factual basis, take as true that Defendants “induce” consumers to buy pirated content with their cards. “Inducement” is a legal determination, and dismissal may not be avoided by characterizing a legal determination as a factual one. We must determine whether the facts as pled constitute a “clear expression” of a specific intent to foster infringement, and, for the reasons above noted, we hold that they do not.

2. Vicarious Copyright Infringement

[10] Vicarious infringement is a concept related to, but distinct from, contributory infringement. Whereas contributory infringement is based on tort-law principles of enterprise liability and imputed intent, vicarious infringement’s roots lie in the agency principles of *respondeat superior*. See *Fonovisa,*
76 F.3d at 261-62. To state a claim for vicarious copyright infringement, a plaintiff must allege that the defendant has (1) the right and ability to supervise the infringing conduct and (2) a direct financial interest in the infringing activity. Ellison, 357 F.3d at 1078; Napster, 239 F.3d at 1022 (citations omitted). The Supreme Court has recently offered (in dictum) an alternate formulation of the test: "One . . . infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." Grokster, 545 U.S. at 930 (internal citations omitted). Perfect 10 alleges that Defendants have the right and ability to control the content of the infringing websites by refusing to process credit card payments to the websites, enforcing their own rules and regulations, or both. We hold that Defendants' conduct alleged in Perfect 10's first amended complaint fails to state a claim for vicarious copyright infringement.

a. Right and Ability to Supervise the Infringing Activity

[11] In order to join a Defendant's payment network, merchants and member banks must agree to follow that Defendant's rules and regulations. These rules, among other things, prohibit member banks from providing services to merchants engaging in certain illegal activities and require the members and member banks to investigate merchants suspected of engaging in such illegal activity and to terminate their participation in the payment network if certain illegal activity is found. Perfect 10 has alleged that certain websites are infringing Perfect 10's copyrights and that Perfect 10 sent notices of this alleged infringement to Defendants. Accordingly, Perfect 10 has adequately pled that (1) infringement of Perfect 10's copyrights was occurring, (2) Defendants were aware of the

---

Footnote: Essentially viewed "supervision" in this context in terms of the swap meet operator's ability to control the activities of the vendors, 76 F.3d at 262, and Napster essentially viewed it in terms of Napster's ability to police activities of its users, 239 F.3d at 1023.
infringement, and (3) on this basis, Defendants could have stopped processing credit card payments to the infringing websites. These allegations are not, however, sufficient to establish vicarious liability because even with all reasonable inferences drawn in Perfect 10’s favor, Perfect 10’s allegations of fact cannot support a finding that Defendants have the right and ability to control the infringing activity.

In reasoning closely analogous to the present case, the Amazon.com court held that Google was not vicariously liable for third-party infringement that its search engine facilitates. In so holding, the court found that Google’s ability to control its own index, search results, and webpages does not give Google the right to control the infringing acts of third parties even though that ability would allow Google to affect those infringing acts to some degree. Amazon.com, 2007 WL 1428632, at *20-21. Moreover, and even more importantly, the Amazon.com court rejected a vicarious liability claim based on Google’s policies with sponsored advertisers, which state that it reserves “the right to monitor and terminate partnerships with entities that violate others’ copyright[s].” Id. at *20 (alteration in original). The court found that

Google’s right to terminate an AdSense partnership does not give Google the right to stop direct infringement by third-party websites. An infringing third-party website can continue to reproduce, display, and distribute its infringing copies of Perfect 10 images after its participation in the AdSense program has ended.

Id. This reasoning is equally applicable to the Defendants in this case. Just like Google, Defendants could likely take certain steps that may have the indirect effect of reducing infringing activity on the Internet at large. However, neither Google nor Defendants has any ability to directly control that activity, and the mere ability to withdraw a financial “carrot” does not create the “stick” of “right and ability to control” that
vicarious infringement requires. A finding of vicarious liability here, under the theories advocated by the dissent, would also require a finding that Google is vicariously liable for infringement—a conflict we need not create, and radical step we do not take.

Perfect 10 argues that this court’s decision in Napster compels a contrary result. The Napster court found a likelihood of vicarious liability because Napster “had the right and ability to police its system and failed to exercise that right to prevent the exchange of copyrighted material.” 239 F.3d at 1023. The Napster program created a forum for the exchange of digital music files and the program administrators had the ability to block certain users from accessing that forum to upload or download such files. As pled by Perfect 10, Defendants also provide a system that allows the business of infringement for profit to operate on a larger scale than it otherwise might, and Defendants have the ability to deny users access to that payment system.

This argument fails. The Napster program’s involvement with—and hence its “policing” power over—the infringement was much more intimate and directly intertwined with it than Defendants’ payment systems are. Napster provided users with the tools to enable the easy reproduction and distribution of the actual infringing content and to readily search out and identify infringing material. Defendants’ payment systems do not. Napster also had the right and ability to block user access to its program and thereby deprive particular users of access to their forum and use of their location and distribution tools. Defendants can block access to their payment system, but they cannot themselves block access to the Internet, to any particular websites, or to search engines enabling the location of such websites. Defendants are involved with the payment resulting from violations of the distribution right, but have no direct role in the actual reproduction, alteration, or distribution of the infringing images. They cannot take away the

\[14\] The same analysis of Defendants’ role in any violation of the distribution right under 17 U.S.C. §106(3), discussed in note 11, supra, is equally
tools the offending websites use to reproduce, alter, and distribute the infringing images over the Internet. They can only take away the means the websites currently use to sell them. 15

Perfect 10 offers two counter-arguments. Perfect 10 first claims that Defendants’ rules and regulations permit them to require member merchants to cease illegal activity—presumably including copyright infringement—as a condition to their continuing right to receive credit card payments from the relevant Defendant entities. Perfect 10 argues that these contractual terms effectively give Defendants contractual control over the content of their merchants’ websites, and that contractual control over content is sufficient to establish the “right and ability” to control that content for purposes of vicarious liability. In the sense that economic considerations can influence behavior, these contractual rules and regulations do give Defendants some measure of control over the offending websites since it is reasonable to believe that fear of losing access to credit card payment processing services would be a sufficient incentive for at least some website operators to

applicable here. While the Napster program allowed its operators to block users from violation of the distribution right, Defendants’ “policing” power is limited to refusing to process payments resulting from such violations and does not extend to directly stopping the violations themselves.

The conclusion that the Defendants operate outside the scope of the Napster rule is further bolstered by consideration—though as persuasive authority only—of this court’s opinion in Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 360 F.3d 1154 (9th Cir. 2004), which the Supreme Court vacated on other grounds, 545 U.S. 913 (2005). In Grokster, we found the defendants not vicariously liable in part because they could not block individual users or remove copyrighted material from the network. Id. at 1165. Similarly, because none of the infringing images resides on or passes through present Defendants’ own systems or any systems over which Defendants exercise direct control, Defendants have no ability to actually remove infringing material from the Internet or directly block its distribution. This distinguishes credit card companies from Napster, which could block access to the tools needed for the easy reproduction and distribution of the actual infringing content.
comply with a content-based suggestion from Defendants. But the ability to exert financial pressure does not give Defendants the right or ability to control the actual infringing activity at issue in this case. Defendants have no absolute right to stop that activity—they cannot stop websites from reproducing, altering, or distributing infringing images. Rather, the credit card companies are analogous to Google, which we held was not liable for vicarious copyright infringement even though search engines could effectively cause a website to disappear by removing it from their search results, and reserve the right to do so. Like Google, the credit card companies “cannot stop any of the third-party websites from reproducing, displaying, and distributing unauthorized copies of Perfect 10’s images because that infringing conduct takes place on the third-party websites.” Amazon.com, 2007 WL 1428632, at *20. Defendants can only refuse to process credit card payments to the offending merchant within their payment network, or they can threaten to do so if the merchant does not comply with a request to alter content. While either option would likely have some indirect effect on the infringing activity, as we discuss at greater length in our analysis of the Grokster “stop or limit” standard below, so might any number of actions by any number of actors. For vicarious liability to attach, however, the defendant must have the right and ability to supervise and control the infringement, not just affect it, and Defendants do not have this right or ability.

Perfect 10 relies heavily on the reasoning of Fonovisa and Napster to support this argument, but that reliance is misplaced. The swap meet operator in Fonovisa and the software operator in Napster both had the right to remove individual

---

16We do not, as the dissent suggests, hold that an absolute right to stop the infringement is a prerequisite for vicarious liability. Dissent at 7878-79. Rather, we consider the Defendants’ inability to directly control the actual infringing activities of third-party websites—reproduction, alteration, display, and distribution over the Internet, not over Defendants’ payment systems—as evidence that they, much like Google, lack the right and ability to control those activities.
infringers from the very place the infringement was happening. Defendants, like the defendants in *Amazon.com*, have no such right. As already discussed, Defendants cannot take away the software the offending websites use to copy, alter, and distribute the infringing images, cannot remove those websites from the Internet, and cannot themselves block the distribution of those images over the Internet. Defendants can refuse to process credit card payments for those images, but while this refusal would reduce the number of those sales, that reduction is the result of indirect economic pressure rather than an affirmative exercise of contractual rights.\(^\text{17}\)

Perfect 10 also argues that were infringing websites barred from accepting the Defendants’ credit cards, it would be impossible for an online website selling adult images to compete and operate at a profit.\(^\text{18}\) While we must take this allega-

\(^{17}\)We do not hold, as the dissent suggests, that the ability to exert financial pressure is categorically insufficient to establish sufficient control for vicarious liability. We recognize that financial pressure is often very powerful, but it is precisely for this reason that we hesitate to expand the law of vicarious liability to encompass the sort of financial pressure Defendants may exert. The dissent believes that the gravamen of “right and ability to control” is the “practical ability” to limit infringement. Dissent at 7878-79. But if this were true, despite the dissent’s protestations to the contrary, there are many providers of essential services who could limit infringement by refusing to offer those services. If “practical ability” is the test, it does not matter if software operators, network technicians, or even utility companies do not have a contractual right to affect the websites’ content. It is an article of faith of the free market that, subject to certain limited exceptions, one can refuse to deal with anyone for any reason, and by refusing to deal with the offending websites, these providers could limit infringement.

\(^{18}\)Specifically, Perfect 10 defines “Stolen Content Websites” as “websites . . . that routinely offer for sale to the public stolen [images],” First Am. Compl. at 2, ¶ 6 (emphasis added), and alleges that “Stolen Content Websites cannot exist without the knowledge and direct participation of the financial institutions that process the credit card transactions for such unlawful material,” id. at 2, ¶ 7. We do acknowledge that at this procedural stage, Perfect 10 is entitled to all reasonable inferences, but we
tion as true, it still fails to state a claim because it conflates the power to stop profiteering with the right and ability to control infringement. Perfect 10’s allegations do not establish that Defendants have the authority to prevent theft or alteration of the copyrighted images, remove infringing material from these websites or prevent its distribution over the Internet. Rather, they merely state that this infringing activity could not be profitable without access to Defendants’ credit card payment systems. The alleged infringement does not turn on the payment; it turns on the reproduction, alteration and distribution of the images, which Defendants do not do, and which occurs over networks Defendants do not control.

[12] The Supreme Court’s recent decision in Grokster does not undermine the validity of this distinction. As we held in Amazon.com, 2007 WL 1428632, at *19-20, Grokster does not stand for the proposition that just because the services provided by a company help an infringing enterprise generate revenue, that company is necessarily vicariously liable for that infringement. Numerous services are required for the third party infringers referred to by Perfect 10 to operate. In addition to the necessity of creating and maintaining a website, numerous hardware manufacturers must produce the computer on which the website physically sits; a software engineer must create the program that copies and alters the stolen images; technical support companies must fix any hardware and software problems; utility companies must provide the electricity that makes all these different related operations run, etc. All these services are essential to make the businesses described viable, they all profit to some degree from those businesses, and by withholding their services, they understand this to be a factual allegation that the “Stolen Content Websites” could not continue to exist as websites offering images for sale online should defendants withdraw their services, not an allegation that the websites would completely vanish or that infringement by these sites in all its forms would necessarily cease.
could impair—perhaps even destroy—the commercial viability of those businesses. But that does not mean, and Grokster by no means holds, that they are all potentially liable as vicarious infringers. Even though they have the “right” to refuse their services, and hence the literal power to “stop or limit” the infringement, they, like Defendants, do not exercise sufficient control over the actual infringing activity for vicarious liability to attach.

b. Obvious and Direct Financial Interest in the Infringing Activity

[13] Because Perfect 10 has failed to show that Defendants have the right and ability to control the alleged infringing conduct, it has not pled a viable claim of vicarious liability. Accordingly, we need not reach the issue of direct financial interest.

B. Secondary Liability for Trademark Infringement

The tests for secondary trademark infringement are even more difficult to satisfy than those required to find secondary copyright infringement. See Sony Corp. v. Universal City Studios, 464 U.S. 417, 439 n.19 (1984); Fonovisa, 76 F.3d at 265 (noting that “trademark infringement liability is more narrowly circumscribed than copyright infringement”). While the tests for such infringement are somewhat different in the trademark context, Perfect 10’s factual allegations in support of these claims are essentially identical to those alleged in Perfect 10’s copyright claims, and they fail to state a claim for similar reasons.

1. Contributory Trademark Infringement

[14] To be liable for contributory trademark infringement, a defendant must have (1) “intentionally induced” the primary infringer to infringe, or (2) continued to supply an infringing product to an infringer with knowledge that the infringer is
C. Libel and Intentional Interference with Prospective Economic Advantage

The district court dismissed Perfect 10's claims of libel and intentional interference with prospective economic advantage with prejudice on multiple grounds. We affirm on the ground that both are time-barred. Under California law, a libel claim must be filed within one year of publication of the allegedly libelous statement, Cal. Civ. Proc. § 340(c), and an intentional interference claim must be filed within two years of the underlying harmful act, Cal. Civ. Proc. § 339. Perfect 10 claims the same underlying wrongful act as the basis for both claims: its placement on the industry “black list” in the Spring of 2001. However, Perfect 10 failed to file suit until January 2004—well beyond the statute of limitations applicable to each claim—and has failed to show any possible exception under either statute. Those claims are time-barred.

CONCLUSION

We decline to create any of the radical new theories of liability advocated by Perfect 10 and the dissent and we affirm the district court's dismissal with prejudice of all causes of action in Perfect 10's complaint for failure to state a claim upon which relief can be granted.

AFFIRMED.

KOZINSKI, Circuit Judge, dissenting for the most part:

Federal law gives copyright owners the exclusive right to “distribute copies [of their works] . . . to the public by sale.”

1I join part C of the “California Statutory and Common Law Claims” section of the opinion, dealing with plaintiff's libel and prospective economic advantage claims.
17 U.S.C. § 106(3). Plaintiff alleges that certain third parties it refers to as the "Stolen Content Websites" unlawfully copy its protected images and sell them to the public, using defendants' payment systems as financial intermediaries. According to plaintiff, the Stolen Content Websites "maintain no physical presence in the United States in order to evade criminal and civil liability for their illegal conduct." First Am. Compl. at 8 ¶ 26. Plaintiff also claims that "Defendants do not enforce their own rules against [the] Stolen Content Websites because Defendants do not want to lose the substantial revenues and profits they receive from the websites." Id. at 10 ¶ 35. Plaintiff has repeatedly notified defendants that they are abetting the sale of stolen merchandise by "knowingly providing crucial transactional support services for the sale of millions of stolen photos and film clips worth billions of dollars," id. at 1 ¶ 5, but to no avail. Frustrated in its effort to protect the rights Congress has given it, plaintiff turns to the federal courts for redress. We should not slam the courthouse door in its face.

Accepting the truth of plaintiff's allegations, as we must on a motion to dismiss, the credit cards' are easily liable for indirect copyright infringement: They knowingly provide a financial bridge between buyers and sellers of pirated works, enabling them to consummate infringing transactions, while making a profit on every sale. If such active participation in infringing conduct does not amount to indirect infringement,

---

2Throughout this dissent, I refer to defendants collectively as credit card companies or credit cards. In so doing, I am adopting the same simplifying assumptions as the majority. I am aware that Visa and MasterCard don't deal directly with merchants; rather, merchants obtain credit card accounts from banks, which are in turn authorized by Visa or MasterCard to use their respective payment systems. Some of the other defendants are involved in clearing these transactions. For a description of how the system works, see Emery v. Visa Int'l Serv. Ass'n, 95 Cal. App. 4th 952, 956 (2002). It may well be that some of the defendants will be absolved of liability because they have no direct contact with merchants or consumers, but that is a matter to be sorted out after discovery.
it’s hard to imagine what would. By straining to absolve defendants of liability, the majority leaves our law in disarray.

**Contributory Infringement**

We have long held that a defendant is liable for contributory infringement if it “materially contributes to the infringing conduct.” *AE&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2001) (internal quotations omitted) (citing *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971)). Our recent opinion in *Perfect 10, Inc. v. Amazon.com, Inc.*, slip op. at 5751 (9th Cir. 2007), canvasses the caselaw in this area and concludes that Google “could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10’s copyrighted works, and failed to take such steps.” *Amazon*, slip op. at 5793. Substitute “payment systems” for “search engine” in this sentence, and it describes defendants here: If a consumer wishes to buy an infringing image from one of the Stolen Content Websites, he can do so by using Visa or MasterCard, just as he can use Google to find the infringing images in the first place. My colleagues engage in wishful thinking when they claim that “Google’s search engine itself assists in the distribution of infringing content to Internet users, while Defendants’ payment systems

---

3As the majority points out, maj. op. at 7842 n.6, 7846 n.11, plaintiff’s allegations might also support a theory of direct infringement. See First Am. Compl. at 8 ¶ 30 (“Defendants, jointly with the Stolen Content Websites, are engaged in . . . the willful and systematic infringement of the intellectual property rights of” plaintiff and others). Because plaintiff has not argued this theory on appeal, we have no occasion to address it. But the fact that defendants may also be committing direct infringement does not diminish their responsibility as indirect infringers for providing essential services to buyers and sellers of stolen merchandise. A defendant can be liable for both direct and indirect infringement based on the same conduct. See, e.g., *Alcatel USA, Inc. v. DGI Technologies, Inc.*, 166 F.3d 772, 791 (5th Cir. 1999).
do not” and that “[h]elping users to locate an image might substantially assist users to download infringing images, but processing payments does not.” Maj. op. at 7841, 7842.4

The majority struggles to distinguish Amazon by positing an “additional step in the causal chain” between defendants’ activities and the infringing conduct. Id. at 7842. According to the majority, “Google may materially contribute to infringement by making it fast and easy for third parties to locate and distribute infringing material, whereas Defendants make it easier for infringement to be profitable, which tends to increase financial incentives to infringe, which in turn tends to increase infringement.” Id. The majority is mistaken; there is no “additional step.” Defendants participate in every credit card sale of pirated images; the images are delivered to the buyer only after defendants approve the transaction and process the payment. This is not just an economic incentive for infringement; it’s an essential step in the infringement process.

In any event, I don’t see why it matters whether there is an “additional step.” Materiality turns on how significantly the activity helps infringement, not on whether it’s characterized as one step or two steps removed from it. The majority recognizes that “Defendants make it easier for websites to profit from this infringing activity,” maj. op. at 7841; that defendants’ conduct “tends to increase infringement,” id. at 7842; that defendants “have the effect of increasing . . . infringement,” id. at 7843; that “Defendants have the power to undermine the commercial viability of” the Stolen Content

4Neither Google nor the credit cards here were designed for infringement. The majority tries to distinguish this case from Napster and Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005), where defendants’ services were designed for no other purpose. Maj. op. at 7845 n.10, 7849. But Napster and Grokster are not the endpoint of this court’s caselaw: Even though Google has many legitimate, noninfringing uses, Amazon held that it would be guilty of contributory infringement if it could modify its service to avoid helping infringers.
Websites and that they "make it easier for websites to profit from this infringing activity," id. at 7847; that "Defendants could likely take certain steps that may have the indirect effect of reducing infringing activity on the Internet," id. at 7852-53; and that defendants could "reduce the number of those [infringing] sales," id. at 7856. Taking the majority at its word, it sounds like defendants are providing very significant help to the direct infringers.

My colleagues recognize, as they must, that helping consumers locate infringing content can constitute contributory infringement, but they consign the means of payment to secondary status. Maj. op. at 7846 ("Defendants merely provide a method of payment . . . ."); id. at 7850 ("All parties involved simply use Defendants' system to process payments for that infringing material."); id. at 7854 ("They can only take away the means the websites currently use to sell [the infringing images]."); id. at 7855 ("Defendants can only refuse to process credit card payments to the offending merchant within their payment network . . . ."). But why is locating infringing images more central to infringement than paying for them? If infringing images can't be found, there can be no infringement; but if infringing images can't be paid for, there can be no infringement either. Location services and payment services are equally central to infringement; the majority's contrary assertion is supported largely by disparaging use of "merely," "simply" and "only." See also id. at 7852 ("[M]ere ability to withdraw a financial 'carrot' does not create the 'stick' of 'right and ability to control' . . . .").

Amazon, as well as Napster and Grokster, hold as much.

The majority argues that "[b]ecause location services lead Internet users directly to infringing images, and often display them on the website of the service itself, we find that location services are more important and more essential—indeed, more 'material'—to infringement than payment services are." Maj. op. at 7842-43 n.8. Skipping lightly over the fact that we lack the power to "find" anything, the majority admits that payment services are important, essential and material. That location services may—or may not—be more so, is of no consequence; this is not a race where there can be only one winner.
The majority dismisses the significance of credit cards by arguing that “infringement could continue on a large scale [without them] because other viable funding mechanisms are available.” Maj. op. at 7842. Of course, the same could be said about Google. As the majority admits, if Google were unwilling or unable to serve up infringing images, consumers could use Yahoo!, Ask.com, Microsoft Live Search, A9.com or AltaVista instead. Id. at 7842-43 n.8. Even if none of these were available, consumers could still locate websites with infringing images through e-mails from friends, messages on discussion forums, tips via online chat, “typo-squatting,” peer-to-peer networking using BitTorrent or eDonkey, offline and online advertisements (see pp. 7882 infra), disreputable search engines hosted on servers in far-off jurisdictions or even old-fashioned word of mouth. The majority’s claim that search engines “could effectively cause a website to disappear by removing it from their search results,” maj. op. at 7855, is quite a stretch.

If the test for contributory infringement really were whether “infringement could continue on a large scale [without the aid of the defendant] because other viable . . . mechanisms are available,” Amazon should have absolved Google of liability because of the availability of such obvious alternatives. But Amazon held that Google could be liable for contributory infringement because it “substantially assists” users in finding infringing materials; the existence of other means of infringe-

The majority’s claim that “Perfect 10’s factual allegations are not to the contrary,” maj. op. at 7842 n.7, is simply not accurate. Indeed, elsewhere in the opinion, the majority concedes that plaintiff has made “a factual allegation” that the Stolen Content Websites “could not continue to exist as websites offering images for sale online.” Id. at 7856 n.18. How then can the majority hold here, apparently as a matter of law, that defendants are absolved of liability because “other viable funding mechanisms are available”? Maj. op. at 7842. If we accept as true, as the majority says it does, that the Stolen Content Websites will no longer be able to sell their images, how can we hold that they could still do so by developing other (unknown and unsuspected) ways to get paid?
ment was not even considered because no case has suggested this to be a relevant consideration. The majority’s “other viable . . . mechanisms” test conflicts with Amazon, Napster, Grokster and every other material assistance case that I know of.

The majority does even worse when it tries to describe the “other viable funding mechanisms” that could serve as alternatives to credit cards. According to the majority, the Stolen Content Websites “might . . . make [their] profits from advertising” or “might develop other payment mechanisms that do not depend on the credit card companies.” Maj. op. at 7842 (emphasis added). This shows that my colleagues have a healthy imagination but contravenes our responsibilities, the most fundamental of which is that we must work with the facts the parties presented below, not invent new facts on appeal. Defendants have presented no evidence that the pirates could survive without credit cards, nor could they, as the case is still at the motion to dismiss stage. Even if speculation as to what the Stolen Content Websites “might” do were admissible evidence, which I seriously doubt, we must still wait for one of the parties to present it, not conjure it up ourselves. At the pleadings stage, we must accept plaintiff’s allegations that credit cards are indispensable to the operation of the Stolen Content Websites, and that these websites would be forced out of business without them. See First Am. Compl. at 2 ¶ 7 (“Stolen Content Websites cannot exist without the knowledge and direct participation of [defendants].”); id. at 10 ¶ 35 (“[T]he Stolen Content Websites would be eradicated.”). If my colleagues can’t justify their result without con-

*I note in passing that, even if we were to accept the majority’s speculations, they would be insufficient. That the Stolen Content Websites “might” change the way they do business or develop alternative payment mechanisms hardly proves that “other viable funding mechanisms are available.” Maj. op. at 7842 (emphasis added). The majority’s prognostication as to what “might” happen in the future leaves open the likelihood that it will not happen, and positively admits that there are no viable alternative payment mechanisms today.
trajecting plaintiff’s allegations, this is a pretty good hint that they’re wrong. See also p. 7869 n.7 supra; pp. 7878 n.15, 7848-50 infra.

The majority’s attempt to distinguish location services from payment services by trying to show that there are viable alternatives for the latter but not the former cuts entirely against them. As plaintiff alleges, and experience tells us, there are numerous ways of locating infringing images on the Internet, but there are no adequate substitutes for credit cards when it comes to paying for them. A few consumers might use checks or money orders to pay for infringing images, but this would be far more cumbersome, time-consuming and risky than using credit cards. See pp. 7845-46 & n.14 infra. If it mattered whether search engines or credit cards are more important to peddling infringing content on the Internet, the cards would win hands down.

But it doesn’t matter. Material assistance turns on whether the activity in question “substantially assists” infringement. *Amazon*, slip op. at 5793. It makes no difference whether the primary infringers might do without it by finding a workaround, which is why the majority can cite no case supporting its analysis. We presume that primary infringers have good reasons for selecting a particular means to infringe, and that other ways to do so will be more costly, more cumbersome and less efficient. Moreover, infringement can always be carried out by other means; if the existence of alternatives were a defense to contributory infringement then there could never be a case of contributory infringement based on material assistance. The majority makes some very new—and very bad—law here.

The majority also makes a slightly different argument: “While Perfect 10 has alleged that Defendants make it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display and distribution, which can occur without payment. Even if infringing images
were not paid for, there would still be infringement.” Maj. op. at 7840-41. What the majority seems to be arguing here is that helping an infringer get paid cannot materially assist infringement because the actual process of infringement—“reproduction, alteration, display and distribution”—does not include payment. There are two problems with this argument. The first is that the Stolen Content Websites are alleged to infringe plaintiff’s right of distribution “by sale,” 17 U.S.C. § 106(3). It’s not possible to distribute by sale without receiving compensation, so payment is in fact part of the infringement process. Second, this argument runs head-on into Amazon, where we held that helping to find infringing images materially assists infringement, even though locating infringing images also isn’t “reproduction, alteration, display [or] distribution.” To be sure, locating images, like paying for them, makes it a lot easier to infringe, but neither is intrinsic to the infringement process, as the majority conceives it.

Nor can today’s opinion be squared with Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996). In Fonovisa, defendant allowed known infringers to sell pirated works from stalls at its swap meet. We found material assistance based on the fact that “it would [have been] difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet.” 76 F.3d at 264. The pivotal role played by the swap meet in Fonovisa is played by the credit cards in cyberspace, in that they make “massive quantities” of infringement possible that would otherwise be impossible. Indeed, the assistance provided here is far more material than in Fonovisa. A pirate kicked out of a swap meet could still peddle his illicit wares through newspaper ads or by word of mouth, but you can’t do business at all on the Internet without credit cards. Plaintiff thus plausibly alleges that the “Stolen Content Websites would be eradicated” if defendants withdrew their support. First Am. Compl. at 10 ¶ 35.
The majority rejects Fonovisa by pointing out that the swap meet there provided a "centralized place" for the infringement to take place, maj. op. at 7845, whereas defendants here "have no direct connection to [the] infringement," id. at 7840. But material assistance does not depend on physical contact with the infringing activity. If you lend money to a drug dealer knowing he will use it to finance a drug deal, you materially assist the transaction, even if you never see the drugs. Or, if you knowingly drive a principal to the scene of the crime, you provide material assistance, even if nothing happens during the ride. See United States v. Lopez, 482 F.3d 1067, 1076-79 (9th Cir. 2007). Material assistance turns on whether the conduct assists infringement in a significant way, not on pedantic factual distinctions unrelated to how much the activity facilitates infringement.

Sure, a marketplace for pirated works (as in Fonovisa) or an index for such works (as in Napster and Grokster) is important to infringement, but so is a means of getting paid. Defendants are directly involved in every infringing transaction where payment is made by credit card, which (according to plaintiff) amounts to virtually every sale of pirated works. First Am. Compl. at 9 ¶ 35. Credit cards don't provide some tangential service that marginally affects sales; they are the financial lifeblood of the Stolen Content Websites.

The majority's concern that imposing liability on defendants here would implicate vast numbers of other actors who provide incidental services to infringers, maj. op. at 7847, is unfounded. Line-drawing is always a bit tricky, but courts have shown themselves adept at dealing with it from time out of mind, in resolving such issues as proximate causation and

---

8 The majority seeks to distinguish Napster and Grokster on similar grounds by arguing that the defendants do not provide the "tools to locate infringing material," id. at 7846, and that the infringing material "[n]ever reside[s] on or pass[es] through any network or computer Defendants operate," id.
reasonable suspicion. Contributory infringement requires material assistance to the infringing activity, and those the majority worries about would doubtless be absolved of liability because their contribution to the infringing activity is insufficiently material.

Courts have, in fact, had no difficulty in distinguishing those who are materially involved in copyright infringement from those who are not. As Fonovisa explains, two lines of cases developed in the first part of the last century: the absentee landlord cases and the dance hall cases. The first line involved landlords who "lacked knowledge of the infringing acts of [their] tenant[s] and who exercised no control over the leased premises." Fonovisa, 76 F.3d at 262. These were held not liable for the infringement committed by tenants on the premises. See, e.g., Deutsch v. Arnold, 98 F.2d 686, 688 (2d Cir. 1938). In the second line of cases, "the operator of an entertainment venue was held liable for infringing performances when the operator (1) could control the premises and (2) obtained a direct financial benefit from the audience, who paid to enjoy the infringing performance." 76 F.3d at 262 (citing Buck v. Jewell-LaSalle Realty Co., 283 U.S. 191 (1931), and Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929)).

10The majority consigns the dance hall/absentee landlord cases to oblivion by holding that they have no relevance to the Internet. Maj. op. at 7843 n.9. It is true that these cases were developed in a brick and mortar world, but the distinction they draw between those who materially assist infringement (and are therefore liable) and those who are more remotely involved (and are therefore not liable) is equally important—perhaps even more important—in cyberspace than in real space. That Napster and Grokster did not consider these cases is hardly significant. The defendants there were centrally involved in the infringing transactions—indeed, as the majority reminds us, their systems were created solely to promote infringement, maj. op. at 7845 n.10, 7849—and thus there could be no argument that their involvement in the infringing transactions was too peripheral to give rise to a claim of secondary infringement. The Seventh Circuit managed to apply the dance hall cases to the Internet, see In re Aimster Copyright Litig., 334 F.3d 643, 654 (7th Cir. 2003), and I'm confident that federal judges west of the Rockies could have figured out how to do the same.
These cases show that courts are able to forestall the majority’s parade of horribles. But our case does not present a close or difficult question: Defendants here are alleged to provide an essential service to infringers, a service that enables infringement on a massive scale. Defendants know about the infringements; they profit from them; they are intimately and causally involved in a vast number of infringing transactions that could not be consummated if they refused to process the payments; they have ready means to stop the infringements. Were we to rule for plaintiff, as we should, I have every confidence that future courts would be able to distinguish this case when and if they are confronted with lawsuits against utility companies, software vendors and others who provide incidental services to infringers.

Vicarious Infringement

A party “infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.” Amazon, slip op. at 5794 (quoting Grokster, 545 U.S. at 930) (internal quotation marks omitted). There is no doubt that defendants profit from the infringing activity of the Stolen Content Websites; after all, they take a cut of virtually every sale of pirated material. First Am. Compl. at 4 ¶ 13, 7 ¶ 25. The majority does not dispute this point so I need not belabor it. Maj. op. at 7857-58.

Defendants here also have a right to stop or limit the infringing activity, a right they have refused to exercise. As the majority recognizes, “Perfect 10 . . . claims that Defendants’ rules and regulations permit them to require member merchants to cease illegal activity—presumably including copyright infringement—as a condition to their continuing right to receive credit card payments from the relevant Defen-

11Amazon interprets the “stop or limit” language as requiring “a legal right to stop or limit the allegedly infringing conduct, as well as the practical ability to do so.” Amazon, slip op. at 5786-87.
dant entities." Maj. op. at 7854. Assuming the truth of this allegation, the cards have the authority, given to them by contract, to force the Stolen Content Websites to remove infringing images from their inventory as a condition for using defendants' payment systems. If the merchants comply, their websites stop peddling stolen content and so infringement is stopped or limited. If they don't comply, defendants have the right—and under copyright law the duty—to kick the pirates off their payment networks, forcing them to find other means of getting paid or go out of business. In that case, too, infringement is stopped or limited. The swap meet in Fonovisa was held vicariously liable precisely because it did not force the pirates to stop infringing or leave; there is no reason to treat defendants here differently.

That the pirates might find some other way of doing business is of no consequence; our cases make this perfectly clear. It didn't matter in Fonovisa that the infringers there could have continued their illegal sales by mail order or by hawking their unlawful merchandise on street corners. Nor did it matter

12Plaintiff's allegation on this point, as on many others, is very specific:

When MasterCard or Visa learns of a merchant engaged in illegal, fraudulent, or otherwise improper business practices, their own regulations require them to cause member banks to investigate and, depending on the nature of the misconduct, terminate the merchants from the Visa and MasterCard systems. The rules of both associations strictly prohibit members from servicing illegal businesses.

First Am. Compl. at 6 ¶ 20.

13In fact, there can be no doubt that it's true. For example, the MasterCard Merchant Rules Manual provides that "[a] Payment Transaction may not be effected for any of the following reasons: . . . to transfer gambling winnings or funds related to chips, currency, or other value usable for gambling that were purchased in connection with gambling; for any illegal purpose or any other purpose deemed by MasterCard to be impermissible." MasterCard International, Merchant Rules Manual § 2.1.11.3(6) (2006) (emphasis added), available at http://www.mastercard.com/us/en/PDF/12999_MERC-Entire_Manual.pdf.
in Napster or Grokster that the direct infringers might find some other means of illegally sharing their protected content with others. Indeed, there is no case involving secondary infringement, going back to the dance hall cases of the last century, where the secondary infringer’s refusal to do business with the direct infringer could have stopped infringement altogether and forever. Yet, courts have presumed that removing the particular means of infringement challenged in each case would make direct infringement more difficult and thereby diminish the scale of infringing activity.

Here, the Stolen Content Websites have chosen credit cards as a form of payment, and for good reason. Credit cards are ubiquitous and permit the transfer of funds electronically in a matter of seconds. Consumers need not wait days or weeks for a check to reach its destination and clear before gaining access to the salacious pictures they crave. Consumers also know that, if goods bought by credit card are not delivered, the cards will likely reverse the transaction. Credit cards thus act as informal escrow agents, effectively guaranteeing that their merchants will deliver the goods. Blocking the ability to accept credit cards would be a heavy blow to the Stolen Content Websites because cards are “overwhelmingly the primary way by which customers pay to view Stolen Content Websites.” First Am. Compl. at 9 ¶ 35. Even if the pirates could find an alternative way of plying their illegal trade, being denied their preferred means of doing business would sharply curtail their unlawful activities.

4Visa’s website, for example, explains that “Visa and its card issuers and acquirers have in place an efficient dispute resolution process.” Visa USA, Chargebacks & Dispute Resolution, http://www.usa.visa.com/merchants/operations/chargebacks_dispute_resolution/index.html (last visited March 24, 2007). It also notes that “[c]hargebacks arise for many reasons, primary among which are customer disputes, fraud, processing errors, authorization issues, and non-fulfillment of copy requests.” Id. (emphasis added).
The majority toils to resist this obvious conclusion but its arguments are not persuasive. For example, it makes no difference that defendants control only the means of payment, not the mechanics of transferring the material. Maj. op. at 7850, 7856, 7858. In a commercial environment, distribution and payment are (to use a quaint anachronism) like love and marriage—you can't have one without the other. If cards don't process payment, pirates don't deliver booty. The credit cards, in fact, control distribution of the infringing material.

The majority also disparages defendants' ability to control the Stolen Content Websites as just "financial pressure" which doesn't give them an "absolute right to stop [the infringing] activity—they cannot stop websites from reproducing, altering, or distributing infringing images." Id. at 7855 (footnote omitted). But we have never required an "absolute right to stop [the infringing] activity" as a predicate for vicarious liability; it's enough if defendants have the "practical ability" to do so. Amazon, slip op. at 5794, 5796. While proclaiming its fidelity to Amazon, maj. op. at 7841, 7852, the

---

16The majority tries to take back in a footnote what it says in text by claiming that an "absolute right to stop" is not "a prerequisite" to vicarious liability, but that its absence is "evidence that [defendants], much like Google, lack the right and ability to control those [infringing] activities." Maj. op. at 7855 n.16. Alas, it won't work. If not having an "absolute right to stop" is merely "evidence" that defendants lack sufficient control for vicarious infringement, then this can be offset by other evidence that they do have such control. Conflicts in the evidence must be resolved after discovery and trial, not on a motion to dismiss.

"Practical ability," the standard announced in Amazon, is a capacious concept, far broader than "absolute right to stop." Even if the majority were right that defendants lack the "absolute right to stop" the infringements, plaintiff would be entitled to show that defendants have the "practical ability" to do so. If the majority means what it says in its footnote, then what it says in text is beside the point. In fact, there can be no doubt that the majority means what it says in text, because it upholds dismissal of the complaint on the ground that defendants lack the "absolute right to stop" the infringers; the footnote is merely an unpersuasive attempt to sweep the conflict with Amazon under the rug.
majority jettisons Amazon’s “practical ability” standard and substitutes its own “absolute right to stop” standard. Id. at 7855.\textsuperscript{16}

It’s perfectly clear that the cards do have the “practical ability” to force websites that display their logos and use their payment systems to remove unlawful merchandise. As the majority admits, “Defendants can . . . refuse to process credit card payments to the offending merchant within their payment network, or they can threaten to do so if the merchant does not comply with a request to alter content.” Maj. op. at 7855 (disparaging “only” omitted). Commercial websites are dependent on credit cards as a form of payment, and the Stolen Content Websites are uniquely so, as virtually all of their illicit sales are paid for by card. First Am. Compl. at 9 ¶ 35. A threat by credit card companies to withdraw use of their payment systems couldn’t be ignored. After all, how many consumers would be willing to send a check or money order to a far-off jurisdiction in the hope that days or weeks later they will be allowed to download some saucy pictures? If the Stolen Content Websites cannot get paid for their unlawful products, or if payment is made more difficult or cumbersome, this will dramatically affect their operations. Some may lose customers who are unwilling to use alternative forms of payment;\textsuperscript{17} others may go out of business; still others may remove the infringing content from their websites. Even the majority admits that “fear of losing access to credit card payment processing services would be a sufficient incentive for at least some website operators to comply with a content-based suggestion from Defendants.” Maj. op. at 7854-55.\textsuperscript{18} As a consequence, infringing activity would be “stop[ped] or limit[ed].” See Amazon, slip op. at 5794.

\textsuperscript{16}The conflict with Amazon is clearly drawn in footnote 17, where the majority explicitly disavows “practical ability” as the standard for vicarious infringement. Maj. op. at 7856 n.17. The majority is free to disagree with the standard adopted by our caselaw, but it is not free to reject it.

\textsuperscript{17}Those customers may take their patronage to plaintiff’s website.

\textsuperscript{18}The majority disparages this as mere “financial pressure,” but I am aware of no prior case holding that the legal right to exercise “financial
The majority also reads the complaint for less than it's worth by "understand[ing]" plaintiff to allege "that the 'Stolen Content Websites' could not continue to exist as websites offering images for sale online should defendants withdraw their services, not [to allege] that the websites would completely vanish or that infringement by these sites in all its forms would necessarily cease." Maj. op. at 7856-57 n.18. But plaintiff expressly alleges what the majority "understand[s]" it not to allege, namely that the sites "cannot exist" without defendants, First Am. Compl. at 2 ¶ 7, and that "the Stolen Content Websites would be eradicated" if they could not use credit cards, id. at 9-10 ¶ 35. It is hornbook law that we must construe complaints liberally on a motion to dismiss. See Gilus v. Brooklyn Eastern Dist. Terminal, 359 U.S. 231, 235 (1959); Conley v. Gibson, 355 U.S. 41, 47-48 (1957). A liberal construction means reading ambiguous provisions in a way that would save the complaint from dismissal, and sometimes even reading between the lines to give plaintiff the benefit of every reasonable inference. I have never heard of reading a complaint liberally by ignoring allegations that are clearly present.

But let's say the majority "understand[s]" plaintiff's allegations correctly: So what? To sustain a vicarious infringement claim, plaintiff need not allege that the Stolen Content Web-
sites “would completely vanish or that infringement by these sites in all its forms would necessarily cease.” Maj. op. at 7856-57 n.18. The standard is “stop or limit” the infringing conduct. Amazon, slip op. at 5787 (emphasis added) (quoting Grokster, 545 U.S. at 930). And my colleagues admit that plaintiff has alleged that “at least some website operators [would] comply with a content-based suggestion from Defendants.” Maj. op. at 7854-55. Q.E.D.

To resolve this case, however, we need not adopt a rule holding all credit cards responsible for all infringing Internet sales because plaintiff has alleged far more than the ordinary credit card/merchant relationship. According to plaintiff, defendants have adopted special rules and practices that apply only to the Stolen Content Websites, and that are designed to make it easier for these websites to ply their illegal trade. First Am. Compl. at 9-11 ¶¶ 33-37. Plaintiff claims that the credit cards have singled out the Stolen Content Websites for preferential treatment because of the unusual and substantial profits they make on such transactions. Read fully and fairly, the complaint alleges that defendants are not merely passive providers of services available on equal terms to legal and illegal businesses alike; they are actually in cahoots with the pirates to prop up their illegal businesses and share their ill-gotten gains. If this is not vicarious infringement, nothing is.

The majority claims that Amazon employs “reasoning closely analogous” to its own, maj. op. at 7852, but it is mistaken. Amazon addressed two questions of vicarious infringement, one involving third-party websites whose images are picked up by Google’s search engine, the other involving websites that participate in its AdSense program. As to the first, Google could not be vicariously liable because “Perfect 10 ha[d] not shown that Google has contracts with third-party websites that empower Google to stop or limit them from reproducing, displaying, and distributing infringing copies of Perfect 10’s images on the Internet.” Slip op. at 5795. In the

---

19Amazon also relied on the district court’s finding that Google “lacks the practical ability to police the third-party websites’ infringing conduct”
absence of such a contractual relationship, there could be no vicarious infringement, because Google lacked "the legal right to stop or limit the direct infringement of third-party websites." *Id.* at 5794. Why the majority believes this is in any way analogous, or even remotely instructive, to our situation, where the credit cards do have contracts giving them a right to control what merchants sell on their websites, is a mystery.

Google’s relationship with websites that participate in its AdSense program presents a somewhat closer analogy because Google did have contracts that would have allowed it to kick websites out of AdSense for displaying infringing images. But that’s as far as the similarity goes: AdSense is an advertising program; Google pays participating merchants to host third-party ads on their websites. This is the cyberspace analogue of renting out space on your land for a billboard. The ads have no effect on the operation of the host websites; users can download infringing content whether or not ads are present. Being excluded from AdSense would thus mean some loss of revenue, but would have no effect on the operation of the business itself. It is therefore far from certain that merchants would be induced to modify their businesses to avoid being excluded from AdSense.  

---

because the technical means for doing so suggested by plaintiff “were not workable.” *Id.* at 5796 (citing district court’s opinion, 416 F. Supp. 2d at 857-58 & n.25). There is not, and cannot be, such a finding here as the case is presented on a 12(b)(6) motion.

Anecdotal evidence suggests that the AdSense program produces vastly less revenue for most program members than what they earn through their businesses. One poll found that 45% of AdSense members surveyed earned less than $30 per month from the program, and only a small percentage earned a substantial amount. Darren Rowse, *AdSense Earnings for November—Poll Results*, ProBlogger (Dec. 19, 2005), http://www.problogger.net/archives/2005/12/19/adsense-earnings-for-november-poll-results/.
Because plaintiff had not presented proof that any third-party websites would stop infringing if they were threatened with exclusion from AdSense, *Amazon* concluded that plaintiff there had not met its burden for a preliminary injunction. Our case is presented on a motion to dismiss and plaintiff here need only make allegations. And plaintiff alleges that the infringing websites could not continue doing business at all without the use of credit cards. *Amazon*’s reasoning on this point gives the majority no help.

The majority’s attempt to distinguish *Napster* is equally thin. My colleagues argue that “[t]he Napster program’s involvement with . . . the infringement was much more intimate and directly intertwined with it than Defendants’ payment systems are.” Maj. op. at 7853-54. But I don’t see how much more “directly intertwined” you can get in a purchase transaction than carrying the payment from buyer to seller. If this were a drug deal, for example, we would never say that the guy entrusted with delivery of the purchase money is less involved in the transaction than the guy who helps find the seller. Both would be held equally culpable.

Thus, the majority’s insistence that defendants “cannot themselves block access to the Internet, to any particular websites, or to search engines enabling the location of such websites,” maj. op. at 7853, is beside the point. Physical control over the infringing activity is one way to stop infringers, but it’s certainly not the only way. Withdrowing crucial services, such as financial support, can be just as effective, and sometimes more effective, than technical measures that can often be circumvented.21

---

21Providing financial support has long been held to be a basis for vicarious infringement, where that financial support carries with it the contractual right to approve the infringing activity. See *Davis v. E.I. DuPont de Nemours & Co.*, 240 F. Supp. 612 (S.D.N.Y. 1965). In *Davis*, DuPont sponsored a dramatization of “Ethan Frome,” which was alleged to infringe several copyrights. DuPont was held vicariously liable, even though it did not own the studio or the broadcast facilities, and could not have prevented airing of the show with another sponsor.
Finally, the majority dismisses the Supreme Court’s opinion in Grokster by suggesting that the Court could not have meant what it said because the standard it announced (and which we adopted in Amazon) would sweep in too many goods and services that contribute to infringing activity. See maj. op. at 7857 (listing hardware manufacturers, software engineers, technical support companies and utilities). The majority misreads the Court’s opinion. Providing a crucial service to an infringer may give someone the practical ability to stop infringement, but that’s only half of what it takes to be a vicarious infringer. The other half is a right, found in contract, to control the infringer’s actions. See Amazon, slip op. at 5795 (requiring “contracts with [direct infringers] that empower [defendant] to stop or limit them from reproducing, displaying, and distributing infringing copies”). Those third parties the majority worries about could not be held vicariously liable because they lack the legal right to stop the infringement. So far as I know, utilities are provided by public franchise, not by contract, and a utility has no right to stop providing electricity or phone service because it learns that its electrons are being put to illegal use. Computer manufacturers don’t usually retain the right to reclaim computers they have sold because they are being used unlawfully. Ditto for software producers and repairmen. Having no contract that authorizes them to stop providing services on account of illegality, these actors do not meet the first prong of the test for vicarious infringement. See p. 7845 n.10 supra.\(^ {22}\)


\(^ {23}\)The majority is also mistaken when it suggests that parties would be held vicariously liable for infringement simply because, in a market economy, they are free not to deal with one another. Maj. op. at 7856 n.17.
"massive quantities" of infringement possible. First Am. Compl. at 18 ¶ 73.

The case on which the majority relies, Emery v. Visa International Service Association, 95 Cal. App. 4th 952 (2002), is not on point because, in that case, plaintiff sued only Visa, not the merchant banks that had a direct relationship with the alleged wrongdoer or the consumers. Id. at 956, 962. Plaintiff there also based his theory of liability on advertising letters bearing the credit card logo. Emery held that plaintiff hadn't proven Visa could police the use of its logo in letters peddling an illegal lottery sent by merchants directly to consumers. By contrast, plaintiff here alleges that defendants are knowingly participants in thousands of transactions that amount to unfair trade practices and infringe on the right of publicity of the women depicted in the stolen images. I see nothing in Emery that would preclude plaintiff's state law claims, as alleged in the complaint.

* * *

It would certainly be much easier for us if plaintiff were suing the Stolen Content Websites rather than the credit cards. No doubt, they would if they could. But direct infringers are sometimes too ubiquitous, too small or too difficult to find. That's why we have cases such as Fonovisa, Napster, Aimster, Grokster and Amazon. Here, plaintiff alleges that many direct infringers have no physical presence in the United States. They operate from far-off jurisdictions, where lawsuits are difficult to bring and remedies impossible to enforce because the infringers can easily move their operations to servers in other remote jurisdictions.

24In fact, Perfect 10 has brought suit against some direct infringers. See Perfect 10, Inc. v. CCBill, LLC, 481 F.3d 751 (9th Cir. 2007) (reversing summary judgment on direct infringement claim); Perfect 10, Inc. v. Talisman Communications Inc., No. CV99-10450, 2000 WL 364813 (C.D. Cal. Mar. 27, 2000).
The weak link in the pirates' nefarious scheme is their need to get paid; for this they must use the services of legitimate financial institutions. If plaintiff's allegations are to be believed, the financial institutions (defendants here) collect billions for sellers of stolen merchandise; in a very real sense, they profit from making piracy possible. I can see no reason they should not be held responsible.

The majority's refrain that imposing liability on defendants here would violate "the public policy of the United States," maj. op. at 7839, 7844, is equally off base. While the majority correctly identifies that policy as facilitating the development of electronic commerce, id. at 7837 n.2, that solicitude does not extend to commerce in illegal merchandise. I am aware of no policy of the United States to encourage electronic commerce in stolen goods, illegal drugs or child pornography. When it comes to traffic in material that violates the Copyright Act, the policy of the United States is embedded in the FBI warning we see at the start of every lawfully purchased or rented video: Infringers are to be stopped and prosecuted. Preventing financial intermediaries from servicing such shady transactions is entirely consistent with that policy. If Congress believes that this places too heavy a burden on credit cards, it can grant the cards immunity (along with corresponding responsibilities), as it did for ISPs in passing the DMCA.25

The majority's solicitude for "credit cards . . . as the primary engine of electronic commerce," and for preserving "the vibrant and competitive free market that presently exists for the Internet," maj. op. at 7837, is understandable but misguided. It does not serve the interests of a free market, or a

25The majority finds it "anomalous" to hold credit cards liable without DMCA-compliant notice, while ISPs are immune unless they receive such a notice. Maj. op. at 7839 n.4. But there is no anomaly in treating parties that are covered by the statute differently from those that are not. Plaintiff here did give ample notice to the credit cards, see p. 7889 infra, and should not have its claim dismissed for failing to allege compliance with a statute that does not apply to them.
free society, to abet marauders who pilfer the property of law-abiding, tax-paying rights holders, and who turn consumers into recipients of stolen property. Requiring defendants to abide by their own rules, which “strictly prohibit members from servicing illegal businesses,” First Am. Compl. at 6 ¶ 20, will hardly impair the operation of a “vibrant and competitive free market,” any more than did the recent law prohibiting the use of credit cards for Internet gambling. See 31 U.S.C. § 5364.

Nor does plaintiff seek to hold the credit cards responsible for illegal activities of which they are unaware. Plaintiff claims that it has repeatedly written to defendants, “putting them on notice of more than 240 specifically identified Celebrity Porn Websites with obvious stolen content that they were supporting.” First Am. Compl. at 19 ¶ 75. Plaintiff has also sent defendants “[d]eclarations from celebrities [such as Britney Spears, Christina Aguilera, Anna Kournikova and Yasmin Bleeth] stating that they have not authorized the use of their name, likeness, or identity on pornographic websites and that they do not want their images and names so used . . . .” Id. at 19 ¶ 77. Credit cards already have the tools to police the activities of their merchants, which is why we don’t see credit card sales of illegal drugs or child pornography. According to plaintiff, “defendants inspect websites and business premises, and obtain and review merchants’ bank statements, tax returns, credit reports, and a merchant’s other financial information . . . .” Id. at 7 ¶ 26. Plaintiff is not asking for a huge change in the way credit cards do business; they ask only that defendants abide by their own rules and stop doing business with crooks. Granting plaintiff the relief it seeks would not, I am confident, be the end of Capitalism as we know it.

This is an easy case, squarely controlled by our precedent in all material respects. Fairly applying our cases to the facts alleged by Perfect 10, we should reverse the district court and give plaintiff an opportunity to prove its case through discovery and trial. In straining to escape the strictures of our
caselaw, the majority draws a series of ephemeral distinctions that are neither required nor permitted; the opinion will prove to be no end of trouble.
Trademark FAQs

From http://www.uspto.gov/web/offices/tac/tmfaq.htm
(Downloaded August 5, 2007)

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.

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.

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.

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.

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.

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.

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.
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.]

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.

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 Intellectual Property 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.

What are common law rights?

Federal registration is not required to establish rights in a trademark. Common law rights arise from actual use of a mark. Generally, the first to either use a mark in commerce or file an intent to use application with the Patent and Trademark Office has the ultimate right to use and registration. However, there are many benefits of federal trademark registration.
Eric Goldman's Helpful Hints
To Knowing Your Trademark Terms

Likelihood of Confusion

Ninth Circuit "Sleekcraft" Factors (from the Ninth Circuit Model Civil Jury Instructions 18,15)

1. STRENGTH OR WEAKNESS OF THE PLAINTIFF'S MARK. The more the consuming public recognizes the plaintiff's trademark as an indication of origin of the plaintiff's goods, the more likely it is that consumers would be confused about the source of the defendant's goods if the defendant uses a similar mark.

2. DEFENDANT'S USE OF THE MARK. If the defendant and plaintiff use their trademarks on the same, related, or complementary kinds of goods there may be a greater likelihood of confusion about the source of the goods than otherwise.

3. SIMILARITY OF PLAINTIFF'S AND DEFENDANT'S MARKS. If the overall impression created by the plaintiff's trademark in the marketplace is similar to that created by the defendant's trademark in [appearance] [sound] or [meaning], there is a greater chance [that consumers are likely to be confused by defendant's use of a mark] [of likelihood of confusion]. [Similarities in appearance, sound or meaning weigh more heavily than differences in finding the marks are similar].

4. ACTUAL CONFUSION. If use by the defendant of the plaintiff's trademark has led to instances of actual confusion, this strongly suggests a likelihood of confusion. However actual confusion is not required for a finding of likelihood of confusion. Even if actual confusion did not occur, the defendant's use of the trademark may still be likely to cause confusion, you may conclude that the amount of actual confusion was not substantial. As you consider whether the trademark used by the defendant creates for consumers a likelihood of confusion with the plaintiff's trademark, you should weigh any instances of actual confusion against the opportunities for such confusion. If the instances of actual confusion have been relatively frequent, you may find that there has been substantial actual confusion. If, by contrast, there is a very large volume of sales, but only a few isolated instances of actual confusion you may find that there has not been substantial actual confusion.

5. DEFENDANT'S INTENT. Knowing use by defendant of the plaintiff's trademark to identify similar goods may strongly show an intent to derive benefit from the reputation of the plaintiff's mark, suggesting an intent to cause a likelihood of confusion. On the other hand, even in the absence of proof that the defendant acted knowingly, the use of plaintiff's trademark to identify similar goods may indicate a likelihood of confusion.

6. MARKETING/ADVERTISING CHANNELS. If the plaintiff's and defendant's (goods) (services) are likely to be sold in the same or similar stores or outlets, or advertised in similar media, this may increase the likelihood of confusion.

7. PURCHASER'S DEGREE OF CARE. The more sophisticated the potential buyers of the goods or the more costly the goods, the more careful and discriminating the reasonably prudent purchaser exercising ordinary caution may be. They may be less likely to be confused by similarities in the plaintiff's and defendant's trademarks

8. PRODUCT LINE EXPANSION. When the parties' products differ, you may consider how likely the plaintiff is to begin selling the products for which the defendant is using the plaintiff's trademark. If there is a strong possibility of expanding into the other party's market, there is a greater likelihood of confusion.
Dilution

(1) mark is “famous” = “widely recognized by the general consuming public of the United States”
  - advertising/publicity duration/extent/geographic reach
  - amount/volume/geographic extent of sales
  - actual recognition
  - registration?
(2) defendant used in commerce
(3) defendant’s use began after the mark became famous
(4) dilution
  - blurring = impairs distinctiveness (factors: mark similarity; level of distinctiveness; degree of
    exclusivity; level of recognition)
  - tarnishment = harms reputation

Uniform Dispute Resolution Procedure

(1) the domain name is confusing similar (or identical) to a third party’s mark
(2) the registrant has no legitimate interests in the name

But registrant can show legitimate rights by:
  - actual or planned bona fide offering of goods/services;
  - it is commonly known by the domain name; or
  - making a legitimate noncommercial or fair use without intent for commercial gain,
    misleading diversion of traffic, or dilution.

(3) the name is being used in bad faith:
  - acquired the name for profitable resale;
  - registered the name to block the legitimate TM owner if a pattern can be shown;
  - acquired name to disrupt a competitor; or
  - name is intended to attract attention to site by creating a likelihood of confusion.

Anticybersquatting Consumer Protection Act

(1) Domain name registrant registers a domain name containing a third party trademark
(2) has a bad faith intent to profit from the domain name
  - the registrant’s IP rights in the domain name
  - if the domain name contains the registrant’s real name
  - the use of the domain name in a bona fide offering of goods/services
  - a bona fide noncommercial or fair use of the domain name
  - an intent to divert consumers in a way that harms the trademark owner’s goodwill
  - an offer to sell the domain name without having used it for a bona fide offering of
    goods/services
  - providing false contact info
  - multiple bogus registrations
  - distinctiveness/famousness of the mark
(3) registers, traffics in or uses a domain name that is identical or confusingly similar to the mark or,
    in the case of a famous mark, dilutes it.
TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1125

§ 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
(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.

(ii) 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 "traffic 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)

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

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

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

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

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

(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.
One Hundred Ninth Congress  
of the  
United States of America  

AT THE SECOND SESSION  

Began and held at the City of Washington on Tuesday,  
the third day of January, two thousand and six  

An Act  

To amend the Trademark Act of 1946 with respect to dilution by blurring or tarnishment.  

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

SECTION 1. SHORT TITLE.  
(a) SHORT TITLE.—This Act may be cited as the “Trademark Dilution Revision Act of 2006”.  
(b) REFERENCES.—Any reference in this Act to the Trademark Act of 1946 shall be a reference to the Act entitled “An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes”, approved July 5, 1946 (15 U.S.C. 1051 et seq.).  

SEC. 2. DILUTION BY BLURRING; DILUTION BY TARNISHMENT.  
Section 43 of the Trademark Act of 1946 (15 U.S.C. 1125) is amended—  
(1) by striking subsection (c) and inserting the following:  
“(c) DILUTION BY BLURRING; DILUTION BY TARNISHMENT.—  
“(1) INJUNCTIVE RELIEF.—Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner’s mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.  
“(2) DEFINITIONS.—(A) For purposes of paragraph (1), a mark is famous if it is widely recognized by the general consuming public of the United States as a designation of source of the goods or services of the mark’s owner. In determining whether a mark possesses the requisite degree of recognition, the court may consider all relevant factors, including the following:  
“(i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.  
“(ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.  
“(iii) The extent of actual recognition of the mark.
H. R. 683—2

"(v) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1906, or on the principal register.

"(B) For purposes of paragraph (1), 'dilution by blurring' is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. In determining whether a mark or trade name is likely to cause dilution by blurring, the court may consider all relevant factors, including the following:

"(i) The degree of similarity between the mark or trade name and the famous mark.
"(ii) The degree of inherent or acquired distinctiveness of the famous mark.
"(iii) The extent to which the owner of the famous mark is engaging in substantially exclusive use of the mark.
"(iv) The degree of recognition of the famous mark.
"(v) Whether the use of the mark or trade name intended to create an association with the famous mark.
"(vi) Any actual association between the mark or trade name and the famous mark.

"(C) For purposes of paragraph (1), 'dilution by tarnishment' is association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.

"(3) EXCLUSIONS.—The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:

"(A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
"(i) advertising or promotion that permits consumers to compare goods or services; or
"(ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
"(B) All forms of news reporting and news commentary.
"(C) Any noncommercial use of a mark.

"(4) BURDEN OF PROOF.—In a civil action for trade dress dilution under this Act for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that—

"(A) the claimed trade dress, taken as a whole, is not functional and is famous; and
"(B) if the claimed trade dress includes any mark or marks registered on the principal register, the unregistered matter, taken as a whole, is famous separate and apart from any fame of such registered marks.

"(5) ADDITIONAL REMEDIES.—In an action brought under this subsection, the owner of the famous mark shall be entitled to injunctive relief as set forth in section 34. The owner of the famous mark shall also be entitled to the remedies set forth in sections 35(a) and 36, subject to the discretion of the court and the principles of equity if—
"(A) the mark or trade name that is likely to cause dilution by blurring or dilution by tarnishment was first used in commerce by the person against whom the injunction is sought after the date of enactment of the Trademark Dilution Revision Act of 2006; and

"(B) in a claim arising under this subsection—

"(i) by reason of dilution by blurring, the person against whom the injunction is sought willfully intended to trade on the recognition of the famous mark; or

"(ii) by reason of dilution by tarnishment, the person against whom the injunction is sought willfully intended to harm the reputation of the famous mark.

"(6) OWNERSHIP OF VALID REGISTRATION A COMPLETE BAR TO ACTION.—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 under this Act shall be a complete bar to an action against that person, with respect to that mark, that—

"(A)(i) is brought by another person under the common law or a statute of a State; and

"(ii) seeks to prevent dilution by blurring or dilution by tarnishment; or

"(B) asserts any claim of actual or likely damage or harm to the distinctiveness or reputation of a mark, label, or form of advertisement.

"(7) SAVINGS CLAUSE.—Nothing in this subsection shall be construed to impair, modify, or supersede the applicability of the patent laws of the United States.; and

(2) in subsection (d)(1)(B)(i)(IX), by striking "(c)(1) of section 43" and inserting "(c)".

SEC. 2. CONFORMING AMENDMENTS.

(a) MARKS REGISTERABLE ON THE PRINCIPAL REGISTER.—Section 2 of the Trademark Act of 1946 (15 U.S.C. 1052(f)) is amended—

(1) by striking the last two sentences; and

(2) by adding at the end the following:—A mark which would be likely to cause dilution by blurring or dilution by tarnishment under section 43(c), may be refused registration only pursuant to a proceeding brought under section 13. A registration for a mark which would be likely to cause dilution by blurring or dilution by tarnishment under section 43(c) may be canceled pursuant to a proceeding brought under either section 14 or sections.

(b) OPPOSITION.—Section 13(a) of the Trademark Act of 1946 (15 U.S.C. 1063(a)) is amended in the first sentence by striking "as a result of dilution" and inserting “the registration of any mark which would be likely to cause dilution by blurring or dilution by tarnishment".

(c) CANCELLATION.—Section 14 of the Trademark Act of 1946 (15 U.S.C. 1064) is amended, in the matter preceding paragraph (1) by striking "mark", including as a result of dilution under section 43(c), and inserting "mark", including as a result of dilution by blurring or dilution by tarnishment under section 43(c),

(d) MARKS FOR THE SUPPLEMENTAL REGISTER.—The second sentence of section 24 of the Trademark Act of 1946 (15 U.S.C. 1092) is amended to read as follows:—
TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1129
§ 1129. Cyberpiracy protections for individuals

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

(B) Exception
A person who in good faith registers a domain name consisting of the name of another living person, or a name substantially and confusingly similar thereto, shall not be liable under this paragraph if such name is used in, affiliated with, or related to a work of authorship protected under title 17, 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).
TITLE 15 > CHAPTER 22 > SUBCHAPTER III > § 1114
§ 1114. Remedies; infringement; innocent infringement by printers and publishers

How Current is This?

(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.

(3)  

(A) Any person who engages in the conduct described in paragraph (11) of section 110 of title 17 and who complies with the requirements set forth in that paragraph is not liable on account of such conduct for a violation of any right under this chapter. This subparagraph does not preclude liability, nor shall it be construed to restrict the defenses or limitations on rights granted under this chapter, of a person for conduct not described in paragraph (11) of section 110 of title 17, even if that person also engages in conduct described in paragraph (11) of section 110 of such title.

(B) A manufacturer, licensee, or licensor of technology that enables the making of limited portions of audio or video content of a motion picture imperceptible as described in subparagraph (A) is not liable on account of such manufacture or license for a violation of any right under this chapter, if such manufacturer, licensee, or licensor ensures that the technology provides a clear and conspicuous notice at the beginning of each performance that the performance of the motion picture is altered from the performance intended by the director or copyright holder of the motion picture. The limitations on liability in subparagraph (A) and this subparagraph shall not apply to a manufacturer, licensee, or licensor of technology that fails to comply with this paragraph.

(C) The requirement under subparagraph (B) to provide notice shall apply only with respect to technology manufactured after the end of the 180-day period beginning on April 27, 2005.

(D) Any failure by a manufacturer, licensee, or licensor of technology to qualify for the exemption under subparagraphs (A) and (B) shall not be construed to create an inference that any such party that engages in conduct described in paragraph (11) of section 110 of title 17 is liable for trademark infringement by reason of such conduct.

LII has no control over and does not endorse any external Internet site that contains links to or references LII.
Uniform Domain Name Dispute Resolution Policy

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

Notes:

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

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

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

Uniform Domain Name Dispute Resolution Policy
(As Approved by ICANN on October 24, 1999)

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

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

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

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

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

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

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


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. **Transfers During a Dispute.**

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

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

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at 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.
Note: These rules are now in effect. See [www.icann.org/udrp/udrp-schedule.htm](http://www.icann.org/udrp/udrp-schedule.htm) for the implementation schedule.

Rules for Uniform Domain Name Dispute Resolution Policy

(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."

(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.
PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

Christopher Lamparello,
Plaintiff-Appellant,

v.

Jerry Falwell; Jerry Falwell
Ministries,

Defendants-Appellees.

No. 04-2011

American Civil Liberties Union;
ACLU Foundation of Virginia;
Intellectual Property Law
Faculty,

Amici Supporting Appellant.

Christopher Lamparello,
Plaintiff-Appellee,

v.

Jerry Falwell; Jerry Falwell
Ministries,

Defendants-Appellants.

No. 04-2122

American Civil Liberties Union;
ACLU Foundation of Virginia;
Intellectual Property Law
Faculty,

Amici Supporting Appellee.
LAMPARELLO v. FALWELL

OPINION

DIANA GRIBBON MOTZ, Circuit Judge:

Christopher Lamparello appeals the district court’s order enjoining him from maintaining a gripe website critical of Reverend Jerry Falwell. For the reasons stated below, we reverse.

I.

Reverend Falwell is "a nationally known minister who has been active as a commentator on politics and public affairs." *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 47 (1988). He holds the common law trademarks "Jerry Falwell" and "Falwell," and the registered trademark "Listen America with Jerry Falwell." Jerry Falwell Ministries can be found online at "www.falwell.com," a website which receives 9,000 hits (or visits) per day.

Lamparello registered the domain name "www.falwell.com" on February 11, 1999, after hearing Reverend Falwell give an interview "in which he expressed opinions about gay people and homosexuality that [Lamparello] considered ... offensive." Lamparello created a website at that domain name to respond to what he believed were "un-truths about gay people." Lamparello’s website included headlines such as "Bible verses that Dr. Falwell chooses to ignore" and "Jerry Falwell has been bearing false witness (Exodus 20:16) against his gay and lesbian neighbors for a long time." The site also contained in-depth criticism of Reverend Falwell’s views. For example, the website stated:

Dr. Falwell says that he is on the side of truth. He says that he will preach that homosexuality is a sin until the day he dies. But we believe that if the reverend were to take another thoughtful look at the scriptures, he would discover that they have been twisted around to support an anti-gay political agenda ... at the expense of the gospel.

Although the interior pages of Lamparello’s website did not contain a disclaimer, the homepage prominently stated, "This website is NOT
affiliated with Jerry Falwell or his ministry"; advised, "If you would like to visit Rev. Falwell’s website, you may click here"; and provided a hyperlink to Reverend Falwell’s website.

At one point, Lamparello’s website included a link to the Amazon.com webpage for a book that offered interpretations of the Bible that Lamparello favored, but the parties agree that Lamparello has never sold goods or services on his website. The parties also agree that "Lamparello’s domain name and website at www.falwell.com," which received only 200 hits per day, "had no measurable impact on the quantity of visits to [Reverend Falwell’s] website at www.falwell.com."


1As the district court noted, although Reverend Falwell "assert[s] a claim under 15 U.S.C. [§] 1126 for a violation of federal unfair competition law, no such cause of action exists. False Designation of Origin is commonly referred to as unfair competition law . . . ." Lamparello v. Falwell, 360 F. Supp. 2d 768, 773 n.2 (E.D. Va. 2004). Accordingly, the district court "construed any claim by [Falwell] for violation of federal unfair competition law as a claim for violation of 15 U.S.C. [§] 1125." Id. We will do the same. Furthermore, because "[t]he test for trademark infringement and unfair competition under the Lanham Act is essentially the same as that for common law unfair competition under Virginia law because both address the likelihood of confusion as to the source of the goods or services involved," Lone Star Steakhouse & Saloon, Inc. v. Alpha of Va., Inc., 43 F.3d 922, 930 n.10 (4th Cir. 1995), Reverend Falwell’s state-law unfair competition claim rises or falls with his federal claims of infringement and false designation of origin. Therefore, we will not analyze his state-law claim separately.
The parties stipulated to all relevant facts and filed cross-motions for summary judgment. The district court granted summary judgment to Reverend Falwell, enjoined Lamparello from using Reverend Falwell’s mark at www.falwell.com, and required Lamparello to transfer the domain name to Reverend Falwell. Lamparello, 360 F. Supp. 2d at 773, 775. However, the court denied Reverend Falwell’s request for statutory damages or attorney fees, reasoning that the "primary motive" of Lamparello’s website was "to put forth opinions on issues that were contrary to those of [Reverend Falwell]" and "not to take away monies or to profit." Id. at 775.

Lamparello appeals the district court’s order; Reverend Falwell cross-appeals the denial of statutory damages and attorney fees. We review de novo a district court’s ruling on cross-motions for summary judgment. See People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359, 364 (4th Cir. 2001) [hereinafter "PETA"].

II.

We first consider Reverend Falwell’s claims of trademark infringement and false designation of origin.

A.

Section 32 of the Lanham Act creates a cause of action against:

[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.

15 U.S.C. § 1114(1). Similarly, Section 43(a) creates a cause of action against:

[any person who, on or in connection with any goods or services, . . . uses in commerce any word . . . [or] name . . . ,
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.


Both infringement and false designation of origin have five elements. To prevail under either cause of action, the trademark holder must prove:

(1) that it possesses a mark; (2) that the [opposing party] used the mark; (3) that the [opposing party’s] use of the mark occurred "in commerce"; (4) that the [opposing party] used the mark "in connection with the sale, offering for sale, distribution, or advertising" of goods or services; and (5) that the [opposing party] used the mark in a manner likely to confuse consumers.


Trademark law serves the important functions of protecting product identification, providing consumer information, and encouraging the production of quality goods and services. See Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 164 (1995). But protections "against unfair competition" cannot be transformed into "rights to control language." CPC Int'l, Inc. v. Skippy Inc., 214 F.3d 456, 462 (4th Cir. 2000) (quoting Mark A. Lemley, The Modern Lanham Act and the Death of Common Sense, 108 Yale L.J. 1687, 1710-11 (1999)). "Such a transformation" would raise serious First Amendment concerns because it would limit the ability to discuss the products or criticize the conduct of companies that may be of widespread public concern and importance. Much useful social and commercial discourse
would be all but impossible if speakers were under threat of an infringement lawsuit every time they made reference to a person, company or product by using its trademark.

_Id._ (internal quotation marks and citations omitted).

Lamparello and his amici argue at length that application of the Lanham Act must be restricted to "commercial speech" to assure that trademark law does not become a tool for unconstitutional censorship. The Sixth Circuit has endorsed this view, see _Taubman Co. v. Webfeats_, 319 F.3d 770, 774 (6th Cir. 2003), and the Ninth Circuit recently has done so as well, see _Bosley Med. Inst., Inc. v. Kremer_, 403 F.3d 672, 674 (9th Cir. 2005).

In its two most significant recent amendments to the Lanham Act, the Federal Trademark Dilution Act of 1995 ("FTDA") and the Anti-cybersquatting Consumer Protection Act of 1999 ("ACPA"), Congress left little doubt that it did not intend for trademark laws to impinge the First Amendment rights of critics and commentators. The dilution statute applies to only a "commercial use in commerce of a mark," 15 U.S.C. § 1125(c)(1), and explicitly states that the "[n]oncommercial use of a mark" is not actionable. _Id._ § 1125(c)(4). Congress explained that this language was added to "adequately address[ ] legitimate First Amendment concerns," H.R. Rep. No. 104-374, at 4 (1995), _reprinted in_ 1995 U.S.C.C.A.N. 1029, 1031, and "incorporate[d] the concept of 'commercial' speech from the 'commercial speech' doctrine." _Id._ at 8, _reprinted in_ 1995 U.S.C.C.A.N. at 1035; cf. _Lorillard Tobacco Co. v. Reilly_, 533 U.S. 525, 554 (2001) (defining commercial speech as "speech proposing a commercial transaction") (internal quotation marks and citation omitted). Similarly, Congress directed that in determining whether an individual has engaged in cybersquatting, the courts may consider whether the person's use of the mark is a "bona fide noncommercial or fair use." 15 U.S.C. § 1125(d)(1)(B)(i)(IV). The legislature believed this provision necessary to "protect[] the rights of Internet users and the interests of all Americans in free speech and protected uses of trademarked names for such things as parody, comment, criticism, comparative advertising, news reporting, etc." S. Rep. No. 106-140 (1999), 1999 WL 594571, at *8.
In contrast, the trademark infringement and false designation of origin provisions of the Lanham Act (Sections 32 and 43(a), respectively) do not employ the term "noncommercial." They do state, however, that they pertain only to the use of a mark "in connection with the sale, offering for sale, distribution, or advertising of any goods or services," 15 U.S.C. § 1114(1)(a), or "in connection with any goods or services," id. § 1125(a)(1). But courts have been reluctant to define those terms narrowly.\(^2\) Rather, as the Second Circuit has explained, "[t]he term services has been interpreted broadly" and so "[t]he Lanham Act has . . . been applied to defendants furnishing a wide variety of non-commercial public and civic benefits." *United We Stand Am., Inc.* v. *United We Stand, Am. N.Y., Inc.*, 128 F.3d 86, 89-90 (2d Cir. 1997). Similarly, in *PETA* we noted that a website need not actually sell goods or services for the use of a mark in that site’s domain name to constitute a use "in connection with goods or services." *PETA*, 263 F.3d at 365; see also *Taubman Co.*, 319 F.3d at 775 (concluding that website with two links to websites of for-profit entities violated the Lanham Act).

Thus, even if we accepted Lamparello’s contention that Sections 32 and 43(a) of the Lanham Act apply only to commercial speech, we would still face the difficult question of what constitutes such speech under those provisions. In the case at hand, we need not resolve that question or determine whether Sections 32 and 43(a) apply exclusively to commercial speech because Reverend Falwell’s claims of trademark infringement and false designation fail for a more obvious reason. The hallmark of such claims is a likelihood of confusion — and there is no likelihood of confusion here.

**B.**

**I.**

"[T]he use of a competitor’s mark that does not cause confusion as to source is permissible." *Dorr-Oliver, Inc.* v. *Fluid-Quip, Inc.*, 94 F.3d 376, 380 (7th Cir. 1996). Accordingly, Lamparello can only be

\(^2\) Indeed, Lamparello agreed at oral argument that the Lanham Act’s prohibitions on infringement and false designation apply to more than just commercial speech as defined by the Supreme Court.
liable for infringement and false designation if his use of Reverend Falwell's mark would be likely to cause confusion as to the source of the website found at www.fallwell.com. This likelihood-of-confusion test "generally strikes a comfortable balance" between the First Amendment and the rights of markholders. Mattel, Inc. v. MCA Records, Inc., 296 F.3d 894, 900 (9th Cir. 2002).

We have identified seven factors helpful in determining whether a likelihood of confusion exists as to the source of a work, but "not all these factors are always relevant or equally emphasized in each case." Pizzeria Uno Corp. v. Temple, 747 F.2d 1522, 1527 (4th Cir. 1984) (internal quotation marks, citations, and brackets omitted). The factors are: "(a) the strength or distinctiveness of the mark; (b) the similarity of the two marks; (c) the similarity of the goods/services the marks identify; (d) the similarity of the facilities the two parties use in their businesses; (e) the similarity of the advertising used by the two parties; (f) the defendant's intent; (g) actual confusion." Id. (citation omitted).

Reverend Falwell's mark is distinctive, and the domain name of Lamparello's website, www.fallwell.com, closely resembles it. But, although Lamparello and Reverend Falwell employ similar marks online, Lamparello's website looks nothing like Reverend Falwell's; indeed, Lamparello has made no attempt to imitate Reverend Falwell's website. Moreover, Reverend Falwell does not even argue that Lamparello's website constitutes advertising or a facility for business, let alone a facility or advertising similar to that of Reverend Falwell. Furthermore, Lamparello clearly created his website intending only to provide a forum to criticize ideas, not to steal customers.

Most importantly, Reverend Falwell and Lamparello do not offer similar goods or services. Rather they offer opposing ideas and commentary. Reverend Falwell's mark identifies his spiritual and political views; the website at www.fallwell.com criticizes those very views. After even a quick glance at the content of the website at www.fallwell.com, no one seeking Reverend Falwell's guidance would be misled by the domain name — www.fallwell.com — into believing Reverend Falwell authorized the content of that website. No one would believe that Reverend Falwell sponsored a site criticizing himself, his positions, and his interpretations of the Bible. See New
Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302, 308-09 (9th Cir. 1992) (stating that use of a mark to solicit criticism of the markholder implies the markholder is not the sponsor of the use).³

Finally, the fact that people contacted Reverend Falwell's ministry to report that they found the content at www.falwell.com antithetical to Reverend Falwell's views does not illustrate, as Reverend Falwell claims, that the website engendered actual confusion. To the contrary, the anecdotal evidence Reverend Falwell submitted shows that those searching for Reverend Falwell's site and arriving instead at Lamparello's site quickly realized that Reverend Falwell was not the source of the content therein.

For all of these reasons, it is clear that the undisputed record evidences no likelihood of confusion. In fact, Reverend Falwell even conceded at oral argument that those viewing the content of Lamparello’s website probably were unlikely to confuse Reverend Falwell with the source of that material.

2.

Nevertheless, Reverend Falwell argues that he is entitled to prevail under the "initial interest confusion" doctrine. This relatively new and sporadically applied doctrine holds that "the Lanham Act forbids a competitor from luring potential customers away from a producer by initially passing off its goods as those of the producer's, even if confusion as to the source of the goods is dispelled by the time any sales are consummated." Dorr-Oliver, 94 F.3d at 382. According to Reverend Falwell, this doctrine requires us to compare his mark with Lamparello’s website domain name, www.falwell.com, without

³If Lamparello had neither criticized Reverend Falwell by name nor expressly rejected Reverend Falwell’s teachings, but instead simply had quoted Bible passages and offered interpretations of them subtly different from those of Reverend Falwell, this would be a different case. For, while a gripe site, or a website dedicated to criticism of the markholder, will seldom create a likelihood of confusion, a website purporting to be the official site of the markholder and, for example, articulating positions that could plausibly have come from the markholder may well create a likelihood of confusion.
considering the content of Lamparello's website. Reverend Falwell argues that some people who misspell his name may go to www.falwell.com assuming it is his site, thus giving Lamparello an unearned audience — albeit one that quickly disappears when it realizes it has not reached Reverend Falwell's site. This argument fails for two reasons.

First, we have never adopted the initial interest confusion theory; rather, we have followed a very different mode of analysis, requiring courts to determine whether a likelihood of confusion exists by "examining the allegedly infringing use in the context in which it is seen by the ordinary consumer." *Anheuser-Busch, Inc. v. L & L Wings, Inc.*, 962 F.2d 316, 319 (4th Cir. 1992) (emphasis added) (citing cases); see also *What-A-Burger of Va., Inc. v. WHATABURGER, Inc.*, 357 F.3d 441, 450 (4th Cir. 2004).

Contrary to Reverend Falwell's arguments, we did not abandon this approach in *PETA*. Our inquiry in *PETA* was limited to whether Doughney's use of the domain name "www.peta.org" constituted a successful enough parody of People for the Ethical Treatment of Animals that no one was likely to believe www.peta.org was sponsored or endorsed by that organization. For a parody to be successful, it "must convey two simultaneous — and contradictory — messages: that it is the original, but also that it is not the original and is instead a parody." *PETA*, 263 F.3d at 366 (internal quotation marks and citation omitted). Doughney argued that his domain name conveyed the first message (that it was PETA's website) and that the content of his website conveyed the requisite second message (that it was not PETA's site). *Id.* Although "[t]he website's content ma[de] it clear that it [wa]s not related to PETA," *id.*, we concluded that the website's content could not convey the requisite second message because the site's content "[wa]s not conveyed simultaneously with the first message, [i.e., the domain name itself,] as required to be considered a parody." *Id.* at 366. Accordingly, we found the "district court properly rejected Doughney's parody defense." *Id.* at 367.

*PETA* simply outlines the parameters of the parody defense; it does not adopt the initial interest confusion theory or otherwise diminish the necessity of examining context when determining whether a likelihood of confusion exists. Indeed, in *PETA* itself, rather than embrac-
ing a new approach, we reiterated that "[t]o determine whether a likelihood of confusion exists, a court should not consider how closely a fragment of a given use duplicates the trademark, but must instead consider whether the use in its entirety creates a likelihood of confusion." Id. at 366 (internal quotation marks and citation omitted) (emphasis added). When dealing with domain names, this means a court must evaluate an allegedly infringing domain name in conjunction with the content of the website identified by the domain name.  

Moreover, even if we did endorse the initial interest confusion theory, that theory would not assist ReverendFalwell here because it provides no basis for liability in circumstances such as these. The few appellate courts that have followed the Ninth Circuit and imposed liability under this theory for using marks on the Internet have done so only in cases involving a factor utterly absent here — one business's use of another's mark for its own financial gain. See, e.g., PACCAR Inc. v. Telescan Techs., L.L.C., 319 F.3d 243, 253 (6th Cir. 2003); Promatek Indus., Ltd. v. Equitrac Corp., 300 F.3d 808, 812 (7th Cir. 2002); Brookfield Communications, Inc. v. West Coast Ent'n'T Corp., 174 F.3d 1036, 1055-56 (9th Cir. 1999).

Profiting financially from initial interest confusion is thus a key element for imposition of liability under this theory. When an alleged  

Contrary to ReverendFalwell's suggestions, this rule does not change depending on how similar the domain name or title is to the mark. Hence, ReverendFalwell's assertion that he objects only to Lamparello using the domain name www.falwell.com and has no objection to Lamparello posting his criticisms at "www.falwelliswrong.com," or a similar domain name, does not entitle him to a different evaluation rule. Rather it has long been established that even when alleged infringers use the very marks at issue in titles, courts look to the underlying content to determine whether the titles create a likelihood of confusion as to source. See, e.g., Parks v. LaFace Records, 329 F.3d 437, 452-54 (6th Cir. 2003); Mattel, 296 F.3d at 901-02; Westchester Media v. PRL USA Holdings, Inc., 214 F.3d 658, 667-68 (5th Cir. 2000); Rogers v. Grimaldi, 875 F.2d 994, 1000-01 (2d Cir. 1989).

Offline uses of marks found to cause actionable initial interest confusion also have involved financial gain. See Elvis Presley Enters., Inc. v. Capece, 141 F.3d 188, 204 (5th Cir. 1998); Mobil Oil Corp. v. Pegasus
infringer does not compete with the markholder for sales, "some initial confusion will not likely facilitate free riding on the goodwill of another mark, or otherwise harm the user claiming infringement. Where confusion has little or no meaningful effect in the marketplace, it is of little or no consequence in our analysis." Checkpoint Sys., 269 F.3d at 296-97. For this reason, even the Ninth Circuit has stated that a firm is not liable for using another's mark in its domain name if it "could not financially capitalize on [a] misdirected consumer [looking for the markholder's site] even if it so desired." Interstellar Starship Servs., Ltd. v. Epix, Inc., 304 F.3d 936, 946 (9th Cir. 2002).

This critical element — use of another firm's mark to capture the markholder's customers and profits — simply does not exist when the alleged infringer establishes a gripe site that criticizes the markholder. See Hannibal Travis, The Battle For Mindshare: The Emerging Consensus that the First Amendment Protects Corporate Criticism and Parody on the Internet, 10 Va. J.L. & Tech. 3, 85 (Winter 2005) ("The premise of the 'initial interest' confusion cases is that by using the plaintiff's trademark to divert its customers, the defendant is engaging in the old 'bait and switch.' But because . . . Internet users who find [gripe sites] are not sold anything, the mark may be the 'bait,' but there is simply no 'switch.'") (citations omitted).6 Applying

Petroleum Corp., 818 F.2d 254, 260 (2d Cir. 1987). And even those courts recognizing the initial interest confusion theory of liability but finding no actionable initial confusion involved one business's use of another's mark for profit. See, e.g., Savin Corp. v. The Savin Group, 391 F.3d 439, 462 n.13 (2d Cir. 2004); AM Gen. Corp. v. DaimlerChrysler Corp., 311 F.3d 796, 827-28 (7th Cir. 2002); Checkpoint Sys., Inc. v. Check Point Software Techs., Inc., 269 F.3d 270, 298 (3d Cir. 2001); Hasbro, Inc. v. Chue Computing, Inc., 232 F.3d 1, 2 (1st Cir. 2000); Syndicate Sales, Inc. v. Hampshire Paper Corp., 192 F.3d 633, 638 (7th Cir. 1999); Rust Env't & Infrastructure, Inc. v. Temnissen, 131 F.3d 1210, 1217 (7th Cir. 1997); Dorr-Oliver, 94 F.3d at 383.

6 Although the appellate courts that have adopted the initial interest confusion theory have only applied it to profit-seeking uses of another’s mark, the district courts have not so limited the application of the theory. Without expressly referring to this theory, two frequently-discussed district court cases have held that using another’s domain name to post con-
the initial interest confusion theory to gripe sites like Lamparello's would enable the markholder to insulate himself from criticism — or at least to minimize access to it. We have already condemned such uses of the Lanham Act, stating that a markholder cannot "shield itself from criticism by forbidding the use of its name in commentaries critical of its conduct." CPC Int'l, 214 F.3d at 462 (quoting L.L. Bean, Inc. v. Drake Publishers, Inc., 811 F.2d 26, 33 (1st Cir. 1987)). "[J]ust because speech is critical of a corporation and its business practices is not a sufficient reason to enjoin the speech." Id.

In sum, even if we were to accept the initial interest confusion theory, that theory would not apply in the case at hand. Rather, to determine whether a likelihood of confusion exists as to the source of a gripe site like that at issue in this case, a court must look not only to the allegedly infringing domain name, but also to the underlying content of the website. When we do so here, it is clear, as explained above, that no likelihood of confusion exists. Therefore, the district court erred in granting Reverend Falwell summary judgment on his infringement, false designation, and unfair competition claims.

III.

We evaluate Reverend Falwell's cybersquatting claim separately because the elements of a cybersquatting violation differ from those of traditional Lanham Act violations. To prevail on a cybersquatting claim, Reverend Falwell must show that Lamparello: (1) "had a bad

tent antithetical to the markholder constitutes infringement. See Planned Parenthood Fed'n of Am., Inc. v. Bucci, No. 97 Civ. 0629, 1997 WL 133313 (S.D.N.Y. March 24, 1997), aff'd, 152 F.3d 920 (2d Cir. 1998) (table) (finding use of domain name "www.plannedparenthood.com" to provide links to passages of anti-abortion book constituted infringement); Jews for Jesus v. Brodsky, 993 F. Supp. 282 (D.N.J. 1998), aff'd, 159 F.3d 1351 (3d Cir. 1998) (table) (finding use of "www.jewsforjesus.org" to criticize religious group constituted infringement). We think both cases were wrongly decided to the extent that in determining whether the domain names were confusing, the courts did not consider whether the websites' content would dispel any confusion. In expanding the initial interest confusion theory of liability, these cases cut it off from its moorings to the detriment of the First Amendment.
faith intent to profit from using the [www.fallwell.com] domain name," and (2) the domain name www.fallwell.com "is identical or confusingly similar to, or dilutive of, the distinctive and famous [Fallwell] mark." PETA, 263 F.3d at 367 (citing 15 U.S.C. § 1125(d)(1)(A)).

"The paradigmatic harm that the ACPA was enacted to eradicate" is "the practice of cybersquatters registering several hundred domain names in an effort to sell them to the legitimate owners of the mark." Lucas Nursery & Landscaping, Inc. v. Grosse, 359 F.3d 806, 810 (6th Cir. 2004). The Act was also intended to stop the registration of multiple marks with the hope of selling them to the highest bidder, "distinctive marks to defraud consumers" or "to engage in counterfeiting activities," and "well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's site to the cybersquatter's own site, many of which are pornography sites that derive advertising revenue based on the number of visits, or 'hits,' the site receives." S. Rep. No. 106-140, 1999 WL 594571, at *5-6. The Act was not intended to prevent "noncommercial uses of a mark, such as for comment, criticism, parody, news reporting, etc.," and thus they "are beyond the scope" of the ACPA. Id. at *9.

To distinguish abusive domain name registrations from legitimate ones, the ACPA directs courts to consider nine nonexhaustive factors:

(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 the 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.


These factors attempt "to balance the property interests of trademark owners with the legitimate interests of Internet users and others
who seek to make lawful uses of others' marks, including for purposes such as comparative advertising, comment, criticism, parody, news reporting, fair use, etc." H.R. Rep. No. 106-412, 1999 WL 970519, at *10 (emphasis added). "The first four [factors] suggest circumstances that may tend to indicate an absence of bad-faith intent to profit from the goodwill of a mark, and the others suggest circumstances that may tend to indicate that such bad-faith intent exists." Id. However, "[t]here is no simple formula for evaluating and weighing these factors. For example, courts do not simply count up which party has more factors in its favor after the evidence is in." Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214, 234 (4th Cir. 2002).
In fact, because use of these listed factors is permissive, "[w]e need not . . . march through" them all in every case. Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 269 (4th Cir. 2001). "The factors are given to courts as a guide, not as a substitute for careful thinking about whether the conduct at issue is motivated by a bad faith intent to profit." Lucas Nursery & Landscaping, 359 F.3d at 811.


7We note that factor IV does not protect a faux noncommercial site, that is, a noncommercial site created by the registrant for the sole purpose of avoiding liability under the FTDA, which exempts noncommercial uses of marks, see 15 U.S.C. § 1125(c)(4)(B), or under the ACPA. As explained by the Senate Report discussing the ACPA, an individual cannot avoid liability for registering and attempting to sell a hundred domain names incorporating famous marks by posting noncommercial content at those domain names. See S. Rep. No. 106-140, 1999 WL 594571, at *14 (citing Panavision Int'l v. Toeppen, 141 F.3d 1316 (9th Cir. 1998)). But Lamparello's sole purpose for registering www.falwell.com was to criticize Reverend Falwell, and this noncommercial use was not a ruse to avoid liability. Therefore, factor IV indicates that Lamparello did not have a bad faith intent to profit.
a link to an Amazon.com webpage selling a book he favored does not diminish the communicative function of his website. The use of a domain name to engage in criticism or commentary "even where done for profit" does not alone evidence a bad faith intent to profit, H.R. Rep. No. 106-412, 1999 WL 970519, at *11, and Lamparello did not even stand to gain financially from sales of the book at Amazon.com. Thus factor IV weighs heavily in favor of finding Lamparello lacked a bad faith intent to profit from the use of the domain name.

Equally important, Lamparello has not engaged in the type of conduct described in the statutory factors as typifying the bad faith intent to profit essential to a successful cybersquatting claim. First, we have already held, supra Part II.B, that Lamparello's domain name does not create a likelihood of confusion as to source or affiliation. Accordingly, Lamparello has not engaged in the type of conduct — "creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site," 15 U.S.C. § 1125(d)(1)(B)(i)(V) — described as an indicator of a bad faith intent to profit in factor V of the statute.

Factors VI and VIII also counsel against finding a bad faith intent to profit here. Lamparello has made no attempt — or even indicated a willingness — "to transfer, sell, or otherwise assign the domain name to [Reverend Falwell] or any third party for financial gain." 15 U.S.C. § 1125(d)(1)(B)(i)(VI). Similarly, Lamparello has not registered "multiple domain names," 15 U.S.C. § 1125(d)(1)(B)(i)(VIII); rather, the record indicates he has registered only one. Thus, Lamparello's conduct is not of the suspect variety described in factors VI and VIII of the Act.

Notably, the case at hand differs markedly from those in which the courts have found a bad faith intent to profit from domain names used for websites engaged in political commentary or parody. For example, in PETA we found the registrant of www.peta.org engaged in cybersquatting because www.peta.org was one of fifty to sixty domain names Doughney had registered, PETA, 263 F.3d at 362, and because Doughney had evidenced a clear intent to sell www.peta.org to PETA, stating that PETA should try to "settle" with him and 'make him an offer.'" Id. at 368. See also Virtual Works, 238 F.3d at 269-70. Similarly, in Coca-Cola Co. v. Purdy, 382 F.3d 774 (8th Cir. 2004),
the Eighth Circuit found an anti-abortion activist who had registered domain names incorporating famous marks such as "Washington Post" liable for cybersquatting because he had registered almost seventy domain names, had offered to stop using the Washington Post mark if the newspaper published an opinion piece by him on its editorial page, and posted content that created a likelihood of confusion as to whether the famous markholders sponsored the anti-abortion sites and "had[ ] taken positions on hotly contested issues." Id. at 786. In contrast, Lamparello did not register multiple domain names, he did not offer to transfer them for valuable consideration, and he did not create a likelihood of confusion.

Instead, Lamparello, like the plaintiffs in two cases recently decided by the Fifth and Sixth Circuits, created a gripe site. Both courts expressly refused to find that gripe sites located at domain names nearly identical to the marks at issue violated the ACPA. In TMI, Inc. v. Maxwell, 368 F.3d 433, 434-35 (5th Cir. 2004), Joseph Maxwell, a customer of homebuilder TMI, registered the domain name "www.trendmakerhome.com," which differed by only one letter from TMI’s mark, Trendmaker Homes, and its domain name, "www.trendmakerhomes.com." Maxwell used the site to complain about his experience with TMI and to list the name of a contractor whose work pleased him. After his registration expired, Maxwell registered "www.trendmakerhome.info." TMI then sued, alleging cybersquatting. The Fifth Circuit reversed the district court’s finding that Maxwell violated the ACPA, reasoning that his site was noncommercial and designed only "to inform potential customers about a negative experience with the company." Id. at 438-39.

Similarly, in Lucas Nursery & Landscaping, a customer of Lucas Nursery registered the domain name "www.lucasnursery.com" and posted her dissatisfaction with the company’s landscaping services. Because the registrant, Grosse, like Lamparello, registered a single domain name, the Sixth Circuit concluded that her conduct did not constitute that which Congress intended to proscribe — i.e., the registration of multiple domain names. Lucas Nursery & Landscaping, 359 F.3d at 810. Noting that Grosse’s gripe site did not create any confusion as to sponsorship and that she had never attempted to sell the domain name to the markholder, the court found that Grosse’s conduct was not actionable under the ACPA. The court explained: "One
of the ACPA's main objectives is the protection of consumers from slick internet peddlers who trade on the names and reputations of established brands. The practice of informing fellow consumers of one's experience with a particular service provider is surely not inconsistent with this ideal."

Id. at 811.

Like Maxwell and Grosse before him, Lamparello has not evidenced a bad faith intent to profit under the ACPA. To the contrary, he has used www.fallwell.com to engage in the type of "comment[ ] [and] criticism" that Congress specifically stated militates against a finding of bad faith intent to profit. See S. Rep. No. 106-140, 1999 WL 594571, at *14. And he has neither registered multiple domain names nor attempted to transfer www.fallwell.com for valuable consideration. We agree with the Fifth and Sixth Circuits that, given these circumstances, the use of a mark in a domain name for a gripe site criticizing the markholder does not constitute cybersquatting.

IV.

For the foregoing reasons, Lamparello, rather than Reverend Falwell, is entitled to summary judgment on all counts. Accordingly, the judgment of the district court is reversed and the case is remanded for entry of judgment for Lamparello.

REVERSED AND REMANED

*Given our resolution of Lamparello's appeal, Reverend Falwell's cross-appeal with respect to statutory damages and attorney fees is moot.
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 com-
petitor, 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 website. 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 website; the keyword metatags, at least in theory, contain keywords relating to the contents of the website. 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 Brookfield Communications, Inc. v. West Coast Entm't Corp., 174 F.3d 1036, 1045 (9th Cir. 1999).

² The parties agree that Equitrac meant to use the term "Copitrak" as its metatag rather than "Copitrack."
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 "Copitrak" is a registered trademark of Promatek Industries, Ltd., which can be found at www.promatek.com or www.copitrak.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 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 891, 896 (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.
Ty, 237 F.3d at 895. Finally, the court must consider any consequences to the public from denying or granting the injunction. Id. Sitting as a court of equity, the court then weighs all these factors employing a sliding-scale approach. Abbott Labs, 971 F.2d at 12. That is, the more likely the plaintiff’s chance of success on the merits, the less the balance of harms need weigh in its favor. Id. We review the grant of a preliminary injunction for an abuse of discretion, giving great deference to the district court’s weighing of the factors and will reverse only when the district court commits a clear error of fact or law. Ty, 237 F.3d at 896.

A. The District Court Was Correct in Granting the Injunction

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. In order to prevail under the Lanham Act, 15 U.S.C. § 1125(a), Promatek must establish that Copitrak is a protectable trademark and that Equitrac’s use of the term is likely to cause confusion among consumers. See Ty, 237 F.3d at 897. Preregistration of Promatek’s Copitrak trademark is prima facie evidence of the mark’s validity, see Publications Int’l, Ltd. v. Landoll, Inc., 164 F.3d 337, 340 (7th Cir. 1998), which Equitrac does not dispute. Therefore, we turn to the issue of whether consumers would be confused by Equitrac’s use of Copitrak as a metatag.

In assessing the likelihood of consumer confusion, we consider: (1) the similarity between the marks in appearance and suggestion, (2) the similarity of the products, (3) the area and manner of concurrent use of the products, (4) the degree of care likely to be exercised by consumers,
(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 Copitrack 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, "[s]uing 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 of this Court issued on 8/13/02 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,

v.

NETWORK SOLUTIONS, INC., Defendant-Counter-Claimant-Appellee.

No. 97-56734.

United States Court of Appeals,
Ninth Circuit.

Argued and Submitted June 8, 1999.

Filed Oct. 25, 1999

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

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

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

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

TROTT, Circuit Judge:

Plaintiff Lockheed Martin Corp. ("Lockheed") appeals summary judgment in favor of Defendant Network Solutions, Inc. ("NSI") on Lockheed's action for trademark infringement, unfair competition, dilution, and contributory infringement under the Lanham Trademark Act of 1946, 15 U.S.C. §§ 1051-1127 (1994 & Supp. I 1995), as amended (the "Lanham Act"). The district court published its decision granting summary judgment to NSI and refusing to grant Lockheed's motion for leave to amend its complaint. 985 F.Supp. 949 (C.D.Cal.1997). Lockheed contends that (1) genuine issues of material fact remain on its contributory infringement claim, (2) the district court erred in holding that 15 U.S.C. § 1114(2) did not create an independent basis for liability, and (3) the district court should have permitted Lockheed to amend the complaint to add a cause of action for contributory dilution. We have jurisdiction under 28 U.S.C. § 1291 (1994), and we affirm the judgment of the district court.

I

This appeal concerns the NSI registration scheme for domain-name combinations, which we discussed in our recent Avery Dennison Corp. v. Sumpton, 189 F.3d 868 (9th Cir.1999), decision. An interested reader may wish to review the district court's in-depth discussion of the Internet technology that forms the basis of this cause of action. 985 F.Supp. at 951-53.

When a third party seeks to maintain an Internet web site, that party must reserve a location, called an Internet Protocol ("IP") Address, and do the necessary programming. When an Internet user accesses the third party's web site, the user enters the domain-name combination that corresponds to the IP

http://cyber.law.harvard.edu/property00/domain/Lockheed.html 7/29/2007
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

http://cyber.law.harvard.edu/property00/domain/Lockheed.html

7/29/2007
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>, <skunkwork.com>, <skunkwerks.com>, <skunkworx.com>, <theskunkworks.com>, <skunkworks1.com>, <skunkworks.org>, <skunkwear.com>, <the-skunkworks.com>, <skunkwurks.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. Margolis v. Ryan, 140 F.3d 850, 852 (9th Cir. 1998). Viewing the evidence in the light most favorable to the non-moving party, summary judgment is appropriate if no genuine issues of material fact remain and the non-moving party is entitled to judgment as a matter of law. See id. We review for an abuse of discretion the district court's decision denying a motion to amend a complaint. Griggs v. Pace Am. Group, Inc., 170 F.3d 877, 879 (9th Cir. 1999).

IV

Contributory infringement occurs when the defendant either intentionally induces a third party to infringe the plaintiff's mark or supplies a product to a third party with actual or constructive knowledge that the product is being used to infringe the service mark. Inwood Lab., Inc. v. Ives Lab., Inc., 456 U.S. 844, 853-54, 102 S.Ct. 2182, 72 L.Ed.2d 606 (1982). Lockheed alleges only the latter basis for contributory infringement liability and therefore must prove that NSI supplies a product to third parties with actual or constructive knowledge that its product is being used to infringe "Skunk Works." Id. at 854, 102 S.Ct. 2182.

The district court assumed for purposes of summary judgment that third parties were infringing Lockheed's "Skunk Works" service mark, and NSI does not ask us to affirm on the alternate ground that no genuine issue of material fact exists as to infringement. We are thus left to consider two issues on
Lockheed's contributory infringement cause of action: (1) whether NSI supplied a product to third parties and (2) whether NSI had actual or constructive knowledge of any infringement. Because we accept the district court's excellent analysis on the first question, see 985 F.Supp. at 960-32, we affirm summary judgment without reaching the second.

A

Under the plain language of the Inwood Lab. formulation, to be liable for contributory infringement, NSI must supply a "product" to a third party with which the third party infringes Lockheed's service mark. 456 U.S. at 854, 102 S.Ct. 2182. In Inwood Lab., the Supreme Court considered an action against a manufacturer of generic pharmaceuticals. Id. at 847, 102 S.Ct. 2182. Non-party pharmacists packaged the defendant's less-expensive generic pills, but labeled them with the plaintiff's brand name. Id. at 850, 102 S.Ct. 2182. The plaintiff stated a cause of action for contributory infringement by alleging that the defendant "continued to supply [the product] to pharmacists whom the petitioners knew were mislabeling generic drugs." Id. at 855, 102 S.Ct. 2182.

Inwood Lab. has been applied in the broader context of renting booth space at a flea market. See Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148-49 (7th Cir.1992). In Hard Rock, the Seventh Circuit explicitly addressed the distinction between a product and a service, noting that while the pharmaceutical company in Inwood Lab. clearly supplied a product to the third-party pharmacists, a "temporary help service ... might not be liable if it furnished [to the defendant] the workers he employed to erect his stand." Hard Rock, 955 F.2d at 1148. The court then held that space at a flea market was more comparable to pharmaceuticals than to manpower, in part because of the close comparison between the legal duty owed by a landlord to control illegal activities on his or her premises and by a manufacturer to control illegal use of his or her product. Id. at 1149. We adopted the Hard Rock analysis in Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir.1996), holding that a flea market could be liable for contributory infringement if it "suppl[ied] the necessary marketplace" for the sale of infringing products. Id. at 265 (citing Hard Rock, 955 F.2d at 1149).

Hard Rock and Fonovisa teach us that when measuring and weighing a fact pattern in the contributory infringement context without the convenient "product" mold dealt with in Inwood Lab., we consider the extent of control exercised by the defendant over the third party's means of infringement. Hard Rock, 955 F.2d at 1148-49 (noting the common-law responsibilities of a landlord regarding illegal activity on a rented premises); see Fonovisa, 76 F.3d at 265 (adopting Hard Rock's analysis). Direct control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark permits the expansion of Inwood Lab.'s "supplies a product" requirement for contributory infringement.

B

The case at bench involves a fact pattern squarely on the "service" side of the product/service distinction suggested by Inwood Lab and its offspring. All evidence in the record indicates that NSI's role differs little from that of the United States Postal Service: when an Internet user enters a domain-name combination, NSI translates the domain-name combination to the registrant's IP Address and routes the information or command to the corresponding computer. Although NSI's routing service is only available to a registrant who has paid NSI's fee, NSI does not supply the domain-name combination any more than the Postal Service supplies a street address by performing the routine service of routing mail. As the district court correctly observed, Where domain names are used to infringe, the infringement does not result from NSI's publication of the domain name list, but from the registrant's use of the name on a 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.

http://cyber.law.harvard.edu/property00/domain/Lockheed.html 7/29/2007
The "direct control and monitoring" rule established by Hard Rock and Fonovisa likewise fails to reach the instant situation. The district court correctly recognized that NSI's rote translation service does not entail the kind of direct control and monitoring required to justify an extension of the "supplies a product" requirement. See 985 F.Supp. at 962 ("While the landlord of a flea market might reasonably be expected to monitor the merchandise sold on his premises, NSI cannot reasonably be expected to monitor the Internet."). Such a stretch would reach well beyond the contemplation of Inwood Lab. and its progeny.

In an attempt to fit under Fonovisa's umbrella, Lockheed characterizes NSI's service as a licensing arrangement with alleged third-party infringers. Although we accept Lockheed's argument that NSI licenses its routing service to domain-name registrants, the routing service is just that—a service. In Fonovisa and Hard Rock, by contrast, the defendants licensed real estate, with the consequent direct control over the activity that the third-party alleged infringers engaged in on the premises. Hard Rock, 955 F.2d at 1149; see Fonovisa, 76 F.3d at 265.

Lockheed also urges that NSI is liable as a printer or publisher under 15 U.S.C. § 1114(2) (1994), which reads in pertinent part:

[The remedies given to the owner of a right infringed under this chapter or to a person bringing an action under section 1125(a) of this title shall be limited as follows:

(A) Where an infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer or innocent violator, the [plaintiff] shall be entitled as against such infringer or violator only to an injunction against future printing.

(B) Where the infringement or violation complained of is contained in ... an electronic communication ..., the remedies ... shall be limited to an injunction against the presentation ... in future transmissions of such electronic communications.

Id. Section 1114(2) does not create an independent cause of action, but limits the remedies available to a plaintiff from an innocent infringer, requiring infringement of a trademark right or success on an unfair competition claim for injunctive relief. Barrios v. American Thermal Instruments, Inc., 712 F.Supp. 611, 620 (S.D.Ohio 1988) ("It is important to note that § 1114(2)(a) ... does not relate to the potential liability of a printer. Instead, this statute limits the relief which a Court may grant against a printer to an injunction against future printing."); see 3 J. Thomas McCarthy, Trademarks & Unfair Competition, § 25:29 (Supp.1998) ("The Lanham Act, as amended effective in 1989, limits the liability of innocent infringement..."). Because Lockheed does not appeal summary judgment for NSI on Lockheed's claims of service mark infringement and unfair competition, Lockheed cannot establish the necessary predicate for its § 1114(2) argument on appeal.

VI

Finally, Lockheed argues that the district court abused its discretion in failing to grant leave to amend its complaint to (1) add a contributory dilution cause of action and (2) include allegations of several other offending domain-name combinations. As a general rule, leave to amend should be "freely given when justice so requires." Fed.R.Civ.P. 15(a); Foman v. Davis, 371 U.S. 178, 83 S.Ct. 227, 9 L.Ed.2d 222 (1962). We consider four factors when reviewing a decision whether to permit an amendment: (1) bad faith on the part of the plaintiffs; (2) undue delay; (3) prejudice to the opposing party; and (4) futility of the proposed amendment. Griggs, 170 F.3d at 877.

Although delay is not a dispositive factor in the amendment analysis, it is relevant, Morongo Band of Mission Indians v. Rose, 893 F.2d 1074, 1079 (9th Cir.1990), especially when no reason is given for the
Prima Facie TM Infringement Case

- Ownership of valid trademark
- Priority
- Use in commerce in connection with sale of goods/services
- Likelihood of consumer confusion

Use in Commerce

- Reading #1: Use in “commerce” = “all commerce which may lawfully be regulated by Congress” (15 U.S.C. §1127)
  - Ex: SMJ Group v. 417 Lafayette Restaurant, 439 F. Supp. 2d 281 (S.D.N.Y. 2006) (gripper’s service was distributing educational literature)

- Reading #2: “Use in commerce” = “bona fide use of a mark in the ordinary course of trade” (15 U.S.C. §1127)
  - Non-commercial actors don’t make "trade" usage
  - Requires trademark use to be perceivable by consumers

- THE STATUTE IS FACIALLY AMBIGUOUS
### Keyword Triggering = Use in Commerce?

<table>
<thead>
<tr>
<th>Advertisers</th>
<th>Adware Vendors</th>
<th>Search Engines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Silo Poo-1 v. Better Metal, 06-CV-6508 (E.D.N.Y. May 3, 2007)</td>
<td></td>
</tr>
</tbody>
</table>
|             | 1-800 Contacts v. WheeL, 414 F.3d 400 (2d Cir. 2005) | - Brookfield: "use of another’s trademark in a manner reasonably calculated to capture initial consumer attention, even though no actual sale is finally completed as a result of the confusion"
|             | | - Harm paradigms
|             | |   - Sponsorship confusion (2d Cir.)
|             | |   - Attention diversion (Brookfield)
|             | |   - Deceptive diversion (7th Cir.)
|             | |   - Competitive diversion (9th Cir., 3rd Cir.)
|             | |   - Don't recognize IIC at all (1st Cir., 4th Cir.)?
|             | | Confusion generally isn't amenable to SJ
|             | | - But J.G. Wentworth case

### Likelihood of Consumer Confusion

- Multi-factor tests are generally unpredictable...
- ...especially when they don't fit
  - When defendants aren't in business at all
  - When defendant intermediaries are in totally different business
    - Contributory infringement is more appropriate
- Bypass: "Initial interest confusion"
  - Brookfield: "use of another’s trademark in a manner reasonably calculated to capture initial consumer attention, even though no actual sale is finally completed as a result of the confusion"
    - Harm paradigms
      - Sponsorship confusion (2d Cir.)
      - Attention diversion (Brookfield)
      - Deceptive diversion (7th Cir.)
      - Competitive diversion (9th Cir., 3rd Cir.)
      - Don't recognize IIC at all (1st Cir., 4th Cir.)?
- Confusion generally isn't amenable to SJ
  - But J.G. Wentworth case
Infringement Defenses

- Nominative use
  - Not readily identifiable without TM reference
  - Took only what was necessary
  - No implied sponsorship/endorsement

- Descriptive fair use (15 U.S.C. §1115(b)(4))


- Imperfections of defenses
  - Defense bears burden
  - Fair use doctrines are narrow
  - Nominative use doctrine not universally recognized
  - Parody/comparative ad doctrines inadequate and incomplete

State Anti-KeyWord Laws

- Utah/Alaska prohibit using adware to display TM-triggered pop-up ads... but moot?
  - Utah Spyware Control Act (13-40-102 to 13-40-301) requires TM infringement
  - Alaska SB 140: consumers can consent to pop-up ad delivery

- Utah SB 236 (the “Trademark Protection Act,” March 19, 2007)
  - “Electronic Registration Mark” = “word, term, or name that represents a business, goods, or a service”
  - Infringement to use an ERM “to cause the delivery or display of an advertisement for a business, goods, or a service (i) of the same class (other than the ERM registrant’s business); or (ii) if that advertisement is likely to cause confusion between the two businesses)” if ad displayed in Utah or advertiser/keyword vendor located in Utah

- Legal challenges
  - Dormant Commerce Clause
  - First Amendment
  - Conflict preemption?
  - 47 USC 230 (Perfect 10 v. CCBill, 2007 WL 925727 (9th Cir. March 23, 2007))
Tips for TM Owners

- Use search engines' TM complaint policies
  - Yahoo and MSN allow TM owners to block some competitive keyword buys
  - Google allows TM owners to block TM references in ad copy

- Don’t be duplicitious
  - Ex: Humble Abode settlement

- Be rational (invest litigation $ wisely)
  - Cost of keyword litigation > value of “diverted” consumer
  - In 800-JR Cigar, search engine had gross revenues of $345

An Academic’s Observations

- Courts need to get their facts straight
  - Keyword mislabeling
  - Breda et al v. Blockbuster, 106 F.3d 1553 (10th Cir. 1997); Blockbusters, Inc v. Blockbuster, 126 F.3d 1561 (11th Cir. 2009)
  - Differences in ad copy

- We need to clarify how keyword triggering creates harm
  - The initial intent confusion doctrine hurts the discount
    - Courts can define it
    - Defendants can’t defend against it
    - Complete lack of social science support
    - Harmonize online/offline paradigms
    - Does TM law protect consumers or producers?

- Keywords efficiently help consumers express their preferences
  - Searching for “TM” doesn’t mean consumers want TM
  - Regulating keywords reduces intermediaries’ ability to cater to searcher preferences
  - Misapplied, trademark law can counterproductively increase consumer search costs

- We should deregulate keywords
  - Commercial effortful uses ≠ use in commerce
  - Invisible triggering ≠ use in commerce
  - Extend 15 U.S.C. §1114(2)(D)(III) to search engines
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.” 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.²

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 uncontroverted 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 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 otherwise, specific facts showing that there is a genuine issue for trial." We may not weigh the evidence

---

5Lopez v. Smith, 203 F.3d 1122, 1131 (9th Cir. 2000).
6Id.
8Id. (quoting Fed. R. Civ. P. 56(e)).
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. 9


10 Brookfield 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 without PEI's permission.

[2] PEI's strongest argument for a likelihood of confusion is for a certain kind of confusion: initial interest confusion. Initial interest confusion is customer confusion that creates initial interest in a competitor's product. Although dispelled before an actual sale occurs, initial interest confusion impermissibly capitalizes on the goodwill associated with a mark and is therefore actionable trademark infringement.

[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. In addition, many of the advertisements instruct users to "click

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.


13 Indeed, we find insufficient evidence to defeat summary judgment on any other theory.

14 Brookfield, 174 F.3d at 1062-63.

15 Id. at 1057.

16 Note that if a banner advertisement clearly identified its source or, even better, overtly competed 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 cite. 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 "movieth.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 'movieth.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.
[4] 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.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.

[5] The Ninth Circuit employs an eight-factor test, 'originally set forth in AMF Inc. v. Sleekcraft Boats,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;

23 Id. at 1062-65.
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.²⁵

In the Internet context, courts must be flexible in applying the factors, as some may not apply.²⁶ 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.²⁷ 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

²⁵Id.

²⁶Brookfield, 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.

²⁷Thane 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.
[6] 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

38Thane, 305 F.3d at 902.

39Sleekcraft, 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").

32Indeed, 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).

33Defendants 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.


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. **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. **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{\textit{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. **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.39 Accordingly, we turn to defendants’ other asserted defenses.

[9] Defendants assert that they make a nominative use of PEI’s marks. We apply a slightly different test for confusion in the nominative use, as opposed to the fair use, context.40 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.

41 *New Kids on the Block*, 971 F.2d at 308 (footnote omitted).

42 *See, 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).

43 Doing so might eliminate the likelihood of initial interest confusion that exists in this case.
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. Defendants do not wish to identify PEI or its products when they key banner advertisements to PEI’s marks. 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.

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. We do not have such a case here.

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

---

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).

45 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.\(^{47}\)

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.

[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.

B. Trademark Dilution

We reverse the district court's grant of summary judgment on PEI's second cause of action, trademark dilution,\(^{48}\) 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.\(^{49}\) We will address each of the three disputed elements in turn.

\(^{47}\) Qualitex, 514 U.S. at 169-70.

\(^{48}\) 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. Sumption, 189 F.3d 868, 874 (9th Cir. 1999). Accordingly, we do not separately address state law claims.

\(^{49}\) 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.
JOSEPH F. BIANCO, District Judge:

Plaintiff FragranceNet.com seeks leave to file a Third Amended Complaint pursuant to Fed. R. Civ. P. 15(a) to add state and federal claims based on FragranceX.com, Inc.'s ("defendant") alleged misuse of plaintiff's trademark (1) as a keyword to prompt defendant's appearance as a sponsored link in Google's search engine and (2) by inclusion of plaintiff's trademark in defendant's website metatags. Defendant opposes the amendment on futility grounds, arguing that the allegations cannot survive a Federal Rule of Civil Procedure 12(b)(6) motion to dismiss. For the reasons that follow, plaintiff's motion to amend the complaint is denied as futile.

Federal Rule of Civil Procedure 15(a) allows a party to amend its pleadings by leave of the court, and further directs that "leave shall be freely given when justice so requires." Fed. R. Civ. P. 15(a). Indeed, "it is within the sound discretion of the district court to grant or deny leave to amend." McCarthy v. Dun & Bradstreet Corp., 482 F.3d 184, 200 (2d Cir. 2007). Absent "undue delay, bad faith, or dilatory motive on the part of movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of amendment, etc. -- the leave sought should, as the rules require, be "freely given."": Foman v. Davis, 371 U.S. 178, 182 (1962); see also McCarthy, 482 F.3d
II. DISCUSSION

Plaintiff’s Proposed Third Amended Complaint alleges new claims for (1) federal trademark infringement pursuant to 15 U.S.C. § 1125(a) (Count II), (2) trademark dilution pursuant to 15 U.S.C. § 1125(c)(1) (Count III), (3) passing off pursuant to 15 U.S.C. § 1125(a) (Count IV), (4) common law trademark infringement (Count V), (5) violations of N.Y. Gen. Bus. Law § 343 (Count VI), (6) state law dilution in violation of N.Y. Gen. Bus. § 360-1 (Count VII), (7) injury to business reputation (Count VIII), (8) common law unfair competition and misappropriation (Count IX), (9) common law passing off (Count X), and (10) unjust enrichment (Count XI). Each of these claims arises from the alleged use of plaintiff’s trademark by defendant as a keyword in search engines that triggers a “Sponsored Link” and as a website metatag. Defendant

1 A claim of injury to business reputation and a claim of dilution are essentially equivalent – both constitute violations of N.Y. Gen. Bus. Law § 360-1 and require the same elements of proof. See N.Y. Gen. Bus. Law § 360-1 (2007); Savin Corp. v. Savin Group, 391 F.3d 439, 455 (2d Cir. 2004).

2 A “Sponsored Link” is a form of advertising whereby a company bids on a keyword in order to trigger the appearance of that company’s website next to the search results screen that appears based on a search of that keyword. (Proposed Third Am. Compl. ¶ 24.) See also Merck & Co., 425 F. Supp. 2d 402, 408 (S.D.N.Y. 2006) (“Google, Yahoo, and others ‘sell advertising linked to search terms, so that when a consumer enters a particular search term, the results page displays not only a list of Websites generated by the search engine program using neutral and objective criteria, but also links to Websites of paid
asserts that courts within the Second Circuit do not recognize Lanham Act "use" based on such allegations. Plaintiff concedes that, though most courts in other circuits allow a trademark infringement claim based on such use, district courts in this Circuit have not allowed these types of trademark infringement claims to go forward. Plaintiff contends, however, that the courts in this Circuit that have decided this issue were wrong or that such cases are factually distinguishable. (Pl.'s Mem at 8) As discussed below, the Court disagrees with plaintiff and finds that such allegations cannot support claims sounding in the law of trademark infringement or unfair competition.


---

3 Metatags are codes, invisible to the average user, that are used to provide Internet search engines with information about the content of a website which then provides the basis for ranking and displaying the web site in the results of a search that is conducted for a word or term contained in a metatag. (Proposed Third Am. Compl. ¶ 23.)

⁴ Contrary to plaintiff’s assertion, the “use” requirement applies to all of plaintiff’s claims, including the claims asserted under New York law. As stated above, “[t]he standard for trademark infringement under the Lanham Act is similar to the standard for analogous state law claims.” Merck & Co., 425 F. Supp. 2d at 410 n.6 (S.D.N.Y. 2006). Although the Second Circuit has cautioned that “it is not clear that [N.Y. Gen. Bus. Law § 360-1] is coextensive with [the Trademark Dilution Revision Act of 2006],” the “use” requirement exists for plaintiff’s proposed state law claims and is analyzed in the same manner as under the federal claims. Starbucks Corp. v. Wolfe’s Borough Coffee, 477 F.3d 765, 766 (2d Cir. 2007) (per curiam). Specifically, though N.Y. Gen. Bus. § 360-1 does not explicitly state “use in commerce,” that statute requires infringement of a mark to receive injunctive relief for injury to business reputation or dilution. See N.Y. Gen. Bus. Law § 360-1 (“Likelihood of injury to business reputation or of dilution of the distinctive quality of a mark or trade name shall be a ground for injunctive relief in cases of infringement of a mark.”). Infringement of a mark under state law requires use of the trademark, and the definition of “use” under N.Y. Gen. Bus. Law § 360 mirrors the definition of “use” in the Lanham Act. Compare N.Y. Gen. Bus. Law § 360(h) with 15 U.S.C. § 1127; see also Beverage

In 1-800 Contacts, Inc. v. WhenU.com, the Second Circuit addressed whether 1-800 Contacts, Inc.’s (“1-800”) trademark was infringed in violation of the Lanham Act, where defendant caused pop-up ads of 1-800’s competitors to appear on the desktops of computer users who downloaded defendant’s software, when those computer users accessed 1-800’s website. 414 F.3d at 401. The Court reversed the district court’s entry of a preliminary injunction and remanded for dismissal of plaintiff’s trademark infringement claim, holding that plaintiff could not establish that its trademarks were “used” within the meaning of the Lanham Act. Id. at 403. In 1-800 Contacts, defendant had placed 1-800’s website address, not its trademark, in the directory that triggered the delivery of pop-up ads when a user accessed 1-800’s website. Id. at 404. The Second Circuit recognized that “in order for [defendant] to capitalize on the fame and recognition of 1-800’s trademark—the improper motive both 1-800 and the district

Mktg. USA v. S. Beach Bev. Co., 799 N.Y.S.2d 242, 244 (N.Y. App. Div. 2005) (“A party asserting a claim for unfair competition predicated upon trademark infringement or dilution in violation of General Business Law §§ 360-k and 360-l must show that the defendant’s use of the trademark is likely to cause confusion or mistake about the source of the allegedly infringing product.”). In addition, N.Y. Gen. Bus. Law § 133 explicitly requires use. See N.Y. Gen. Bus. Law § 133 (“No person, firm, or corporation shall, with intent to deceive or mislead the public, assume, adopt or use.”). Accordingly, because each of plaintiff’s claims are premised on the alleged use of plaintiff’s mark, all of plaintiff’s state claims relating to defendant’s alleged use of plaintiff’s mark in keywords and metatags are examined under the same analysis applied under the Lanham Act and, thus, are similarly futile for the reasons discussed infra.
court ascribed to [defendant] -- [defendant] would have needed to put the actual trademark on the [directory] list." *Id.* at 409. However, the Court noted, "[t]his observation ... 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." *Id.* at 409 n.11.

However, in addressing 1-800's argument that the pop-up ads were likely to confuse computer users, the Court concluded:

*[T]his 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.*

*Id.* at 412. The Court then explained:

>A company's internal utilization of a trademark in a way that does not communicate it to the public is analogous to an 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.

*Id.* at 409. The Lanham Act provides that, in connection with goods, a trademark is "used in commerce" when the trademark "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." 15 U.S.C. § 1127(1). In connection with services, a trademark is "used in commerce" when the trademark "is used or displayed in the sale or advertising of services and the services rendered in commerce." 15 U.S.C. § 1127(2). Thus, "[t]rademark use . . . is[] one indicating source or origin." *Pirone*, 894 F.2d at 583.

Though plaintiff is correct that 1-800 *Contacts* addressed Lanham Act "use" in a factual scenario different from the facts of the instant case, the reasoning of 1-800 *Contacts* supports a conclusion that no Lanham Act "use" exists for the use of a trademark in a keyword or metatag. *6* It would be inconsistent

---

*5* The Court also distinguished the use of pop-up ads from the Ninth Circuit's decisions in *Brookfield Commc'ns*, Inc. v. W. Coast Entm't Corp., 174 F.3d 1036 (9th Cir. 1999), where the court held that defendant's use of a trademark in metatags constituted a "use in commerce" under the Lanham Act, and *Playboy Enters., Inc. v. Netscape Commc'n Corp.*, 354 F.3d 1020, 1024 (9th Cir. 2004), where the court held that an infringement claim could be based on defendant's insertion of unidentified banner ads on Internet user's search-results pages. *Id.* at 411. However, the Second Circuit noted, "in distinguishing cases such as *Brookfield*, [and] *Playboy*, we do not necessarily endorse their holdings." 1-800 *Contacts*, 414 F.3d at 411 n.15.

*6* As recognized by plaintiff, in 1-800 *Contacts*, the Court took great care to distinguish its facts from cases in other circuits that addressed Lanham Act use in the context of keywords and metatags, but the Court specifically declined to address whether such keyword and metatag use would constitute Lanham Act use.
with the reasoning set forth in *I-800 Contacts* to conclude that the use of trademarks in keywords and metags constitutes Lanham Act "use" where, as here, defendant does not place the trademark on any product, good or service nor is it used in any way that would indicate source or origin. Here, the use of plaintiff’s trademark is strictly internal and, because such use is not communicated to the public, the use does not indicate source or origin of the mark.

In plaintiff’s reply papers and at oral argument, plaintiff emphasized that this case should be analyzed under a theory of "passing off" and that the district courts within the Second Circuit that have addressed the issue have overlooked this theory. Passing off, which is also referred to as "palming off," is a situation in which "A" sells its product under "B's name." *Waldman Pub'g Corp.*

---

7 *See also 4 McCarthy on Trademarks and Unfair Competition § 25:3 (4th Edition) which describes "palming off" as follows:

A kind of conduct properly designated "palming off" is a seller knowingly substituting brand A in response to a request or order for brand B. Such "substitution" has often been characterized as "palming off."

***

Such substitution can be achieved by merely sending one product in response to an order for another, or can be achieved by placing a confusingly similar trademark on the substitution, or by other methods which misrepresent source to the buyer. Such direct "substitution" is illustrated in the many COCA-COLA cases where a restaurant’s substitution of another product in response to a request for COKE or COCA-COLA has been labeled palming off, passing off or substitution. Similarly, the re-filling of genuine COCA-COLA bottles with a non-genuine cola-like beverage is another form of passing off.

(internal footnotes omitted).
individual being handed a non-Coca-Cola product under the guise that it is Coca-Cola; rather, the individual is simply being shown alternatives. Thus, no goods are being sold under “false pretenses.” See DaimlerChrysler AG v. Bloom, 315 F.3d 932, 937 (8th Cir. 2003) (“[T]he primary flaw in [plaintiff’s] argument is that it never identifies any good or service that [defendant] sold under false pretenses. As such, [plaintiff] cannot prevail on a passing off claim, even if asserted.”).

In fact, the Court finds that the situation presented in the instant case is even further removed from a “passing off” situation than the menu of choices example. In Sporty’s Farm L.L.C. v. Sportsman’s Mkt., Inc., 202 F.3d 489, 493 (2d Cir. 2000), the Second Circuit explained:

For consumers to buy things or gather information on the Internet, they need an easy way to find particular companies or brand names. The most common method of locating an unknown domain name is simply to type in the company name or logo with the suffix .com. If this proves unsuccessful, then Internet users turn to a device called a search engine. 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 user must sort in order to find what he or she is looking for. As a result, companies strongly prefer that their domain name be comprised of the company or brand trademark and the suffix .com.

(internal footnotes omitted). The menu of choices example refers more closely to a situation in which an internet user types FragranceNet.com into the web address space and, rather than being immediately taken to FragranceNet.com, is presented with a list of choices. This is not the allegation in the instant case. Here, plaintiff alleges that a search of plaintiff’s mark using a search engine produces a list of choices. Thus, the “Sponsored link” is not triggered by typing FragranceNet.com into the web address line, but rather is only triggered when the user performs a keyword search in the search engine. Though, as the Second Circuit noted, “there are many people who use a search engine before typing in a company plus .com,” Sporty’s Farm LLC, 202 F.3d at 493 n.4, this does not mean that companies must be prohibited from internally using trademarks so that a search of a trademark in a search engine only produces a single result. In the world outside the Internet, individuals in search of a company or product are not blinded to competitive products. In other words, it is not unlawful to strategically place billboards or even store locations next to billboards or store locations of competitors. For example, an individual in search of a McDonald’s restaurant will often be confronted with a Burger King restaurant. As long as Burger King did not mislead the consumer under false pretenses to its location, the mere fact that it decided to place itself in close proximity to a McDonald’s, in an effort to potentially draw customers in search of fast food, is not “passing off.” When these same marketing strategies are performed on the Internet, such strategies are not transformed into a “passing off” situation simply because the strategy is electronic.

Though the Court assumes “likelihood of
confusion” for purposes of this motion, such confusion cannot be attributed to defendant’s actions for purposes of trademark infringement liability where defendant is not “using” plaintiff’s mark. Plaintiff has not alleged claims based on defendant’s display of plaintiff’s mark or claims based on similarity of the marks and resulting consumer confusion between the parties’ respective marks; rather, plaintiff’s claim is based exclusively on defendant’s internal use of plaintiff’s mark to obtain a display position in search results proximate to links to plaintiff’s website. “The owner of the mark acquires the right to prevent his goods from being confused with those of others and to prevent his own trade from being diverted to competitors through their use of misleading marks. ‘There are no rights in a trade-mark beyond these.’” Pirone, 894 F.2d at 581 (quoting Industrial Rayon Corp. v. Dutchess Underwear Corp., 92 F.2d 33, 35 (2d Cir. 1937)). With the technological development of the Internet, the landscape for the advertisement of goods and services has changed dramatically; however, internal uses of trademarks in cyberspace are not converted into Lanham Act “uses” merely because of the advancements in the effectiveness and scope of advertising that has come with development of the Internet.

Also relying on the Second Circuit’s

---

Interestingly, plaintiff’s Proposed Third Amended Complaint alleges that “Defendant has failed and refused to use a negative match, a well-known and commonly used mechanism, to avoid having Defendant’s Web site appear as a Sponsored Link when consumers run an Internet keyword search for ‘Fragrance Net’ or other variations of Plaintiff’s mark.” (Proposed Third Am. Compl. ¶ 27.) Though use of the mark to create a “negative match” would produce search results different from the use of plaintiff’s mark to create a match, the “use” of plaintiff’s mark in both instances is the same. Thus, it can be said that plaintiff attempts to have it both ways - plaintiff seeks to have defendant “use” plaintiff’s mark to the extent it prevents defendant’s website from appearing as a result of a search, but also argues that such “use” of the mark is Lanham Act use to the extent it causes defendant’s website to appear upon conducting a search.
decision in *I-800 Contacts, Inc.*, three other courts within this Circuit have held that the purchase of a trademark as a “Sponsored Link” is not “use” within the meaning of the Lanham Act. In the first of these cases, *Merck & Co.*, 425 F. Supp. 2d 402, Judge Chin held that the trademark ZOCOR was not “used in commerce” when it was purchased by defendants, Canadian online pharmacies, as a keyword for “Sponsored Links” from internet search engines Google and Yahoo!. Specifically, the Court found that the use at issue in the search engine context—that is, use of the trademark to trigger defendants’ websites as “Sponsored Links” — does not involve “placement” of the trademark “on any goods or containers or displays or associated documents” or use “to indicate source or sponsorship” and thus, is “not use of the mark in a trademark sense.” *Merck & Co.*, 425 F. Supp. 2d at 415. As the court noted, this conclusion was consistent with the Second Circuit’s recognition in *I-800 Contacts*, that “[a] company’s internal utilization of a trademark in a way that does not communicate it to the public is analogous to an individual’s private thoughts about a trademark.” *Id.* (quoting *I-800 Contacts*, 414 F.3d at 409). In denying plaintiff’s motion for reconsideration, Judge Chin further explained:

In *I-800 Contacts*, the Second Circuit emphasized that commercial use is not the equivalent of “use in commerce” for trademark purposes. It observed that, “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.” 414 F.3d at 412. Trademark use “ordinarily” involves placing a trademark on goods or services to indicate that the goods or services emanate from or are authorized by the owner of the mark. *Id.* at 408.

Here, in the search engine context, defendants do not “place” the ZOCOR marks on goods, containers, displays, or associated documents, nor do they use the marks to indicate source or sponsorship. Rather, the marks are used only in the sense that a computer user’s search of the keyword “Zocor” will trigger the display of sponsored links to defendants’ websites. This internal use of the keyword “Zocor” is not use of the mark in the trademark sense; rather, this use is more akin to the product placement marketing strategy employed in retail stores, where, for example, a drug store places its generic products alongside similar national brand products to capitalize on the latter’s name recognition. See *id.* at 411. The sponsored link marketing strategy is the electronic equivalent of product placement in a retail store.¹⁰

¹⁰ Judge Chin also noted that “defendants actually sell Zocor, albeit Zocor manufactured by Merck’s Canadian affiliates. Hence, there was nothing improper — in the trademark sense — with their purchase of sponsored links tied to searches of the keyword ‘Zocor.’” *Id.* Unlike in *Merck & Co.*, because plaintiff’s mark is used as a website name and plaintiff does not sell any actual products bearing the mark, defendant does not actually sell any product bearing the mark at issue on its website; rather, when an individual types in plaintiff’s trademark, according to plaintiff, that individual is looking for plaintiff’s website. The Court finds that this minor distinction does not support a claim that defendant is using the plaintiff’s trademark in the trademark sense because the use of the trademark as a metatag and
Merck & Co., 431 F. Supp. 2d at 428 (citing 1-800 Contacts, 414 F.3d at 408-412).

Similarly, in Rescuecom Corp., the court held that the use of a trademark as a keyword was not “use” within the meaning of the Lanham Act. 456 F. Supp. 2d at 403. Specifically, after distinguishing Playboy Enters., 354 F. 3d at 1024, Brookfield Communications, 174 F.3d at 1036, and Bihari v. Gross, 119 F. Supp. 2d 309 (S.D.N.Y. 2000), the court concluded that, “in the absence of allegations that defendant placed plaintiff’s trademark on any goods, displays, containers, or advertisements, or used plaintiff’s trademark in any way that indicates source or origin, plaintiff can prove no facts in support of its claim which demonstrate trademark use.” Id. at 403. Plaintiff attempts to distinguish Rescuecom from the instant case because, in Rescuecom, the claims were alleged against Google, the party that sold the keyword, whereas here, the claims are alleged against the party that bought the keyword. (Pl.’s Mem. at 11.) Plaintiff fails to explain how such a distinction changes the analysis and, in any event, the Court finds that it is a distinction without a difference as the issue is whether the trademark is placed on any goods or containers or used in such a way as to indicate source or sponsorship. In other words, the

Court fails to see how the analysis in connection with the sale of a trademark as a keyword would be different from the purchase of a trademark as a keyword.

Most recently, on May 9, 2007, Magistrate Judge Reyes held that the use of a plaintiff’s trademark as a metatag and the purchase of plaintiff’s trademark for a Yahoo! search algorithm were not “uses” within the meaning of the Lanham Act and granted defendant’s motion to dismiss plaintiff’s claims of trademark infringement, unfair competition and dilution under the Lanham Act and common law unfair competition. Site Pro-I, Inc. v. Better Metal, LLC, No. 06-CV-6508 (ILG) (RER), 2007 U.S. Dist. LEXIS 34107, at *14 (E.D.N.Y. May 9, 2007). In so holding, the court recognized that “courts in other circuits have generally sustained such claims,” but recognized that “courts in this Circuit . . . have largely rejected such claims.” Id. at *6-7 (collecting cases). Persuaded by the reasoning in Merck & Co. and Rescuecom, “as well as by the underlying rationale of 1-800 Contacts,” the court determined that “[t]he key question is whether the defendant placed plaintiff’s trademark on any goods, displays, containers, or advertisements, or used plaintiff’s trademark in any way that indicates source or origin.” Id. at *13. Because the complaint contained no such allegation, the court held that Lanham Act “use” was not alleged. Id. (“Indeed, the search results submitted as an exhibit to the complaint make clear that [defendant] did not place plaintiff’s . . . trademark on any of its goods, or any advertisements or displays associated with the sale of its good. Neither the link to [defendant’s] website nor the surrounding text mentions [plaintiff] or [plaintiff’s] trademark. The same is true with respect to [defendant’s] metadata, which is not displayed to consumers.”).
In Hamzik v. Zale Corp./Delaware, No. 06-CV-1300 (TJM), 2007 U.S. Dist. LEXIS 28981, at *8 (N.D.N.Y. Apr. 19, 2007), the Court agreed with the reasoning in Rescuecom and Merck, but denied the motion to dismiss, because a search of plaintiff’s trademark not only returned defendant’s website among the search results, but plaintiff’s trademark also appeared next to defendant’s name, demonstrating that plaintiff’s trademark could be displayed in a way indicating an association with defendant. Id. at *3 (“Thus, unlike Rescuecom and Merck & Co., in this case there may be facts demonstrating that Plaintiff’s trademark does appear on the displays associated with [defendant’s] goods or documents associates with the goods or their sale.”). Here, there is no allegation that links to defendant’s website appear in a way that contains plaintiff’s trademark.

Plaintiff would have this Court reject the holdings in Merck & Co., Rescuecom and Site Pro-1, Inc., and rely instead on the conclusions reached in other circuits. See e.g., Australian Gold, Inc. v. Hatfield, 436 F.3d 1228, 1249 (10th Cir. 2006) (affirming denial of judgment as a matter of law on Lanham Act claims based on the use of trademarks in metatags); Promatek Indus., LTD v. Equitrac Corp., 300 F.3d 808, 814 (7th Cir. 2002) (affirming district court’s grant of a preliminary injunction where plaintiff alleged Lanham Act claim based on defendant’s use of the mark in metatags); Brookfield Commc’ns., Inc., 174 F.3d at 1066 (holding that defendant’s use of trademarks in metatags constituted trademark infringement); J.G. Wentworth, S.S.C. Ltd. P’ship v. Settlement Funding LLC, No. 06-CV-0597 (TNO), 2007 U.S. Dist. LEXIS 288, at *17 (E.D. Pa. Jan. 4, 2007) (concluding that use of a mark in keywords and metatags is Lanham Act “use”); Buying for the Home, LLC v. Humble Abode, LLC, 459 F. Supp. 2d 310, 323 (D. N.J. 2006) (holding that purchase of keyword is Lanham Act use); Edina Realty, Inc. v. TheMLSonline.com, No. 04-CV-4371 (JRT), 2006 U.S. Dist. LEXIS 13775, at *9-*10 (D. Minn. Mar. 20, 2006) (same). Several of these cases conflate the issue of “use” and “likelihood of confusion.” Such analysis is in stark contrast to the Second Circuit’s instruction in 1-800 Contacts that “use” and “likelihood of confusion” are two distinct elements of a Lanham Act claim and that to consider “likelihood of confusion” without first independently analyzing the “use” element, “puts the cart before the horse.” 1-800 Contacts, 414 F.3d at 412. Furthermore, the reasoning of these opinions is inconsistent with 1-800 Contacts holding that “internal utilization of a trademark in a way that does not communicate it to the public” does not violate the Lanham Act. 414 F.3d at 409.

Thus, this Court agrees with the sound reasoning of the courts in Merck & Co., Rescuecom and Site Pro-1, Inc. and reaches the same conclusion. Accordingly, the Court finds that plaintiff’s proposed claims, based on defendant’s alleged use of plaintiff’s trademark as a keyword in Google and as a metatag on its website, cannot survive a motion to dismiss. Therefore, plaintiff’s motion to amend the complaint is denied, as the proposed amendments would be futile.11

11 Defendants also assert that all of plaintiff’s claims are futile on the basis that plaintiff’s alleged trademark is generic or highly descriptive as a matter of law, and thus, not protectable. See, e.g., CES Publ’g Corp. v. St. Regis Publ’ns, Inc., 531 F.2d 11 (2d Cir. 1975) (holding that “Consumer Electronics” was generic and not protectable as a matter of law); McSpadden v. Caron, No. 03-CV-6285 (CJS), 2004 WL
III. CONCLUSION

For the foregoing reasons, plaintiff's motion to amend the complaint is denied as futile.

SO ORDERED.

_________________________
JOSEPH F. BIANCO
United States District Judge

Dated: June 12, 2007
Central Islip, New York

***

The attorneys for plaintiff are Robert L. Sherman, Esq., and Rebecca Myers, Esq., Paul, Hastings, Janofsky & Walker LLP, 75

210 8394 at *13 (W.D.N.Y. Sept. 20, 2004) (finding “usamedicine.com” merely descriptive); InterState Net Bank v. Ne@nk, Inc., 221 F. Supp. 2d 513 (D.N.J. 2002) (finding “NETBANK” generic); Allied Maint. Corp. v. Allied Mech. Trades, Inc., 369 N.E.2d 1162, 1166 (N.Y. 1977) (“[O]nly those trade names which are truly of distinctive quality or which have acquired a secondary meaning in the mind of the public should be entitled to protection under the anti-dilution statute.”); see also Abercrombie & Fitch Co. v. Hunting World, Inc., 537 F.2d 4, 9 (2d Cir. 1976) (“[N]o matter how much money and effort the user of a generic term has poured into promoting the sale of its merchandise and what success it has achieved in securing public identification, it cannot deprive competing manufacturers of the product of the right to call an article by its name.”). Because plaintiff's claims are futile for the reasons stated above on the issue of use, the Court declines to address whether the plaintiff's mark is protectable.
Eric Goldman’s Helpful Hints
To Knowing Your Porn Terms!

- Obscenity is: “(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.” [Miller]

- Indecency is: “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]

Compare the CDA: “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.”

- Harmful to minor is: “(a) patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; (b) appeals to the prurient interests of minors; and (c) is utterly without redeeming social importance for minors.” [Ginsberg]

Compare COPA: “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.”

- Child pornography is: “works that visually depict sexual conduct by children below a specified age, where the category of “sexual conduct” proscribed is suitably limited and described.” [Ferber] In the New York statute’s case, “sexual conduct” was defined as “actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals.”

- Pornography is: ??????
U.S. Supreme Court

No. 96-511

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

on appeal from the united states district court for the eastern district of pennsylvania

[June 26, 1997]

Justice Stevens delivered the opinion of the Court.

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

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

The Internet

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

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

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

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

E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." 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." 10

**Sexually Explicit Material**

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest core." 11 These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community." 12 Thus, for example,

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

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

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

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

**Age Verification**
The problem of age verification differs for different uses of the Internet. The District Court categorically determined that there "is no effective way to determine the identity or the age of a user who is accessing material through email, mail explosives, 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
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, 28 the two cases were consolidated, and a three judge District Court was convened pursuant to §561 of the Act. 29 After an evidentiary hearing, that Court entered a preliminary injunction against enforcement of both of the challenged provisions. Each of the three judges wrote a separate opinion, but their judgment was unanimous.

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

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

Judge Dalzell's review of "the special attributes of Internet communication" disclosed by the evidence convinced him that the First Amendment denies Congress the power to regulate the content of protected speech on the Internet. Id., at 867. His opinion explained at length why he believed the Act would abridge significant protected speech, particularly by noncommercial speakers, while "[p]erversely, commercial pornographers would remain relatively unaffected." Id., at 879. He construed our cases as requiring a "medium specific" approach to the analysis of the regulation of mass communication, id., at 873, and concluded that the Internet—"as the most participatory form of mass speech yet developed," id., at 883—is entitled to "the highest protection from governmental intrusion," ibid. 30.
The judgment of the District Court enjoins the Government from enforcing the prohibitions in §223(a) (1)(B) insofar as they relate to "indecent" communications, but expressly preserves the Government's right to investigate and prosecute the obscenity or child pornography activities prohibited therein. The injunction against enforcement of §§223(d)(1) and (2) is unqualified because those provisions contain no separate reference to obscenity or child pornography.

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

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

In Ginsberg, we upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene as to them even if not obscene as to adults. We rejected the defendant's broad submission that "the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor." 390 U.S., at 636. In rejecting that contention, we relied not only on the State's independent interest in the well being of its youth, but also on our consistent recognition of the principle that "the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society." 31 In four important respects, the statute upheld in Ginsberg was narrower than the CDA. First, we noted in Ginsberg that "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children." Id., at 639. Under the CDA, by contrast, neither the parents' consent—nor even their participation—in the communication would avoid the application of the statute. 32 Second, the New York statute applied only to commercial transactions, id., at 647, whereas the CDA contains no such limitation. Third, the New York statute 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. 33 Moreover, the Internet is not as "invasive" as radio or television. The District Court specifically found that "[c]ommunications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'" 929 F. Supp., at 844 (finding 88). It also found that "[a]lmost all sexually explicit images are preceded by warnings as to the content," and cited testimony that "'odds are slim' that a user would come across a sexually explicit sight by accident." 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 "scare" expressive commodity. It provides relatively unlimited, low cost capacity for communication of all kinds. The Government estimates that "[a]s many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." 34 This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought." 929 F. Supp., at 842 (finding 74). We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

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

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

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

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

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

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

The Government's reasoning is also flawed. Just because a definition including three limitations is not
vague, it does not follow that one of those limitations, standing by itself, is not vague. 38 Each of
Miller's additional two prongs—(1) that, taken as a whole, the material appeal to the "prurient" interest,
and (2) that it "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

467

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 value—the message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute. Under the CDA, a parent allowing her 17 year old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. See 47 U. S. C. A. §223(a)(2) (Supp. 1997). Similarly, a parent who sent his 17 year old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

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

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

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

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

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

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

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

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

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

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

The Government also draws on an additional, less traditional aspect of the CDA's severability clause, 47 U. S. C., §608, which asks any reviewing court that holds the statute facially unconstitutional not to invalidate the CDA in application to "other persons or circumstances" that might be constitutionally permissible. It further invokes this Court's admonition that, absent "countervailing considerations," a statute should "be declared invalid to the extent it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 503-504 (1985). There are two flaws in this argument.
First, the statute that grants our jurisdiction for this expedited review, 47 U. S. C. A. §561 (Supp. 1997), limits that jurisdictional grant to actions challenging the CDA "on its face." Consistent with §561, the plaintiffs who brought this suit and the three judge panel that decided it treated it as a facial challenge. We have no authority, in this particular posture, to convert this litigation into an "as applied" challenge. Nor, given the vast array of plaintiffs, the range of their expressive activities, and the vagueness of the statute, would it be practicable to limit our holding to a judicially defined set of specific applications.

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

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

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

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

For the foregoing reasons, the judgment of the district court is affirmed.

It is so ordered.

U.S. Supreme Court

No. 96-511

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

on appeal from the united states district court for the eastern district of pennsylvania

[June 26, 1997]

Justice O'Connor, with whom The Chief Justice joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. 47 U. S. C. A. §223(a) (1)(B) (May 1996 Supp.). What the Court classifies as a single "patently offensive display" provision, see ante, at 11, is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specific person" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in a[n] 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 segregateindecent 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. States have also denied minors access to speech deemed to be "harmful to minors." 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 "tend[d] to . . . corrupt[t] the morals of youth"); Sable Communications, supra (invalidating federal law that made it a crime to transmit indecent, but nonobscene, commercial telephone messages to minors and adults); Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 74 (1983) (striking down a federal law prohibiting the mailing of unsolicited advertisements for contraceptives). If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In Ginsberg v. New York, 390 U.S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazines to minors in part because adults could still buy those magazines.

The Court in Ginsberg concluded that the New York law created a constitutionally adequate adult zone simply because, on its face, it denied access only to minors. The Court did not question—and therefore necessarily assumed—that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity. See Lessig, Reading the Constitution in Cyberspace, 45 Emory L. J. 869, 886 (1996). A minor can see an adult dance show only if he enters an establishment that provides such entertainment. And should he attempt to do so, the minor will not be able to conceal completely his identity (or, consequently, his age). Thus, the twin characteristics of geography and identity enable the establishment's proprietor to prevent children from entering the establishment, but to let adults inside.

The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities. Cyberspace undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed "locations" on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, see Lessig, supra, at 901, however, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. Lessig, supra, at 888-889. Id., at 887 (cyberspace "is moving . . . from a relatively unzoned place to a universe that is extraordinarily well zoned"). Internet speakers (users who post-material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves—perhaps an adult identification number or a credit card number—before they can access certain areas of cyberspace, 929 F. Supp. 824, 845 (ED Pa. 1996), much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites. Id., at 839-842. The Platform for Internet Content Selection (PICS) project is designed to facilitate user based zoning by encouraging Internet speakers to rate the content of their speech using codes recognized by all screening programs. Id., at 838-839.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, id., at 845; Shea v. Reno, 930 F. Supp. 916, 933-934 (SDNY 1996), it is not available to all Web speakers, 929 F. Supp., at 845-846, and is just
now becoming technologically feasible for chat rooms and USENET newsgroups, Brief for Federal Parties 37-38. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned—and unzoneable. 929 F. Supp., at 846; Shea, supra, at 934. User based zoning is also in its infancy. For it to be effective, (i) an agreed upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available—and widely used—by Internet users. At present, none of these conditions is true. Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." Shea, supra, at 945-946. There is, moreover, no agreed upon "tag" for those programs to recognize. 929 F. Supp., at 848; Shea, supra, at 945.

Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today. Ante, at 36. Given the present state of cyberspace, I agree with the Court that the "display" provision cannot pass muster. Until gateway technology is available throughout cyberspace, and it is not in 1997, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an "adult zone." Thus, the only way for a speaker to avoid liability under the CDA is to refrain completely from using obscene speech. But this forced silence impinges on the First Amendment right of adults to make and obtain this speech and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." Butler, 352 U.S., at 383. As a result, the "display" provision cannot withstand scrutiny. Accord, Sable Communications, 492 U.S., at 126-131; Bolger v. Youngs Drug Products Corp., 463 U.S., at 73-75.

The "indecency transmission" and "specific person" provisions present a closer issue, for they are not unconstitutional in all of their applications. As discussed above, the "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18 years of age. 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.). The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient of his indecent message is a minor. §223(d)(1)(A). Appellant urges the Court to construe the provision to impose such a knowledge requirement, see Brief for Federal Parties 25-27, and I would do so. See Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress").

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors—e.g., when an adult speaker sends an e-mail knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in Ginsberg. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults. He is not prevented from speaking indecently to other adults in a chat room (because there are no other adults participating in the conversation) and he remains free to send indecent e-mails to other adults. The relevant universe contains only one adult, and the adult in that universe has the power to refrain from using indecent speech and consequently to keep all such speech within the room in an "adult" zone.

The analogy to Ginsberg breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group, since they would be transmitting an indecent message to specific persons, one of whom is a
minor. Accord, ante, at 30. The CDA is therefore akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters his store. Even assuming such a law might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store, the absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. And as discussed below, I do not find that the provisions are overbroad in the sense that they restrict minors' access to a substantial amount of speech that minors have the right to read and view. Accordingly, the CDA can be applied constitutionally in some situations. Normally, this fact would require the Court to reject a direct facial challenge. United States v. Salerno, 481 U.S. 739, 745 (1987) ("A facial challenge to a legislative Act [succeeds only if] the challenger . . . establish[es] that no set of circumstances exists under which the Act would be valid"). Appellees' claim arises under the First Amendment, however, and they argue that the CDA is facially invalid because it is "substantially overbroad"—that is, it "sweeps too broadly . . . [and] penaliz[es] a substantial amount of speech that is constitutionally protected," Forsyth County v. Nationalist Movement, 505 U.S. 123, 130 (1992). See Brief for Appellees American Library Association et al. 48; Brief for Appellees American Civil Liberties Union et al. 39-41. I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication.

This conclusion does not end the matter, however. Where, as here, "the parties challenging the statute are those who desire to engage in protected speech that the overbroad statute purports to punish . . . [t]he statute may forthwith be declared invalid to the extent that it reaches too far, but otherwise left intact." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 504 (1985). There is no question that Congress intended to prohibit certain communications between one adult and one or more minors. See 47 U. S. C. A. §223(a)(1)(B) (May 1996 Supp.) (punishing "[w]hoever . . . initiates the transmission of [any indecent communication] knowingly that the recipient of the communication is under 18 years of age"); §223(d)(1)(A) (punishing "[w]hoever . . . send[s] to a specific person or persons under 18 years of age [a patently offensive message]"). There is also no question that Congress would have enacted a narrower version of these provisions had it known a broader version would be declared unconstitutional. 47 U.S.C. § 608 ("If . . . the application [of any provision of the CDA] to any person or circumstance is held invalid, . . . the application of such provision to other persons or circumstances shall not be affected thereby"). I would therefore sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of Internet communications where the party initiating the communication knows that all of the recipients are minors.

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question. In Ginsberg, the New York law we sustained prohibited the sale to minors of magazines that were "harmful to minors." Under that law, a magazine was "harmful to minors" only if it was obscene as to minors. 330 U.S., at 632-633. Noting that obscene speech is not protected by the First Amendment, Roth v. United States, 354 U.S. 476, 485 (1957), and that New York was constitutionally free to adjust the definition of obscenity for minors, 390 U.S., at 638, the Court concluded that the law did not "invad[e] the area of freedom of expression constitutionally secured to minors." Id., at 637. New York therefore did not infringe upon the First Amendment rights of minors. Cf. Erznoznik v. Jacksonville, 422 U.S. 205, 213 (1975) (striking down city ordinance that banned nudity that was not "obscene even as to minors").

The Court neither "accept[s] nor reject[s]" the argument that the CDA is facially overbroad because it substantially interferes with the First Amendment rights of minors. Ante, at 32. I would reject it.
Ginsberg established that minors may constitutionally be denied access to material that is obscene as to minors. As Ginsberg explained, material is obscene as to minors if it (i) is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable . . . for minors"; (ii) appeals to the prurient interest of minors; and (iii) is "utterly without redeeming social importance for minors." 390 U.S., at 633. Because the CDA denies minors the right to obtain material that is "patently offensive"—even if it has some redeeming value for minors and even if it does not appeal to their prurient interests—Congress' rejection of the Ginsberg "harmful to minors" standard means that the CDA could ban some speech that is "indecent" (i.e., "patently offensive") but that is not obscene as to minors.

I do not deny this possibility, but to prevail in a facial challenge, it is not enough for a plaintiff to show "some" overbreadth. Our cases require a proof of "real" and "substantial" overbreadth, Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973), and appellees have not carried their burden in this case. In my view, the universe of speech constitutionally protected as to minors but banned by the CDA—i.e., the universe of material that is "patently offensive," but which nonetheless has some redeeming value for minors or does not appeal to their prurient interest—is a very small one. Appellees cite no examples of speech falling within this universe and do not attempt to explain why that universe is substantial "in relation to the statute's plainly legitimate sweep." Ibid. That the CDA might deny minors the right to obtain material that has some "value," see ante, at 32-33, is largely beside the point. While discussions about prison rape or nude art, see ibid., may have some redeeming education value for adults, they do not necessarily have any such value for minors, and under Ginsberg, minors only have a First Amendment right to obtain patently offensive material that has "redeeming social importance for minors." 390 U.S., at 633 (emphasis added). There is also no evidence in the record to support the contention that "many [e] mail transmissions from an adult to a minor are conversations between family members," ante, at 18, n. 32, and no support for the legal proposition that such speech is absolutely immune from regulation. Accordingly, in my view, the CDA does not burden a substantial amount of minors' constitutionally protected speech.

Thus, the constitutionality of the CDA as a zoning law hinges on the extent to which it substantially interferes with the First Amendment rights of adults. Because the rights of adults are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained. The Court reaches a contrary conclusion, and from that holding that I respectfully dissent.

Footnotes

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

[Footnote 2.] The Court made 410 findings, including 356 paragraphs of the parties' stipulation and 54 findings based on evidence received in open court. See 929 F. Supp. at 830, n. 9, 842, n. 15.

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

[Footnote 4.] Id., at 844 (finding 81).
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.
Opinion of the Court

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 con-
vention 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-
trict 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
Opinion of the Court

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-
posed 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/opds (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.
Opinion of the Court

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 requiring
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 restriction
of nonobscene expression is “narrowly drawn” to
further a “compelling interest” and that the restriction
amounts to the “least restrictive means” available to further
that interest, Sable Communications of Cal., Inc. v. FCC, 492 U. S. 115, 126 (1989). See also Denver Area Ed.
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-
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 *Ginzburg 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 fit 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.
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 alternative 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 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 "blocks 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
BREYER, J., dissenting

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-suppressing 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.
U.S. Code collection

TITLE 47 > CHAPTER 5 > SUBCHAPTER II > Part I > § 230

§ 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).[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
services 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)."

LII has no control over and does not endorse any external Internet site that contains links to or references LII.
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.
EDWARDS, Roanoke, Virginia; Leo Kayser, III, KAYSER & RED-
FERN, New York, New York, for Appellant. Patrick Joseph Carone,
WILMER, CUTLER & PICKERING, Washington, D.C., for Appel-
lee. ON BRIEF: John Payton, Samir Jain, WILMER, CUTLER &
OPINION

WILKINSON, Chief Judge:

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The district court granted judgment for AOL on the grounds that the Communications Decency Act of 1996 ("CDA") -- 47 U.S.C. § 230 -- bars Zeran's claims. Zeran appeals, arguing that § 230 leaves intact liability for interactive computer service providers who possess notice of defamatory material posted through their services. He also contends that § 230 does not apply here because his claims arise from AOL's alleged negligence prior to the CDA's enactment. Section 230, however, plainly immunizes computer service providers like AOL from liability for information that originates with third parties. Furthermore, Congress clearly expressed its intent that § 230 apply to lawsuits, like Zeran's, instituted after the CDA's enactment. Accordingly, we affirm the judgment of the district court.

I.

"The Internet is an international network of interconnected computers," currently used by approximately 40 million people worldwide. Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997). One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. Id. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.
The instant case comes before us on a motion for judgment on the pleadings, see Fed. R. Civ. P. 12(c), so we accept the facts alleged in the complaint as true. Bruce v. Riddle, 631 F.2d 272, 273 (4th Cir. 1980). On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T-Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

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

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death
threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRKO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRKO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRKO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages. After Zeran's suit against AOL was transferred to the Eastern District of Virginia pursuant to 28 U.S.C. § 1404(a), AOL answered Zeran's complaint and interposed 47 U.S.C. § 230 as an affirmative defense. AOL then moved for judgment on the pleadings pursuant to Fed. R. Civ. P. 12(c). The district court granted AOL's motion, and Zeran filed this appeal.

II.

A.

Because § 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

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.
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)(B) By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions - such as deciding whether to publish, withdraw, postpone or alter content - are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Id., § 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, with a mini-

2 Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(e)(2). The term "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Id., § 230(e)(3). The parties do not dispute that AOL falls within the CDA's "interactive computer service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."
mun of government regulation." Id. § 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States... to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." Id. § 230(b)(2) (emphasis added).

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." Id. § 230(b)(5). Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

Congress' purpose in providing the § 230 immunity was thus evident. Interactive computer services have millions of users. See Reno v. ACLU, 117 S. Ct. at 2334 (noting that at time of district court trial, "commercial online services had almost 12 million individual subscribers"). The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, § 230 responded to a New York state court decision, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). There, the plaintiffs sued Prodigy -- an interactive computer service like AOL -- for defamatory comments made by an unidentified party on one of Prodigy's
bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

Congress enacted § 230 to remove the disincentives to self-regulation created by the Stratten Oakmont decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). In line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

B.

Zeran argues, however, that the § 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion. W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 113, at 810 (5th ed. 1984). According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Id., at 811 (explaining that distributors are not liable "in the absence of proof that they knew or had reason to know of the existence of defamatory matter contained in matter published").
Zeran contends that he provided AOL with sufficient notice of the defamatory statements appearing on the company's bulletin board. This notice is significant, says Zeran, because AOL could be held liable as a distributor only if it acquired knowledge of the defamatory statements' existence.

Because of the difference between these two forms of liability, Zeran contends that the term "distributor" carries a legally distinct meaning from the term "publisher." Accordingly, he asserts that Congress' use of only the term "publisher" in § 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected by § 230 and, therefore, his suit should be permitted to proceed against AOL. We disagree. Assuming arguendo that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.

The terms "publisher" and "distributor" derive their legal significance from the context of defamation law. Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action. Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject to this form of tort liability. Restatement (Second) of Torts § 558(b) (1977); Keeton et al., supra, § 113, at 802. Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party -- each alleged by Zeran here under a negligence label -- constitute publication. Restatement (Second) of Torts § 577; see also Tacket v. General Motors Corp., 836 F.2d 1042, 1046-47 (7th Cir. 1987). In fact, every repetition of a defamatory statement is considered a publication. Keeton et al., supra, § 113, at 799.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication . . . is charged with publication." Id. Even distributors are considered to be publishers for purposes of defamation law:

8
Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents -- including the defamatory content -- and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published.

Id. at 803. AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 230's immunity.

Zeran contends that decisions like Stratton Oakmont and Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991), recognize a legal distinction between publishers and distributors. He misapprehends, however, the significance of that distinction for the legal issue we consider here. It is undoubtedly true that mere conduits, or distributors, are subject to a different standard of liability. As explained above, distributors must at a minimum have knowledge of the existence of a defamatory statement as a prerequisite to liability. But this distinction signifies only that different standards of liability may be applied within the larger publisher category, depending on the specific type of publisher concerned. See Keeton et al., supra, § 113, at 799-800 (explaining that every party involved is charged with publication, although degrees of legal responsibility differ). To the extent that decisions like Stratton and Cubby utilize the terms "publisher" and "distributor" separately, the decisions correctly describe two different standards of liability. Stratton and Cubby do not, however, suggest that distributors are not also a type of publisher for purposes of defamation law.

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 investigation of the circumstances surrounding the posted information, a legal judgment concerning the information’s defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Cf. Avril 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 sig-
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 caution 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." Eisenach Co. v. Johnson, 343 U.S. 779, 783 (1952) (quoting Jamison v. Ence, 281 U.S. 635, 640 (1930)); cf. Astoria Fed. Sav. & Loan Ass'n v. Solimeno, 501 U.S. 104, 110-11 (1991) (statute need not expressly delimit manner in which common law principle is abrogated). Zeran's argument flies in the face of this warning. As explained above, interpreting § 230 to leave distributor liability in effect would defeat the two primary purposes of the statute and would certainly "lessen the scope plainly intended" by Congress' use of the term "publisher."

Section 230 represents the approach of Congress to a problem of national and international dimension. The Supreme Court underscored this point in ACLU v. Reno, finding that the Internet allows "tens of millions of people to communicate with one another and to access vast amounts of information from around the world.[R] 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 commerce, state laws regulating that aspect of commerce must fall. The
result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose. Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977) (citations omitted). Here, Congress' command is explicitly stated. Its exercise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.

III

The CDA was signed into law and became effective on February 8, 1996. Zeran did not file his complaint until April 23, 1996. Zeran contends that even if § 230 does bar the type of claim he brings here, it cannot be applied retroactively to bar an action arising from AOL's alleged misconduct prior to the CDA's enactment. We disagree. 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 the complaint"), cert. denied, 116 S. Ct. 2563 (1996); Nurnon v. Cassville Valley Central Sch. Dist., 49 F.3d 886, 889 (8th Cir. 1995) (same).

Even if this were a case implicating the application of a federal statute to pre-enactment events, the Supreme Court's Landgraf framework would nevertheless require § 230's application to Zeran's claims. Landgraf instructs us first "to determine whether Congress has expressly prescribed the statute's proper reach." Landgraf v. US

13
FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Fair Housing Council of San Fernando Valley; The Fair Housing Council of San Diego, individually and on behalf of the General Public,

Plaintiffs-Appellants,

v.

Roommates.com, LLC,

Defendant-Appellee.

No. 04-56916
D.C. No.
CV-03-09386-PA

Fair Housing Council of San Fernando Valley; The Fair Housing Council of San Diego, individually and on behalf of the General Public,

Plaintiffs-Appellees,

v.

Roommate.com, LLC,

Defendant-Appellant.

No. 04-57173
D.C. No.
CV-03-09386-PA

OPINION

Appeal from the United States District Court for the Central District of California
Percy Anderson, District Judge, Presiding

Argued and Submitted
December 5, 2006—Pasadena, California

Filed May 15, 2007


5709
COUNSEL

Gary Rhoades, Rhoades & Al-Mansour, Los Angeles, California; Michael Evans, Costa Mesa, California; and Christopher Brancart, Brancart & Brancart, Pescadero, California, for the plaintiffs-appellants.

Timothy L. Alger, Lesley E. Williams and Steven B. Stiglitz, Quinn Emanuel Urquhart Oliver & Hedges, LLP, Los Angeles, California, for the defendant-appellee.

Patrick J. Carome, Samir Jain and C. Colin Rushing, Wilmer Cutler Pickering Hale & Dorr, LLP, Washington, D.C., as amici curiae in support of the defendant-appellee.

OPINION

KOZINSKI, Circuit Judge:

We consider the scope of immunity accorded to an online roommate matching service by the Communications Decency Act (“CDA”), 47 U.S.C. § 230(c).

Facts

The Internet has opened new channels of communication and self-expression. See Lev Grossman, Time’s Person of the Year: You, TIME MAG., Dec. 13, 2006-Jan. 1, 2007, at 38, 40-41. Countless individuals use message boards, date matching sites, interactive social networks, blog hosting services and video sharing websites to make themselves and their ideas visible to the world.1 While such intermediaries enable the user-driven digital age, they also create new legal problems.

1Confirming perhaps Andy Warhol’s prediction that everyone would eventually enjoy a trillion or so nanoseconds of fame.
This case involves one such intermediary, Roommate.com, LLC ("Roommate"), which operates an online roommate matching website at www.roommates.com. This website helps individuals find roommates based on their descriptions of themselves and their roommate preferences. Roommates.com has approximately 150,000 active listings and receives about a million page views per day.

To become members of Roommate, users respond to a series of online questionnaires by choosing from answers in drop-down and select-a-box menus. Users must disclose information about themselves and their roommate preferences based on such characteristics as age, sex and whether children will live in the household. They can then provide "Additional Comments" through an open-ended essay prompt.

Roommate's free membership allows users to create personal profiles, search lists of compatible roommates and send "roommail" messages to other members. Roommate also sends email newsletters to members seeking housing, listing compatible members who have places to rent out. Roommate's fee-based membership allows users to read their "roommail" and view the "Additional Comments" essays of other members.

The Fair Housing Councils of San Fernando Valley and San Diego ("the Councils") filed suit in federal district court, claiming that Roommate violated the Fair Housing Act ("FHA") and various state laws. The district court held that the Communications Decency Act barred the Councils' FHA claim. As a result, the court granted, in part, Roommate's summary judgment motion and entered judgment in Roommate's favor on the FHA claim. The district court then declined to exercise supplemental jurisdiction over the state-law claims and dismissed them. It also denied Roommate's motion for attorneys' fees and costs. The Councils now appeal the dismissal of their FHA claim and Roommate cross-appeals the denial of fees and costs.
Analysis

[1] According to the CDA, "[n]o provider . . . 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). One of Congress's goals in adopting this provision was to encourage "the unfettered and unregulated development of free speech on the Internet." Bartzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003) (citing 47 U.S.C. § 230(a)(3)-(4), (b)(1)-(2)).

[2] The touchstone of section 230(c) is that providers of interactive computer services are immune from liability for content created by third parties. The immunity applies to a defendant who is the "provider . . . of an interactive computer service" and is being sued "as the publisher or speaker of any information provided by" someone else. 47 U.S.C. § 230(c). "[R]eviewing courts have treated § 230(c) immunity as quite robust." Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

[3] The Councils do not dispute that Roommate is a provider of an interactive computer service. As such, Roommate is immune so long as it merely publishes information pro-

---

2Congress also wanted to allow interactive computer services to regulate their own content without subjecting themselves to liability. Bartzel, 333 F.3d at 1028 (citing 47 U.S.C. § 230(b)(4)); see also n.5 infra.

3The CDA also provides immunity in such circumstances for users of interactive services, but because our case does not involve a claim against users, we have no occasion to consider the scope of this immunity. We therefore omit all references to user immunity when quoting the statutory text.

4The CDA defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2); see also Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002) (date matching website is an "interactive computer service"), aff'd, 339 F.3d 1119 (9th Cir. 2003).
vided by its members. *Batzel*, 333 F.3d at 1031. However, Roommate is not immune for publishing materials as to which it is an “information content provider.” A content provider is “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet.” 47 U.S.C. § 230(f)(3) (emphasis added). In other words, if Roommate passively publishes information provided by others, the CDA protects it from liability that would otherwise attach under state or federal law as a result of such publication. But if it is responsible, in whole or in part, for creating or developing the information, it becomes a content provider and is not entitled to CDA immunity. As we explained in *Carafano*, “an ‘interactive computer service’ qualifies for immunity so long as it does not also function as an ‘information content provider’ for the portion of the statement or publication at issue.” 339 F.3d at 1123.

The Councils claim Roommate violates the FHA in three ways: (1) it posts the questionnaires on its website and requires individuals who want to take advantage of its services to complete them; (2) it posts and distributes by email its members’ profiles; and (3) it posts the information its members provide on the “Additional Comments” form. For all three categories, the question is whether Roommate is “responsible, in whole or in part, for the creation or development of [the] information.” 47 U.S.C. § 230(c), (f)(3); see also *Batzel*, 333 F.3d at 1031.

1. As previously explained, in order to become members of Roommate and take advantage of the services it offers, indi-

---

---

8As we discuss below, a provider of an interactive computer service does not lose its CDA immunity if it merely exercises some control over the posting of information provided by others, such as enforcement of rules as to appropriate content or minor editing. See n.6 *infra*. Nor does it generally lose its immunity if it simply facilitates expression of information by individuals. See pp. 5719-22 *infra*. 
Individuals must complete a series of questionnaires. Individuals looking for a room must first complete a form about themselves. They must use a drop-down menu to identify themselves as either “Male” or “Female” and to disclose whether “Children will be present” or “Children will not be present.” Individuals looking to rent out a room must complete a similar form. They must use a check-box menu to indicate whether “Straight male(s),” “Gay male(s),” “Straight female(s),” and/or “Lesbian(s)” now live in the household, and a drop-down menu to disclose if there are “Children present” or “Children not present.” If users fail to provide answers to any of these questions, they cannot complete the membership registration process.

In addition to completing one of the two forms described above, all prospective members must fill out the “My Roommate Preferences” form. They must use a drop-down menu to indicate whether they are willing to live with “Straight or gay” males, only “Straight” males, only “Gay” males, or “No males,” or may choose to select a blank response. Users must make comparable selections for females. They must also declare “I will live with children,” “I will not live with children” or change the field to a blank. 

*When users select the option “I will not live with children,” Roommate publishes this response as “no children please.” The Councils argue that this alteration makes Roommate a content provider and therefore not immune under the CDA for publishing this statement. However, minor editing that does not affect meaning is protected under the CDA as the “usual prerogative of publishers.” See Battel, 333 F.3d at 1031 (publisher of a newsletter protected under the CDA for making minor editing changes to user-submitted content). Because “no children please” is materially the same as “I will not live with children,” Roommate does not lose its CDA immunity because of the change in wording. On the other hand, the Councils allege that Roommate takes members’ blank selection in the children field and publishes it as “no children please.” We could not find support for this proposition in the record, but if Councils’ allegation is true, then Roommate significantly alters the meaning of the information provided by its members and is not entitled to CDA immunity for posting the resulting content.
[4] As we previously explained, an entity cannot qualify for CDA immunity when it is “responsible, in whole or in part, for the creation or development of [the] information” at issue. 47 U.S.C. § 230(c), (f)(3); see also Batzel, 333 F.3d at 1031. Roommate is “responsible” for these questionnaires because it “create[cd] or develop[cd]” the forms and answer choices. As a result, Roommate is a content provider of these questionnaires and does not qualify for CDA immunity for their publication.

Roommate objects that simply asking questions cannot violate the FHA. Yet the Councils advance two theories under which publication of these forms arguably does violate the FHA. First, the Councils argue that asking users to provide information about themselves and their roommate preferences is a “statement . . . with respect to the sale or rental of a dwelling that indicates . . . an intention to make [a] preference, limitation or discrimination.” See 42 U.S.C. § 3604(c) (emphasis added); see, e.g., Jancik v. Dep’t of Hous. & Urban Dev., 44 F.3d 553, 557 (7th Cir. 1995); Soules v. Dep’t of Hous. & Urban Dev., 967 F.2d 817, 824 (2d Cir. 1992). Second, the Councils claim that requiring members to answer questions that enable other members to discriminate for or against them violates the FHA by “causing[ ] users “to [make] . . . any . . . statement . . . with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination.” 42 U.S.C. § 3604(c) (emphasis added).

[5] At this stage, we are only concerned with whether Roommate is immune from liability under the CDA, not

---

7Although Amici Amazon.com, Inc., America Online, Inc., Ebay Inc., Google Inc., Tribune Company, Yahoo! Inc., Netchoice and United States Internet Service Provider Association support Roommate in this appeal, they acknowledge that “if there were a circumstance in which the content of questions posed by an online intermediary—in isolation, and entirely independent of any user’s answers or any third-party’s use of the questions or users’ answers—was itself unlawful, then section 230 might not protect the intermediary from a cause of action based solely on the questions.”
whether it actually violated the FHA. We describe the Councils' FHA theories only to show that the mere asking of questions might, indeed, violate the FHA. It will be up to the district court on remand to decide initially whether Roommate violated the FHA by publishing its form questionnaires.8

2. We now turn to the more difficult question of whether the CDA exempts Roommate from liability for publishing and distributing its members' profiles, which it generates from their answers to the form questionnaires.

Roommate strongly urges that Carafano settles the issue. In Carafano, an unidentified prankster placed a fraudulent personal ad on a date matching website. 339 F.3d at 1121. This imposter created a profile for Carafano, an actress, listing her real phone number and address. The ad claimed that Carafano was looking for "a one-night stand" with a controlling man. Id. We held that the CDA exempted the service from liability for two reasons.

[6] First, the dating service was not an "information content provider" for the profiles on its website. Although the website required users to complete detailed questionnaires consisting of both multiple choice and essay questions that provided "structure and content" and a "menu of 'pre-prepared responses,' " these forms merely "facilitated the expression of information by individual users." Id. at 1124-25 (internal quo-

8Roommate also argues that we should not consider the Councils' FHA liability theories based on the questionnaires because these arguments were not properly raised below. However, we are reviewing only the district court's grant of summary judgment on CDA grounds and remanding the FHA claim for resolution by the district court. In any event, the Councils, in their First Amended Complaint, cited to the FHA, 42 U.S.C. § 3604(e), and alleged that Roommate "encourages" users to state discriminatory preferences. This is more than enough under our liberal notice pleading rule. See Johnson v. Barker, 799 F.2d 1396, 1401 (9th Cir. 1986) ("Under federal notice pleading, appellants are allowed to vary their theory to conform to proof presented.").
tation marks omitted). We concluded that the service could not "be considered an 'information content provider' under the [CDA] because no profile had any content until a user actively create[d] it." Id. at 1124. Second, even if the dating service could be considered a content provider for publishing its customers' profiles, it was exempt from liability because it did not "create[ ] or develop[ ] the particular information at issue." Id. at 1125. The anonymous user entered Carafano's phone number, address and fabricated sexual proclivities, and his entries were "transmitted unaltered to profile viewers." Id. The service was not a content provider of the offending information because it "did not play a significant role in creating, developing or 'transforming' " it. Id.

Carafano differs from our case in at least one significant respect: The prankster in Carafano provided information that was not solicited by the operator of the website. The website sought information about the individual posting the information, not about unwitting third parties. Nothing in the questions the dating service asked suggested, encouraged or solicited posting the profile of another person, and the website's policies prohibited altogether the posting of last names and contact information. Id. at 1121. While Carafano is written in broad terms, it must be read in light of its facts, Carafano provided CDA immunity for information posted by a third party that was not, in any sense, created or developed by the website operator—indeed, that was provided despite the website's rules and policies. Id. We are not convinced that Carafano would control in a situation where defamatory, private or otherwise tortious or unlawful information was provided by users in direct response to questions and prompts from the operator of the website.

Imagine, for example, www.harrassthem.com with the slogan "Don't Get Mad, Get Even." A visitor to this website would be encouraged to provide private, sensitive and/or defamatory information about others—all to be posted online for a fee. To post the information, the individual would be
invited to answer questions about the target’s name, addresses, phone numbers, social security number, credit cards, bank accounts, mother’s maiden name, sexual orientation, drinking habits and the like. In addition, the website would encourage the poster to provide dirt on the victim, with instructions that the information need not be confirmed, but could be based on rumor, conjecture or fabrication.

It is not clear to us that the operator of this hypothetical website would be protected by the logic of Carafano. The date match website in Carafano had no involvement in the creation and development of the defamatory and private information; the hypothetical operator of harrassthem.com would. By providing a forum designed to publish sensitive and defamatory information, and suggesting the type of information that might be disclosed to best harass and endanger the targets, this website operator might well be held responsible for creating and developing the tortious information. Carafano did not consider whether the CDA protected such websites, and we do not read that opinion as granting CDA immunity to those who actively encourage, solicit and profit from the tortious and unlawful communications of others.

[7] While mapping the outer limits of Carafano’s protection of websites that solicit and post users’ responses is an interesting and difficult task, we need not undertake it today because Roommate does more than merely publish information it solicits from its members. Roommate also channels the information based on members’ answers to various questions, as well as the answers of other members. Thus, Roommate allows members to search only the profiles of members with compatible preferences. For example, a female room-seeker who is living with a child can only search profiles of room-providers who have indicated they are willing to live with women and children. Roommate also sends room-seekers email notifications that exclude listings incompatible with their profiles. Thus, Roommate will not notify our female
about room-providers who say they will not live with women or children.

[8] While Roommate provides a useful service, its search mechanism and email notifications mean that it is neither a passive pass-through of information provided by others nor merely a facilitator of expression by individuals. By categorizing, channeling and limiting the distribution of users' profiles, Roommate provides an additional layer of information that it is "responsible" at least "in part" for creating or developing. 47 U.S.C. § 230(c), (f)(3); see also Batele, 333 F.3d at 1031. Whether these actions ultimately violate the FHA is a question the district court must decide in the first instance.8

3. Finally, we consider whether the CDA exempts Roommate from liability for publishing the content its members provide in the "Additional Comments" portion of their profiles. Members provide this information by filling in a blank text box. Next to this box, Roommate advises users that "[w]e strongly recommend taking a moment to personalize your profile by writing a paragraph or two describing yourself and what you are looking for in a roommate." The responses to this query produce the most provocative and revealing information in many users' profiles. Some state that they "Pref[er] white Male roommates," while others declare that they are "NOT looking for black muslims." Some don't want to deal with annoyances such as "drugs, kids or animals" or "smokers, kids or druggies," while others want to stay away from "psychos or anyone on mental medication." More friendly

---

8Roommate does not ask questions about race, nor does it categorize or channel the information based on racial preferences. Yet, the logic of its position—that it is protected by the CDA for its activities because they are based on answers from its members—would protect it (or one of its competitors), if it did. Thus, if a hypothetical website required members to identify themselves by race, under Roommate's logic, the CDA would protect this site if it prevented members who listed themselves as "African-American" or "Asian" from viewing any "Whites Only" listings. We doubt this is what Congress had in mind when it passed the CDA.
folks are just looking for someone who will get along with their significant other\textsuperscript{10} or their most significant Other.\textsuperscript{11}

[9] We conclude that Roommate’s involvement is insufficient to make it a content provider of these comments. Roommate’s open-ended question suggests no particular information that is to be provided by members; Roommate certainly does not prompt, encourage or solicit any of the inflammatory information provided by some of its members. Nor does Roommate use the information in the “Additional Comments” section to limit or channel access to listings. Roommate is therefore not “responsible, in whole or in part, for the creation or development of” its users’ answers to the open-ended “Additional Comments” form, and is immune from liability for publishing these responses. 47 U.S.C. § 230(c), (f)(3); see also Batsel, 333 F.3d at 1031.

* * *

Having determined that the CDA does not immunize Roommate for all of the content on its website and in its email newsletters, we remand for a determination of whether its non-immune publication and distribution of information violates the FHA, 42 U.S.C. § 3604(c). We also vacate the dismissal of the state law claims so that the district court may reconsider whether to exercise its supplemental jurisdiction in light of our ruling on the federal claims. Fredenburg v. Contra Costa County Dep’t of Health Servs., 172 F.3d 1176, 1183 (9th Cir. 1999). We deny Roommate’s cross-appeal for attorneys’ fees and costs; as the Councils prevail on some of their arguments here, their case is perforce not frivolous.

\textsuperscript{10}“The female we are looking for hopefully wont [sic] mind having a little sexual encounter [sic] with my boyfriend and I [very sig].”

\textsuperscript{11}“We are 3 Christian females who Love our Lord Jesus Christ . . . . We have weekly bible studies and bi-weekly times of fellowship.”
REVERSED in part and REMANDED.

REINHARDT, Circuit Judge, concurring in part and dissenting in part:

I join Judge Kozinski's opinion for the court, except for its holding that the Communications Decency Act (the "Act"), 47 U.S.C. § 230(c), immunizes Roommate from liability with respect to the statements contained in the "Additional Comments" section of users' profiles, some of which expressly state the preferences of landlords for tenants based on race, religion, gender, sexual orientation, and national origin. I would hold instead that none of the information that the Fair Housing Councils of San Fernando Valley and San Diego ("Councils") challenge satisfies the test for § 230(c) immunity.

Roommate cannot receive § 230(c) immunity for publishing information in the "Additional Comments," if it is "responsible . . . in part, for the . . . creation or development of

1A member with the profile name "BLKMAIL4U" states that "The person applying for the room MUST be a BLACK GAY MALE." (emphasis added).

2A member with the profile name "sassy1lady" states that "This is a Christian home and we are looking for a Christian female to rent a downstairs room." (emphasis added).

3A member with the profile name "mrtoy2001" states that "I am looking for sex starved women who are wanting to get that funny familiar forgotten feeling all over again. The better I can make you feel, the better I feel. I don't know about you but I am ready to feel real good. My goal is to PLEASE YOU." (emphasis added).

4A member with the profile name "happyheart" states that "I am looking for a neat freak, christian, non smoking, straight, friendly female to share an apartment with. I am all of the above." (emphasis added).

5A member with the profile name "bali" states that "I am looking for asian/spanish persons to share the apartment." (emphasis added).
information.” § 230(c), (f)(3); see also Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003). The court’s opinion here sets forth two independent tests to determine whether Roommate, an interactive computer service, is responsible in part for creating or developing information under § 230(c): first, whether Roommate categorizes, channels and limits the distribution of information, thereby creating another layer of information, Op. at 5721-22, 5723; and second, whether Roommate actively prompts, encourages, or solicits the unlawful information. Id. at 5720, 5723. Meeting either test results in a computer service’s inability to obtain § 230(c) immunity. Unlike Judge Kozinski, I would hold that Roommate’s conduct with respect to statements in the “Additional Comments” satisfies both tests, and, thus, that Roommate is not immune for publishing that information.

I. Because Roommate Categorizes, Channels, and Limits Complete User Profiles, Which Include the Statements in the “Additional Comments,” Roommate is Responsible for Creating or Developing the Information

The court’s opinion draws a distinction between (1) the statements in the “Household” and “Preferences” portions of users’ profiles, which consist of users’ responses to specific questions about their identities and preferences for tenants on the basis of gender, familial status, and sexual orientation, and (2) the statements in the “Additional Comments” portion of the profiles, which consist of users’ free-form responses, and which in many instances contain preferences based on race, religion, and national origin, and in others expand upon the answers with respect to the preferences listed in the preceding portion of the profiles. It holds that Roommate is not immune for statements in the earlier portions but it is for statements in the “Additional Comments” portion. Op. at 5722-23.

While I agree with Judge Kozinski’s reasons for rejecting immunity for statements in the “Household” and “Preferences” portions — that “[b]y categorizing, channeling and
limiting the distribution of users' profiles, Roommate provides an additional layer of information that it is 'responsible' at least 'in part' for creating or developing,' Op. at 5722 (citations omitted). — I would hold that this principle applies to statements in the "Additional Comments" portion as well. I would do so because the "Additional Comments" portion is an integral part of the entire "users' profiles," which Roommate categorizes, channels and limits in distribution." Id.

Roommate does not display the different portions of a user's profile in distinct e-mails or web pages, but instead aggregates an entire profile and presents it as a whole. Thus, when Roommate "provides an additional layer of information" by channeling the completed "user profiles," id., that additional layer of information includes the "Additional Comments" section with the various responses. Accordingly, Roommate should not be afforded immunity for any of the statements contained in the profile. In other words, the information that we should examine for the purpose of § 230(c) immunity should be the entire profile presented in the single e-mail or web page, including all of the statements therein. There is no justification for slicing and dicing into separate parts the material that Roommate elicits and then channels as an integral part of one package of information to the particular customers to whom it selectively distributes that package.

This view is supported by Batzel, in which we stated that to "meet[] the definition of 'information content provider' [in § 230(f)(3)] with respect to the information in question," the "pertinent question" is whether the interactive computer service "can also be considered to have 'creat[ed]' or 'develop[ed]' [the] e-mail message forwarded to the listserv." 333 F.3d at 1031 (emphasis added). Critically, we considered the "information in question" to be the entire "e-mail message," and not merely selected sentences in the e-mail which the plaintiff had identified as defamatory. Similarly, here, the "information in question" is the entire e-mail or web page,
i.e., the complete profile. By channeling, categorizing and limiting distribution of the complete profile to the particular members who qualify to receive it, Roommate is responsible in part for creating and developing the entire profile.

Because I conclude that the first test for determining whether Roommate is responsible in part for creating or developing the information is satisfied with respect to the entire user profile, including the statements in the “Additional Comments,” I would hold that Roommate cannot receive § 230(c) immunity for those statements.8

II. Because Roommate Encourages, Solicits and Prompts its Users to Make Discriminatory Statements in the “Additional Comments” it is Responsible for Creating or Developing Those Statements

I would also hold that under the court’s second test Roommate similarly lacks § 230(c) immunity for the statements contained in the “Additional Comments.” Contrary to the conclusion in Judge Kozinski’s opinion that Roommate “does not prompt, encourage or solicit any of the inflammatory information provided by some of its members” in the “Additional Comments” portion of their profiles, the record amply demonstrates that it does. Op. at 5723.

On the final page of the sign-up process in which prospective users create their profiles, Roommate’s site states, “We strongly recommend taking a moment to personalize your

8I disagree with the court’s conclusion that “Roommate’s involvement is insufficient to make it a content provider” of the information in the “Additional Comments” portion of the profiles because Roommate does not “use the information in the ‘Additional Comments’ section to limit or channel access to listings.” Op. at 5723. If Roommate is responsible even in part for creating or developing the entire profile, as Judge Kozinski’s opinion makes clear, it is irrelevant that Roommate uses only the statements in the “Preferences” and “Household” portions to guide its categorization decisions.
profile by writing a paragraph or two describing yourself and what you are looking for in a roommate” directly above a blank box. This page immediately follows the “My Roommate Preferences” form, which explicitly asks members to provide their preferences based on gender, sexual orientation and familial status. Judge Kozinski concludes that the “open-ended” recommendation on the “Additional Comments” page “suggests no particular information that is to be provided by members.” Op. at 5722. However, when viewed in the context of the entire sign-up process that conveys the message to prospective users that they should express their preferences for tenants based on race, gender, sexual orientation, national origin and religion, ordinary users would understand the recommendation to constitute a suggestion to expand upon the discriminatory preferences that they have already listed and to list their additional discriminatory preferences in that portion of the profile.

This conclusion finds both subjective and objective support in the record. From a subjective perspective, Roommate’s site is designed so that users will express illicit preferences in their “Additional Comments.” The executive who created the site acknowledges that he intended that users would express preferences in their profiles that can only be mentioned in the “Additional Comments” portion, such as religion. See Declaration of Bryan Peters (“Some Roommate.com users have religious beliefs that impact their selection of roommates. Many are Christians . . . . By referencing these beliefs in their profiles, users avoid the need to contact and interview dozens of incompatible people.”).

Turning to the objective evidence of Roommate’s solicitation, the best evidence of how users perceive the web site generally and the “Additional Comments” section specifically, is the myriad discriminatory statements that users have written in that section. The statements in notes 1 through 5, such as “The person applying for the room MUST be a BLACK GAY MALE,” and the others relating to religious, racial, and gen-
der preferences, are representative of the numerous “Additional Comments” expressing such preferences. Additionally, the web site displays testimonials that suggest to potential users that they are free to obtain “suitable” tenants by listing discriminatory preferences — preferences that can only be set forth in the “Additional Comments.” The site also invites prospective users to preview its search mechanism, thereby exposing them to user profiles that prominently display “nicknames” such as Christianldy, Chinesegirl, Whiteboy73, africanboy, Latinagirl, gaycouple, blackbarbie. By having its search mechanism display these nicknames to prospective users, Roommate suggests that it is desirable, as well as permissible, to use the profiles to achieve discriminatory goals. The site even displays a sample of a completed profile — linked from the front page — that includes a discriminatory preference in the first sentence of the “Additional Comments” section, illustrating how users may express similar preferences in their own profiles. Finally, by placing the “Additional Comments” form directly after the forms in which users must express their “identities,” and in which they are asked to state their preferences with respect to gender, sexual orientation and familial status, the site strongly suggests that the “strong recommend[ation]” to “describ[e] yourself and what you are looking for in a roommate” is in essence an invitation to elaborate on discriminatory preferences already listed and to list others such as race, religion, or national origin.

In light of the objective and subjective evidence that Roommate solicits users to set forth discriminatory requirements in their “Additional Comments,” I conclude that Roommate is not immune under § 230(c), and, at the very least, there is a genuine dispute of material fact as to this question. Accordingly, in no event is partial summary judgment in favor of Roommate appropriate.
IKUTA, Circuit Judge, concurring in part:

I concur in sections one and three of the majority opinion and its holding, but write separately to express my disagreement with section two.

Section 230(f)(3) defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3). Although "[s]ection 230 does not preclude joint liability for the joint development of content," the present case does not require us to determine what types of conduct would make a website operator a joint information content provider. *Blumenthal v. Drudge*, 992 F. Supp. 44, 50 (D.D.C. 1998) (holding that AOL was immune from suit under the CDA, despite contracting with, and promoting the activities of, a gossip columnist and rumor monger, in the absence of evidence that AOL "had some role in writing or editing the material" in the gossip column). Therefore, there is no need for the majority's discussion of this issue. Indeed, the majority agrees that its tentative considerations in section two regarding "the outer limits of Carafano's protection of websites" represents a task that we "need not undertake...today." In light of this acknowledgment, the majority's thoughts are unnecessary and not intended to bind future courts.

Moreover, I disagree with the direction the majority is heading in section two when it explores a possible interpretation of "information content provider." We have previously rejected expansive interpretations of this phrase and have explicitly held that a website operator does not become an information content provider by soliciting a particular type of information or by selecting, editing, or republishing such information.

For example, in *Carafano v. Metrosplash.com, Inc.*, we rejected a district court's determination that Matchmaker's
role in soliciting specific information made it an information content provider and not entitled to CDA immunity under section 230(c). 339 F.3d 1119, 1124 (9th Cir. 2003) aff'g on other grounds 207 F. Supp. 2d 1055 (C.D. Cal. 2002). The district court noted that Matchmaker had solicited responses to a questionnaire with “sexually charged” multiple-choice questions and answers such as “Finally, why did you call?... Scouting out for swinging couples... Looking for a one-night stand.” 207 F. Supp. 2d at 1060, 1066. The district court reasoned that by providing such a tailored questionnaire, “Matchmaker contributed[d] to the content of the profiles” and thus was partly responsible “for the creation or development of information contained in the profiles.” Id. at 1067 (internal quotation marks omitted). We disagreed, indicating that a website operator is not an “information content provider” unless it provides the “essential published content.” 339 F.3d at 1124. We stated:

Under § 230(c), therefore, so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process. The fact that some of the content was formulated in response to Matchmaker’s questionnaire does not alter this conclusion. Doubtless, the questionnaire facilitated the expression of information by individual users. However, the selection of the content was left exclusively to the user.

Id.

We have also rejected the position that a website operator becomes an “information content provider” if it intentionally selects, edits, and publishes defamatory information. In Batzel v. Smith, we upheld the immunity of a website operator dedicated to “museum security and stolen art,” who had received an allegedly defamatory email on this topic, and subsequently edited and republished it on the website. 333 F.3d 1018, 1021
(9th Cir. 2003). We disagree with the analysis of the dissent in that case, which would have held that the website operator was an information content provider because

[a] person’s decision to select particular information for distribution on the Internet changes that information in a subtle but important way: it adds the person’s imprimatur to it.... Information that bears such an implicit endorsement is no longer merely the “information provided by” the original sender. 47 U.S.C. § 230(c)(1). It is information transformed. It is information bolstered, strengthened to do more harm if it is wrongful. A defendant who has actively selected libelous information for distribution thus should not be entitled to CDA immunity for disseminating “information provided by another.”

Id. at 1038-39 (Gould, J., concurring in part and dissenting in part).

Avoiding this broad interpretation of “information content provider,” we held that immunity from “publisher” liability necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message.” Id. at 1031. We noted that “[o]ther courts have agreed that the exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content do not transform an individual into a content provider within the meaning of § 230.” Id. at 1031 n.18 (internal quotation marks omitted); see also Barrett v. Rosenthal, 146 P.3d 510, 528 (Cal. 2006) (relying on Banzel in reaching its conclusion that “[a] user who actively selects and posts material based on its content fits well within the traditional role of ‘publisher’ ” and that “Congress has exempted that role from liability”). Although not expressly addressed by our case law, a “publisher’s traditional editorial functions” also include seeking out and specializing in a specific type of
publication, just as in *Batzel*, where the website operator operated a website dedicated to a specific topic (museum security and stolen art). *Batzel* did not suggest that this fact made the operator an information content provider.

In sum, our binding precedent has already addressed the question when a website operator has jointly created and developed content so as to become an “information content provider.” Unless a website operator directly provides “the essential published content,” *Carafano*, 339 F.3d at 1124, it is not an “information content provider.” The result is robust immunity under section 230(c).
§ 311.6

It is 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 in 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. Violations will be subject to enforcement through civil penalties (as adjusted for inflation pursuant to § 1.38 of this chapter), imprisonment, and/or injunctive relief in accordance with the enforcement provisions of Section 555 of the Energy Policy and Conservation Act (42 U.S.C. 6905).


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 on 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 Reversibility.


SOURCE: 64 FR 56911, Nov. 8, 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.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting that children submit personal information online;

(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator’s records; or

(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.

Commission means the Federal Trade Commission.

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

Disclosure means, with respect to personal information:

(a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this 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. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 46).

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.

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

(a) Receives notice of the operator’s personal information collection, use, and disclosure practices; and

(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that
§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 models, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition; evidence regarding the intended audience; and whether a site uses animated characters and/or child-oriented activities and incentives.

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

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

(e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§312.8).

§312.4 Notice.

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

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

(i) 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 such area.

(ii) Content of the notice. To be complete, the notice of the website or online service’s information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service.
Provided that: the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;

(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, 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 operator; and that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties;

(v) That the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity; and

(vi) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

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

(i) Content of the notice to the parent. (i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

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

(iii) In the case of a notice under the exception in §312.5(c)(3), the notice must also state the following:

(A) That the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;

(B) That the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in §312.5(c)(4), the notice must also state the following:

(A) That the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;

(B) That the parent may refuse to permit the use of the information and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose stated in the notice.
§ 312.5 Parental consent.

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

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

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

(2) Methods to obtain verifiable parental consent that satisfy the requirements of this 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 confirmation 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(f), 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:

(1) Used for the sole purpose of protecting the child's safety;
Federal Trade Commission

(iii) Not used to recontact the child or for any other purpose;

(iv) Not disclosed on the website or online service; and

(v) Where the operator collects a child’s name and online contact information and such information is not used for any other purpose, to the extent reasonably necessary:

(1) To protect the security or integrity of its website or online service;

(2) To take precautions against liability;

(3) To respond to judicial process; or

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

(64 FR 69911, Nov. 3, 1999, as amended at 67 FR 18233, Apr. 17, 2002)

§312.5 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:

(1) Ensure that the requestor is a parent of that child, taking into account available technology; and

(2) 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 (18 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:

(a)
United States Court of Appeals
For the First Circuit

No. 02-2138

IN RE PHARMATRAK, INC. PRIVACY LITIGATION,

NOAH BLUMOFRE, 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. Cachwind, 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 web site 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 HTML³ 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 server⁴ (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 Detrol 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 against Pharmatrak; its parent company, Glocal Communications, Ltd.; and five pharmaceutical companies: American Home Products Corp., Glaxo Wellcome, Inc.,

13 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

\textsuperscript{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. \textit{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. Sueño 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. Segreta, 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).
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 Detroil 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 Nix 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). 16 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

-22-
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.

-23-
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 Distas., 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,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.
Social Networking Sites and the Law
Professor Eric Goldman (egoldman@gmail.com)
Santa Clara University School of Law
May 2007

1. Legal Liability of Users

Social networking sites enable users to publish content. Users may not consider themselves content publishers (especially when they write mundane/brief postings), but they are. Publishing content can create a number of legal issues, such as defamation (making harmful false statements about someone else) or copyright infringement. In this respect, social networking sites don't create any "new" legal issues; users who publish content can be liable for their publication choices just like other content publishers, such as newspapers or magazines.

Question to Consider: Assume that most users don’t know the laws applicable to publishing content. Should they be less liable for their publication choices than more knowledgeable content publishers, like newspapers or magazines?

Users often believe that they have some degree of anonymity for their statements and actions on social networking sites, and in some cases they try to hide their true identity. However, users' identities often can be easily revealed through legal processes. Sometimes, users suffer adverse consequences due to their social networking site, such as school discipline, foregone job offers or employment termination.

Questions to Consider: Should it be easy or hard for harmed parties to discover users’ identities? Should site operators cooperate with plaintiffs or resist their information requests on behalf of their users? When is it appropriate to take adverse actions against a user outside of the courtroom based on the user's social networking activity?

2. Legal Liability of Social Networking Site Vendors

Congress generally protects site vendors from legal liability for user-supplied content. 17 USC §512(c) says that vendors generally aren't liable for user-supplied copyright infringing content unless the copyright owner notifies the vendor and the vendor fails to promptly remove the infringing content. 47 USC §230(c)(1) says that vendors aren’t liable under any circumstance for other types of legal claims based on users’ content (with minor exceptions).

Questions to Consider: What legal responsibility, if any, should vendors have for user-supplied content? Should it matter if vendors (a) receive notice from a harmed party (or are otherwise aware of the problem) and don’t act, or (b) regularly remove user content based on their own editorial standards? Are social networking sites different from other communications media, such as telephones, newspapers or broadcasters?

Some legislators are concerned about the presence of sexual predators on social networking sites, and they have proposed a variety of laws designed to restrict predator access to the sites.

Questions to Consider: What steps should vendors voluntarily take to protect users from sexual predators? What steps should vendors be legally required to take? What liability should vendors face if sexual predators use the site to find and communicate with victims?
The Law of Social Networking Sites

Statutes

17 USC §512(c): a website isn’t liable for hosting user copyright-infringing content unless the website receives a notice from the copyright owner and fails to promptly remove the content.

47 USC §230(c)(1): “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.”

Virginia HB 2749/SB 1071 (enacted April 10, 2007): sexual offenders must register their email addresses and IM screen names, and the police may set up a mechanism for online businesses to check these registries.

Selected Cases

A.B. v. State, 863 N.E. 2d 1212 (Ind. Ct. App. April 9, 2007) (student posting obscenity-laden comments to a fake MySpace page isn’t guilty of criminal harassment because comments were protected political speech).


The Football Association Premier League Ltd v. YouTube, Inc., 1:07-cv-03582-UA (S.D.N.Y. complaint filed May 4, 2007) (can copyright owners bypass the 512(c) notification scheme?)


Viacom International, Inc. v. YouTube, Inc. (S.D.N.Y. complaint filed March 13, 2007) (does YouTube qualify for 512(c) safe harbor for user-posted copyright infringing material?).

Proposed Federal Statutes

Deleting Online Predators Act of 2007 (H.R. 1120/S. 49) (requiring schools/libraries receiving federal funds to block minors’ unrestricted access to social networking sites and chatrooms).

KIDS Act of 2007 (H.R. 719/S. 431) (requiring sexual predators to register their email addresses and other screen names and enabling social networking sites to access those electronic identifiers so that the sexual predators can be blocked from registering with the social networking sites).

H. Res. 224 (resolution requesting that social networking sites proactively remove “enemy propaganda from their sites,” such as videos made by terrorists).
Blog Law

Prof. Eric Goldman
Director - High Tech Law Institute
egoldman@gmail.com

What is a Blog?

- People have been “blogging” since the Internet’s beginning
- Blog = “a web-based publication consisting primarily of periodic articles” (Wikipedia Apr. 2006)
  - Postings in reverse chronological order
  - No third party editors
  - RSS feed
The Blogging Phenomenon

- 70M+ Blogs (TechCrunch: April 2007)
  - 1.4 new blogs every second
  - 1.5M new posts every day
- Boing Boing claims 1.7 million unique readers/day (Open and Shut? Interview with Cory Doctorow, April 2006)
- Blogs influence MSM...
- ...and MSM is becoming more bloggy
- RSS has become an important channel to users' desktops
Blogs and Publishing

- Blog law = publishing law
- Major blogger liability concerns
  - Defamation
  - Invasion of privacy (ex: Steinbuch v. Cutler)
  - Copyright infringement
  - Trade secret misappropriation

Blogs and Publishing

- Selected blog-specific legal issues (non-IP)
  - Blogs as journalists
  - Blogs as advertising
    - Lawyer blogs regulated as advertising
  - Blogs and election laws
  - Blogs, anonymity and retaliation (e.g., "dooced")
## Blogs and Publishing

- **47 USC 230 eliminates most non-IP claims based on third party content**
  - "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"
  - Scienter and editorial control irrelevant
    - Perfect 10 v. ccBill (9th Cir. 2007) extends 230 to state IP claims

## Blogs and IP

- **Bloggers as Copyright Defendants**
  - Ex: Perez Hilton
  - 17 USC 512
- **Bloggers as Copyright Plaintiffs**
  - Splogs and aggregators
  - Creative Commons license
- **Bloggers as Trademark Defendants**
  - Ex: BidZirk v. Smith (4th Cir. 2007)
- **Bloggers as Trademark Plaintiffs**
- **Blogs and Trade Secrets/Patents**
## Group/Guest Blogging

- **Legal issues**
  - Liability
  - Legal compliance
  - Asset disposition

- **Legal paradigms**
  - Partnership
  - Employment
  - Contribution to collective work
  - Joint work

- **Proactive steps**
  - Form entity/joint blogger agreement
  - 512 registration
  - Investigate insurance options

## Blog Law Resources

- **EFF Legal Guide for Bloggers**
  - [http://www.eff.org/bloggers/lg/](http://www.eff.org/bloggers/lg/)

- **Bloggership Conference Papers**

- **Eric Goldman, Co-Blogging Law**

- **Eric Goldman, Blog Law Recap**

- **Eric Goldman Blogroll**
  - [http://www.bloglines.com/blog/ericgoldman](http://www.bloglines.com/blog/ericgoldman)
IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

JANE DOE, Individually and as Next Friend of
JULIE DOE, a minor,
Plaintiffs,

-vs-

MYSPACE, INC., and NEWS CORPORATION,
Defendants.

ORDER

BE IT REMEMBERED on the 1st day of February 2007, the Court held a hearing in the
above-styled cause, to consider Defendants MySpace, Inc. and News Corporation's ("MySpace")
Motion to Dismiss [#6, 7, 15, 16, 36], Plaintiffs' responses thereto [#13, 14, 38], and Defendants'
reply thereto [#20]. Having considered the motion, the responses, the replies, the arguments of
counsel at the hearing, the relevant case law, and the case file as a whole, the Court now enters the
following opinion and orders.

Background

MySpace.com is the most visited web site in the United States, and it is owned by Defendant
MySpace, Inc.2 MySpace.com is a "social networking web site" that allows its members to create
online "profiles," which are individual web pages on which members post photographs, videos, and

1 News Corporation, the parent company of MySpace, Inc., asserts the same motion to dismiss and
adopts the arguments and reasoning presented by MySpace, Inc.; therefore, for purposes of this Order, a
reference to MySpace and its arguments is actually a reference to both MySpace, Inc. and News Corporation.

2 Defendant MySpace, Inc. is wholly owned by Fox Interactive Media, Inc., a subsidiary of
Defendant News Corporation.
information about their lives and interests. The idea of online social networking is that members will use their online profiles to become part of an online community of people with common interests. Once a member has created a profile, she can extend "friend invitations" to other members and communicate with her friends over the MySpace.com platform via e-mail, instant messaging, or blogs.

MySpace.com is free to users who agree to the MySpace Terms of Use Agreement. Every new member of MySpace.com, including Julie Doe, agrees to be bound by the MySpace.com Terms of Service, by clicking a check box on the website. MySpace's Terms of Service provide that MySpace cannot verify the age or identity of MySpace.com members and cautions members not to provide "telephone numbers, street addresses, last names, URLs or email addresses" to other members.

According to Plaintiffs' Verified Complaint, Julie Doe created a MySpace profile when she was 13 years old. At the hearing, Plaintiffs' counsel admitted that Julie Doe lied about her age and represented that she was 18 years old when she joined MySpace.com. Plaintiffs allege Pete Solis, a nineteen-year-old, initiated contact with Julie Doe, then fourteen years old, through MySpace.com on April 6, 2006. Subsequently, Julie Doe provided Pete Solis with her telephone number and the two communicated over the phone for several weeks. At some point, Julie Doe and Pete Solis arranged to meet for a date on May 12, 2006. Plaintiffs allege that during that meeting Pete Solis sexually assaulted Julie Doe. On May 13, 2006, Jane Doe, Julie's mother, called the Austin Police Department to report the sexual assault of her daughter. Pete Solis was subsequently arrested and indicted by the Travis County District Attorney's Office for Sexual Assault, a second degree felony.

3 MySpace.com requires that a user be at least fourteen years old to use their services.
This case was filed in Bronx County, New York, on September 26, 2006, and subsequently removed to the United States District Court for the Southern District of New York on September 29, 2006. The Honorable Miriam Goldman Cedarbaum of the United States District Court for the Southern District of New York transferred the case to this Court, pursuant to 28 U.S.C. § 1404(a), on December 1, 2006. Plaintiffs' Verified Complaint, the live pleading in this case filed in Bronx County, New York, asserts the following causes of action against Defendants: negligence, gross negligence, fraud, and negligent misrepresentation.

I. Defendants’ Motion to Dismiss

MySpace moves to dismiss this case with prejudice pursuant to Federal Rule of Civil Procedure 12(b)(6) and 9(b). Defendants assert they are immune from this suit under the Communications Decency Act of 1996. Defendants also assert Plaintiffs’ negligence claims fail under the common law and Plaintiffs’ fraud and negligent misrepresentation claims do not satisfy the heightened pleading standard of Federal Rule of Civil Procedure 9(b).

A. Communications Decency Act of 1996

The Communications Decency Act of 1996, 47 U.S.C. § 230 (the “CDA” or the “Act”), states that “[n]o 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). Neither party contests that MySpace is an “interactive computer service” as defined by the CDA, and it is clear that MySpace meets the statutory definition of such a service. See 47 U.S.C. § 230(f)(2). 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.” 47 U.S.C. § 230(f)(3). It is also clear that both
Julie Doe and Pete Solis qualify as "information content providers" with respect to their communications through MySpace.

In crafting Section 230, Congress made the following findings:

(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.


The policy underlying the CDA is the promotion of "the continued development of the Internet and other interactive computer services . . . ." 47 U.S.C. § 230(b)(1). To ensure that web site operators and other interactive computer services would not be crippled by lawsuits arising out of third-party communications, the Act provides interactive computer services with immunity. See Dimeo v. Max, 433 F. Supp. 2d 523, 528 (E.D. Pa. 2006) ("The provision 'precludes courts from entertaining claims that would place a computer service provider in a publisher's role,' and therefore bars '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.'") (quoting Green v. America Online, 318 F.3d 465, 471 (3d Cir. 2003); Zeran v. America Online, Inc.,
129 F.3d 327, 330 (4th Cir. 1997)). The CDA thus encourages web sites and other "interactive computer services" to create forums for people to exchange their thoughts and ideas by protecting web sites and interactive computer services from potential liability for each message republished by their services. See Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122–24 (9th Cir. 2003); Zeran, 129 F.3d at 330–31.

Several courts have construed the CDA to date. In Carafano, a case involving false online personal ad listings, which led to Christine Carafano’s receipt of sexually explicit phone calls, letters, and hand-delivered notes, the Ninth Circuit Court of Appeals held that the CDA granted the interactive service provider Matchmaker.com full immunity where a third party willingly provided the essential published content. 339 F.3d at 1124. The Ninth Circuit explained the policy underlying the CDA as follows:

The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Id. at 1124 (quoting Zeran, 129 F.3d at 330–31).

One of the most important and oft-cited cases to date is Zeran v. America Online, Inc. In Zeran, the victim of a vicious prank sued America Online, Inc. ("AOL") for failing to remove a false advertisement offering t-shirts featuring tasteless slogans related to the 1995 Oklahoma City bombing and instructing interested buyers to call the plaintiff to place an order. 129 F.3d at 329. After receiving death threats from people who were outraged by the ad, Zeran learned of the prank and demanded that AOL remove the ad from its bulletin board and post a retraction. Id. AOL failed
original ad, and the unidentified poster also posted several more ads listing the phone number. Id. A local radio station learned of the ads and encouraged its listeners to call. Id. The volume and intensity of the threats became so severe that local police guarded Zeran's home to protect his safety. Id.

Zeran sued AOL for negligence because it failed to remove the ad after specific notice of its falsity and allowed the third party to post additional ads after Zeran had put AOL on notice of his harassment and bodily danger. The Fourth Circuit affirmed the dismissal of the claims on the pleadings, explaining that the CDA necessarily protects interactive computer services from liability even after they are notified of an allegedly defamatory or threatening post because the insupportable legal burden imposed by potential tort liability would undermine the CDA's goal of promoting speech on the Internet. Id. at 330. The Court explained that "[b]y 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." Id. In enacting the CDA, "Congress made a policy choice . . . 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." Id. at 330-31.

Despite Plaintiffs' arguments to the contrary, the Court finds Zeran and its rationale to be applicable to the case at hand. Here, Plaintiffs seek to impose tort liability on MySpace, a company that functions as an intermediary by providing a forum for the exchange of information between third party users. Plaintiffs' allegations that MySpace knew sexual predators were using the service to communicate with minors and failed to react appropriately can be analogized to Zeran's claims that
AOL failed to act quickly enough to remove the ads and to prevent the posting of additional ads after AOL was on notice that the content was false.

Plaintiffs contend the CDA is inapplicable to their claims, so Defendants should not be granted immunity under the CDA. Plaintiffs assert Section 230(c)(1) is inapplicable here because Plaintiffs have not sued MySpace for the publication of third-party content but rather for failing to implement basic safety measures to prevent sexual predators from communicating with minors on MySpace. Plaintiffs attempt to distinguish Carafano, Zeran, and Prickett v. Info USA, Inc., No. 4:05-CV-10, 2006 WL 887431 (E.D. Tex. Mar. 30, 2006), from the case at hand, by pointing out that each of these cases was based on the listing of third-party content without taking into account its defamatory or inaccurate nature. Plaintiffs assert their case is not based on MySpace's posting of third-party content, but rather on MySpace's failure to institute safety measures to protect minors.

Plaintiffs seek to limit CDA immunity to cases involving defamation or related actions and assert that their claims against MySpace have nothing to do with the content of the information provided. Plaintiffs contend that neither the plain language of the CDA nor the cases interpreting it contemplate the extension of the CDA's immunity provision to MySpace in this case.

Nothing on the face of the statute supports Plaintiffs' narrow interpretation that the CDA's immunity applies only to cases involving defamation and defamation-related claims. 47 U.S.C. § 230. The Eastern District of Texas recently addressed the application of CDA immunity in a case involving claims of negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy, and distribution of child pornography. Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006). This case dealt with a lawsuit against Yahoo! Inc., which arose from an e-group hosted by Yahoo! on which illegal child
pornography pictures were posted by a third party. Among the photos were sexually explicit photos of Johnny Doe, a minor. The district court determined that Section 230(c)(1) applied to immunize Yahoo! because Plaintiffs' claims sought to treat Defendant as the "publisher or speaker" of the third-party content (the photos). Id. at *2-4. It is important to note that in Bates, as here, the Plaintiffs did not allege that there was anything defamatory or inaccurate about the posted content, but the court still applied the CDA to immunize Yahoo! from suit.

Defendants have presented numerous cases in which the CDA has been applied to bar non-defamation claims. See, e.g., Ben Ezra, Weinstein & Co. v. America Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000) (negligence claim); Zeran, 129 F.3d at 330 (negligence claims); Bates, 2006 WL 3813758 at *5 (negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, civil conspiracy and distribution of child pornography); Beyond Sys., Inc. v. Keynetics, Inc., 422 F. Supp. 2d 523, 536 (D. Md. 2006) (claim under Maryland Commercial Electronic Mail Act); Barnes v. Yahoo!, Inc., No. Civ. 05-926-AA, 2005 WL 3005602, at *4 (D. Or. Nov. 8, 2005) (negligence claim resulting in personal injury). All of these cases involved attempts to hold an interactive computer service liable for its publication of third-party content or harms flowing from the dissemination of that content.

Plaintiffs argue the CDA does not bar their claims against MySpace because their claims are not directed toward MySpace in its capacity as a publisher. Plaintiffs argue this suit is based on MySpace's negligent failure to take reasonable safety measures to keep young children off of its site and not based on MySpace's editorial acts. The Court, however, finds this artful pleading to be

---

4 Rather, the Plaintiffs in Bates alleged Yahoo! knowingly hosted illegal child pornography on its e-group and that Yahoo! should have prevented, removed, and/or blocked the illegal child pornography from its website. Id. at *20.
disingenuous. It is quite obvious the underlying basis of Plaintiffs' claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs assert they never would have met and the sexual assault never would have occurred. No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities. Therefore, in accordance with the cases cited above, Defendants are entitled to immunity under the CDA, and the Court dismisses Plaintiffs' negligence and gross negligence claims with prejudice under rule 12(c) of the Federal Rules of Civil Procedure.  

i. Self-Regulation

In addition to the protection afforded to interactive computer services in their publishing capacity, the CDA also immunizes such services from liability based on efforts to self-regulate material. Specifically, "[n]o 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 consents to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ." 47 U.S.C. § 230(c)(2)(A). This section reflects Congress's recognition that the potential for liability attendant to implementing safety features and policies created a disincentive for interactive computer services to implement any safety features or policies at all. To the extent Plaintiffs seek to hold MySpace liable for ineffective security measures

---

5 Although Defendants moved to dismiss Plaintiffs' claims based on Federal Rule of Civil Procedure 12(b)(6), the Court may construe such a motion to a motion for judgment on the pleadings under Rule 12(c). Jones v. Greninger, 188 F.3d 322, 324 (5th Cir. 1999).
and/or policies relating to age verification, the Court alternately finds such claims are barred under § 230(c)(2)(A).

B. Duty to Protect under Texas Law

Under Texas Law, to state a claim for negligence or gross negligence, Plaintiffs must allege the existence of a duty, a breach of that duty, and damages proximately caused by the breach. *Western Invs., Inc. v. Urena*, 162 S.W.3d 547, 550 (Tex. 2005). Defendants assert Plaintiffs have failed to state a claim for negligence or gross negligence because MySpace had no legal duty “to institute and enforce” security measures that would substantially decrease the likelihood that Julie Doe would be sexually assaulted. “The existence of a duty is a question of law for the court to decide from the facts surrounding the occurrence in question. As a general rule, a person has no legal duty to protect another from the criminal acts of a third person or control the conduct of another.” *Walker v. Harris*, 924 S.W.2d 375, 377 (Tex. 1996) (internal citations omitted); accord *Greater Houston Transp. Co. v. Phillips*, 801 S.W.2d 523, 525 (Tex. 1990) (“Generally, there is no duty to control the conduct of third persons.”).

The general rule of course has exceptions, such as when a special relationship exists between the actor and the third person, which special relationship imposes a duty upon the actor to control the third person’s conduct. *Phillips*, 801 S.W.2d at 525. These special relationships include the relationship between: (1) employer and employee; (2) parent and child; and (3) independent contractor and contractee under special circumstances. *Id.* Plaintiffs have alleged no such special relationship between MySpace and either Pete Solis or Julie Doe. Here the alleged sexual assault

---

6 The Court finds Plaintiffs' claims particularly unwarranted here given that Julie Doe lied about her actual age to bypass the age requirement and then violated MySpace's express rules by giving out her personal information.
happened offline, after telephone conversations offline, and there is no allegation MySpace was in control of the premises where the crime occurred.\textsuperscript{7} Defendants assert Plaintiffs have failed to state a claim for negligence or gross negligence because MySpace had no legal duty to prevent the alleged sexual assault.

Plaintiffs respond that MySpace had a duty to institute reasonable safety measures to protect minors from sexual predators because it was foreseeable that minors such as Julie Doe could be injured by the criminal acts of adult MySpace users. \textit{Walker}, 924 S.W.2d at 377 (stating that premises owners have a duty to protect persons injured by the criminal acts of third parties on their premises if the criminal acts were foreseeable). “Foreseeability requires only that the general danger, not the exact sequence of events that produced the harm, be foreseeable.” \textit{Id.} (citing \textit{Lofton v. Texas Brine Corp.}, 777 S.W.2d 384, 387 (Tex. 1989)). Plaintiffs also cite \textit{Rodriguez v. Moerbe}, 963 S.W.2d 808, 817 (Tex. App.--San Antonio 1998, no pet.), as recognizing the exception to the no duty rule for a third party’s criminal conduct that is the foreseeable result of the defendant’s negligence. Plaintiffs allege MySpace was on notice of several previous sexual assaults perpetrated by MySpace users against minor members; therefore, Julie Doe’s sexual assault was the foreseeable result of MySpace’s negligent failure to take appropriate safety measures. Plaintiffs assert MySpace had a duty to institute reasonable safety measures to prevent contact between sexual predators and minors on its website.

However, the Court is unconvinced that any exception to the general no duty rule applies to MySpace here. Plaintiffs allege MySpace can be liable under a negligence standard when a minor

\textsuperscript{7} At the hearing counsel stated that the alleged sexual assault occurred in a parking lot in Travis County, Texas.
is harmed after wrongfully stating her age, communicating with an adult, and publishing her personal information. To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace’s business in its tracks and close this avenue of communication, which Congress in its wisdom has decided to protect. The Court declines to extend premises liability cases to the internet context particularly where, as here, the Defendant provides its service to users for free. Plaintiff has cited no case law indicating that the duty of a premises owner should extend to a website as a “virtual premises.” Although it is not controlling here, the Court finds the Seventh Circuit’s analysis of a similar case instructive.

Plaintiffs do not cite any case in any jurisdiction holding that a service provider must take reasonable care to prevent injury to third parties. Consider the Postal Service or Federal Express, which sell transportation services that could be used to carry harmful articles. As far as we can discover, no court has held such a carrier liable for failure to detect and remove harmful items from shipments. . . . Similarly, telephone companies are free to sell phone lines to entities . . . , without endeavoring to find out what use the customers make of the service . . . . Yet an ISP, like a phone company, sells a communications service; it enabled [the user] to post a web site and conduct whatever business [the user] chose. . . . Landlord, phone company, delivery service, and web host all could learn, at some cost, what [the user] was doing with the services and who was potentially injured as a result; but state law does not require these providers to learn, or to act as Good Samaritans if they do. The common law rarely requires people to protect strangers, or for that matter acquaintances or employees. States have enacted statutes to change that norm in some respects; Dram Shop laws are good examples. Plaintiffs do not identify anything along those lines concerning web hosts . . . .

Doe v. GTE Corp., 347 F.3d 655, 661 (7th Cir. 2003) (affirming district court’s dismissal of claims against internet services and web hosting services for hosting images of athletes who were

---

8 To date, MySpace has more than 100 million registered users worldwide, and it is the most visited website in the United States, as previously noted.
unknowingly recorded unclothed in a locker room because web hosting services have no duty to investigate their clients' activities or to prevent potential injury that results therefrom).

Accordingly, the Court finds Plaintiffs have failed to state a claim for negligence or gross negligence because MySpace had no duty to protect Julie Doe from Pete Solis's criminal acts nor to institute reasonable safety measures on its website. If anyone had a duty to protect Julie Doe, it was her parents, not MySpace.9

C. Fraud and Misrepresentation

Defendants move to dismiss Plaintiffs' fraud and negligent misrepresentation claims for failure to state a claim on which relief may be granted because they do not meet the heightened pleading standard of Federal Rule of Civil Procedure 9(b). Rule 9(b) provides that "[i]n all averments of fraud or mistake, the circumstances constituting fraud or mistake shall be stated with particularity." FED. R. CIV. P. 9(b). "At a minimum, Rule 9(b) requires allegations of the particulars of 'time, place, and contents of the false representations, as well as the identity of the person making the misrepresentation and what he obtained thereby.'" Tel-Phonic Servs., Inc. v. TBS Int'l, Inc., 975 F.2d 1134, 1139 (5th Cir. 1992).

The Court agrees with Defendants that Plaintiffs have not plead their fraud and misrepresentation claims with sufficient particularity. Plaintiffs counsel also admitted in open court that Plaintiffs no longer wish to pursue their claims of fraud and misrepresentation because the real basis of their case is negligence. Accordingly, the Court dismisses Plaintiffs claims of fraud and negligent misrepresentation without prejudice pursuant to Federal Rule of Civil Procedure 9(b).

9 Having already determined that dismissal is proper on the foregoing bases, the Court need not reach the question of whether or not Plaintiffs' negligence and gross negligence claims should be dismissed based on a lack of proximate causation under the doctrine of "new and independent cause."
Conclusion

In accordance with the foregoing:

IT IS ORDERED that Defendants MySpace, Inc. and News Corporation’s Motion to Dismiss [#6, 7, 16, 36] is GRANTED; and

IT IS FURTHER ORDERED that Plaintiffs’ claims of negligence and gross negligence are DISMISSED WITH PREJUDICE and Plaintiffs’ claims of fraud and negligent misrepresentation are DISMISSED WITHOUT PREJUDICE.

SIGNED this the 13th day of February 2007.

[Signature]

SAM SPARKS
UNITED STATES DISTRICT JUDGE
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 CAN-SPAM preempts all laws expressly regulating the use of e-mail to send commercial messages (except laws that "relate to acts of fraud or computer crime"). CAN-SPAM Act, supra n. 1, at § 603(2)(B).
⁴ 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.
⁵ 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 understand- ing 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 best 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 Fowles, Pew Internet & American Life Project, Spam: How it is Hurt- ing 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 reasons 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 \<http://www.doubleclick.com/us/knowledge_central/documents/research/dc_consumere-mailstudy_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/spam/030429spamreport.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.18

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.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 spam18 and approximately thirty percent of those surveyed have responded to spam to get more information about the advertised product or service.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

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.

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-94710.html> (May 2, 2003) (citing a survey on npdor.com that seven percent “sometimes” buy from spam, plus another twenty-three percent “very rarely” buy).

19. See The Pew Report, supra n. 10, at ii-iii (thirty-three percent); Mailshell Survey, supra n. 7 (twenty-eight percent).
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 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 'wouldn't see it' when they see it"); see George Johnson, Sp@n Sm@n@nS!, 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[1] 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. 15 (discussing a heightened sense of privacy at home).
tory because it does not explain the seeming dichotomy between the out-
rage over spam and comparative tolerance of junk mail.

A more satisfying explanation can be found by considering the rela-
tive 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 develop-
ing 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. Meanwhile, new generations who grow up
using e-mail should be more tolerant of spam 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.

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 com-
pared to their reactions to other forms of annoying ads. Meanwhile, regu-
lation 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/
de_consumers-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).


29. See generally Stefanie Olsen, CNET News.com, Yahoo, Sendmail to Test Antispam
(discussing new e-mail sender authentication efforts such as DomainKeys, Sender Permit-
ted From, and caller ID for e-mail); Evan I. Schwartz, Spam Wars, Tech. Rev., at 32, 34-35
(Oct. 2003) (discussing technological solutions such as signature-based filtering, col-
1aborative filtering, gateway intercepts, heuristic filtering, Bayesian filtering, circles of
trust; and vaccinations); Hanah Metchis & Solveig Singleton, Spam, That Ill O’ the ISP: A
Reality Check for Legislators, Competitive Enterprise Institute 9-12 <http://www.ce.org/pdf/
3482.pdf> (May 21, 2003) (discussing technological solutions such as content filters, white-
lists, challenge-response systems, collaborative filtering, blacklists (also called “black
lists”), bonded sender programs and protocol redesigns); Ferris Research, Spam Control:
(Jan. 2003) (surveying the various anti-spam technology providers).
sequence is preventing minority interests from exchanging relevant content.

C. SPAMMERS IMPOSE 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, 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, and sometimes spam is likened to junk mail sent with postage due. 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, so consumer recipients do not pay for each e-mail received.

30. Privity 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.com.com/2100-1034_3-5079624.html?tag=st util_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. However, in Intel Corp. v. Hamidi, 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. It remains unclear how subsequent courts will interpret 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 Computer Fraud and Abuse Act ("CFAA") to combat spam. 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. 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 and by providing another basis (in addition to the CFAA) for federal court jurisdiction. As a result, CAN-SPAM should

---


35. 1 Cal. Rptr. 3d 32 (Cal. Sup. Ct. 2003).

36. Id. at 43.


38. CAN-SPAM Act, supra n. 1, at § 7(g).

39. Id. § 7(g)(2)(A).
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.\(^\text{40}\) Indeed, analysts claim that this lost time creates enormous costs.\(^\text{41}\) 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.\(^\text{42}\) Thus, forcing them to internalize the spam-created costs (rather than pushing those costs to a spammer) may motivate them to close the relays.\(^\text{43}\)

---

\(^{40}\) See Intel Corp. v. Hamdi, 1 Cal. Rptr. 3d 32.

\(^{41}\) See Nucleus Research, Spam: The Silent ROI Killer, Research Note D69 (http://www.nucleusresearch.com/research/d69.pdf) (accessed July 1, 2003) (claiming that employees have an average lost productivity of 1.4 percent per year, meaning that spam costs $974 per employee per year); Ferris Research, Spam Control: Problems and Opportunities 7, 16-17 (http://www.ferris.com/report/200301/report.pdf) (accessed Jan. 30, 2003) (“In 2002, the total cost of spam to corporate organizations in the United States was $8.9 billion,” of which fifty-four percent was attributable to lost productivity); Basesx, Spam E-mail and Its Impact on IT Spending and Productivity 5 (http://www.basesx.com/ptyc2003.nsf/6e67dc05617d699c8556e990065a0e7/BR761f74ab3706838356e040019f814BF7EB3esxReportSpam.pdf) (Dec. 2003) (“[the cost of spam to companies worldwide is ca. $30 billion and growing at almost 100% per year].” See generally Saul Hansell, Drowning Estimates of the Cost of Spam, N.Y. Times, at C1 (July 28, 2003) (discussing and critiquing these studies).


\(^{43}\) 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,46 so regulatory protection is appropriate. Indeed, thirty states prohibited forged headers,46 and these states

44. See id. at § 3(6) (defining “header information”).

45. Forged headers can be prevented only if e-mail senders are better authenticated. Project Lumos is being developed to tackle that problem. See Hans Peter Brandmo et al., E-mail Service Provider Coalition, Project Lumos: A Solutions Blueprint for Solving the Spam Problem by Establishing Volume E-mail Sender Accountability <http://www.networkadvertising.org/espa/Project_Lumos_White_Paper.pdf> (Sept. 24, 2003); see also Olsen, supra n. 25.


laws may not be preempted by CAN-SPAM.47 Meanwhile, CAN-SPAM
criminalizes forged headers48 and potentially sets up a private cause of
action for some victims ("providers of Internet access services" who are
"adversely affected").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 trade-
mark law and the CFMA,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 unsupported 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 fi-
nancial 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 under-
standing of the real costs borne by these parties would have likely pro-
duced a more thoughtful legal solution.

D. SPAM CONTAINS OR PROMOTES OBJECTIONABLE CONTENT

Many spam recipients complain about objectionable content of spam,
especially pornographic spam.51 Due to deep feelings towards pornog-
ography spam, Congress specifically targeted it in CAN-SPAM by requir-

---

47. See CAN-SPAM Act, supra n. 1, at § 3(b)(1) (state laws that "prohibit false or
deception in any portion of a commercial electronic mail message or information attached
thereto" are not preempted).
48. See id. §§ 4(a)(1), 5(a)(1).
49. See id. § 7(g)(1).
51. See The Pew Report, supra n. 10, at 44 ("in nearly every measure we tested, por-
nography 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); unsamp, Comprehensive Spam Survey (Oct. 2003) <http://www.unspamp.com/
first_spam_information/survey_oct2003.html> (Oct. 15, 2003) (ninety-six percent of par-
ents are looking to block pornographic spam from reaching their children); see also CAN-
SPAM Act, supra n. 1, at § 2(a)(3) (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 Communications 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.58

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 unconstitutional59 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,\(^60\) reflecting their weak policy underpinnings. Early feedback on CAN-SPAM suggests the federal law will not be any more effective.\(^61\)

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., 56% of Internet E-Mail is NOW Spam According to Anti-Spam Leader Brightmail\(^5\) <http://www.brightmail.com/pressreleases/082003_56-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 Cookie—Despite New Laws <http://news.com.com/2102-1024_3-5156632.html?tag=st.util.print> (Feb. 17, 2004) (“[l] U.S. Justice Department prosecutor warned Tuesday that a new spam law’s criminal sanctions likely will not stem the flow of bulk solicitations that are flooding 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 infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposely disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail purposely 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 messages 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 recipients 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 electronic 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 regulate 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 disparate 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—

(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.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE CONSENT.—The term "affirmative consent", 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 communicated 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) PROCUREMENT.—The term "procure", 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 1630(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 original 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 PREDATORY 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 5 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.
(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(e) 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
(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 fails 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 fails 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 in 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;
PUBLICATION OF THE MARYLAND MAGAZINE

15 USC 7705.

SEC. 6. BUSINESSES KNOWNLY 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

(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 proscribed 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 25 or 25A 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 466 of that Act (7 U.S.C. 238), 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. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association; 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, with the same jurisdiction, powers, 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 INJUNCTIONS 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 the Federal Communications Commission.
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) REQUISITE 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 “PROCURE”.—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-
mitted or attempted to be transmitted over the facilities
of the provider of Internet access service, or that is trans-
mitted 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-
mmitted 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 portion of a 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.
(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).

15 USC 7712.

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 (2);

(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.

15 USC 7713.

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.

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:

---

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;¹

(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;²

(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
I. INTRODUCTION


Presently before this Court are cross-motions for partial summary judgment. Both Plaintiff and Defendant seek summary judgment as to Counts I (Violation of CAN-SPAM), III (Violation of Section 17529.5) and VI (Breach of Contract).

II. FACTUAL BACKGROUND

The following facts are alleged by the parties:

Plaintiff is an online social networking service that allows members to create personal profiles in order to find and communicate with other people. Members of MySpace have access to the MySpace.com website, the MySpace.com Internet Messaging service, and the MySpace.com Mail service, where users can send and receive electronic mail messages ("MySpace e-messages").
To become a MySpace member, a person must set up an account on MySpace.com by creating a profile. The profile includes the user's name, country, zip code, birth date, and gender. The user must also create a password and provide an alternate email address to which confirmations and notifications will be sent. To set up an account, the user must assent to the MySpace Terms of Service Contract ("TOS Contract") by checking a box agreeing to the terms of the TOS Contract, and inputting a verification code. The TOS Contract prohibits spamming, automated use of its system, use of MySpace's service for commercial endeavors, and promotion of information known to be false or misleading.

A MySpace member accesses his e-message account on the internet, at the MySpace.com website. To send a MySpace e-message, the user may either click on a link for "Mail," or go directly to the recipient's unique URL assigned to each individual account.

Defendant is a public company that provides internet-based communications services ("TGLO Products"). Defendant operates one or more websites under various domain names, including glochat.com, tglophone.com, glotalk.com and digitalvoiceglo.com.

Beginning January 2006, Defendant set up at least 95 identical or virtually identical "dummy" MySpace profiles, with corresponding e-message accounts. Defendant used these accounts to send almost 400,000 unsolicited commercial e-messages marketing TGLO Products to MySpace users via scripts. On February 6, 2006, Plaintiff sent a cease and desist letter to Defendant, demanding that Defendant stop sending its commercial e-messages to MySpace members. Thereafter, Defendant ceased its transmission of e-messages. However, the transmissions later resumed and continued through May 2006.

On June 1, 2006, Plaintiff filed the current action against Defendant. In its Complaint, Plaintiff alleges that Defendant's activities violated both federal and state statutory laws, as well as state common laws. By way of its action, Plaintiff seeks an order enjoining Defendants from the conduct giving rise to Plaintiff's claims. Plaintiff also seeks actual damages, liquidated damages, punitive damages, and attorney's fees and costs.

II. JUDICIAL STANDARD

Summary judgment is proper only where "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 a judgment as a matter of law." Fed. R. Civ. P. 56(c)). Upon such a showing, the Court may grant summary judgment as to "all or any part thereof." Fed. R. Civ. P. 56(a), (b).

To prevail on a summary judgment motion, the moving party must show there are no triable issues of fact as to matters upon which it has the burden of proof at trial. See Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). On issues where the moving party does not have the burden of proof at trial, the moving party is required only to show that there is an absence of evidence to support the nonmoving party's case. Id. at 326.

---

1 A script is a computer programming language used to automate simple, repeated actions.
III. DISCUSSION

At issue in these cross-motions are Count I (Violation of CAN-SPAM), Count III (Violation of Section 17529.5) and Count VI (Breach of Contract).

According to Plaintiff, there is no triable issue as to the following alleged facts: Defendant obtained 95 or more MySpace e-message accounts to circumvent MySpace’s daily mail limitations. To obtain these accounts, Defendant set up almost 100 separate email accounts at sites such as hotmail.com to fulfill MySpace’s requirement of providing an alternate email address. Then, Defendant used false information to set up the MySpace accounts with deceptive display names, and purported to use them for personal purposes. In fact, the accounts were used to initiate (via a script) 399,481 unsolicited commercial email messages to MySpace.com users to promote its TGLO Products. Plaintiff asserts that, as a result of this conduct, partial summary judgment should be granted in its favor as to all three counts.

Defendant contends that: (1) Plaintiff has no standing under CAN-SPAM because it is not an ISP; (2) the messages sent over its private messaging system are not e-mail, and therefore neither CAN-SPAM nor Section 17529.5 apply; and (3) the TOS Contract, in general, is an unenforceable contract of adhesion, and the liquidated damages provision, specifically, is unenforceable because it is disproportionate to anticipated damages.

For the following reasons, the Court denies Defendant’s Motion for Partial Summary Judgment, and grants in part, Plaintiff’s Motion for Summary Adjudication.

A. Claims Under CAN-SPAM

CAN-SPAM regulates the manner in which unsolicited commercial emails may be transmitted. See 15 U.S.C. §§ 7701, et seq. The statute also makes unlawful certain conduct relating to such transmissions, including the transmission of false or misleading information, and obtaining email addresses through dictionary attacks. 2 15 U.S.C. §§ 7704(a) - (d). Under CAN-SPAM, an Internet access service provider who is harmed by violations of Section 7704(a), (b) or (d) may seek to enjoin further violation by the defendant, or recover damages equal to the greater of: (1) actual monetary loss incurred by the internet access service provider or (2) statutory damages as provided by Section 7706(g)(3).

Plaintiff alleges that, based on its conduct, Defendant is liable for four separate violations under the statute:

1. Section 7704(a)(1): transmission of commercial email that contain false or misleading information, including header information;
2. Section 7704(a)(2): pattern or practice of transmitting commercial email with deceptive subject headings;

2 Dictionary attacks involve obtaining email addresses using an automated means that generates possible addresses by combining names, letters, or numbers into numerous permutations.
Section 7704(a)(5): pattern or practice of transmitting commercial email which omits identifier, opt-out and physical address information; and

Section 7704(b)(1): using automated means, such as scripts, to generate commercial email to random recipients.

As discussed below, the Court finds no triable issue as to Defendant's violation of the following three of four provisions: Sections 7704(a)(1), 7704(a)(5) and 7704(b)(1)(A)(ii).

1. **Plaintiff Has Standing Under CAN-SPAM**

As an initial matter, CAN-SPAM, which is primarily a criminal statute, authorizes a private right of action only to a “provider of Internet access service.” 15 U.S.C. § 7706(g)(1). Defendant contends that Plaintiff is not a provider of Internet access service, and therefore, has no standing to sue Defendant under the statute.

a. **Plaintiff is an Internet Access Provider**

Under Section 7702(11), “Internet access service” has the meaning given that term in 47 U.S.C. § 231(e)(4) (“Section 231”). Section 231 defines “Internet access service” as “a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers.”

The Ninth Circuit assumes that the legislative purpose of a statute is expressed by the ordinary meaning of the words used. *Leisnoi, Inc. v. Stratman*, 154 F.3d 1062, 1066 (9th Cir. 1998). The plain meaning of the statutory language is unambiguous; “Internet access provider” includes traditional Internet Service Providers (“ISPs”), any email provider, and even most website owners. See *White Buffalo Ventures, LLC v. University of Texas at Austin*, 420 F.3d 366, 373 (5th Cir. 2005); *see also Hypertouch v. Kennedy Western*, 2006 WL 64868 at *3 (N.D. Cal. Mar. 8, 2006). Under this broad definition, Plaintiff is an “Internet access provider.”

b. **MySpace E-Messages Are Electronic Mail**

Notwithstanding the broad definition given to “internet access provider,” CAN-SPAM provides a private right of action to only those Internet access providers who are adversely affected by Section 7704. Since Section 7704 regulates and prohibits conduct involving electronic mail (“electronic mail” or “email”), a private right of action under CAN-SPAM is confined to only those Internet access services that provide access to electronic mail.

CAN-SPAM defines “electronic mail message” as “a message sent to a unique electronic mail address.” 15 U.S.C. § 7702 (6). “Electronic mail address” is defined as “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.” 15 U.S.C. § 7702(5).
According to Plaintiff's evidence, the mail of each MySpace user resides at a unique URL, consisting of a string of characters that includes a reference to a user name or number, and the Internet destination, www.myspace.com. (Ballon Suppl. Decl., Exh.C.2, WhitcomDepo., 71:17-24; Ballon Decl., Tab 4, Wells Decl., ¶ 7.) This evidence shows that MySpace e-messages fall under CAN-SPAM's definition of electronic mail, and Defendant has failed to present any evidence disputing Plaintiff's evidence.

However, Defendant maintains that MySpace e-messages do not constitute CAN-SPAM protected email because: (1) unlike email, MySpace e-messages have no real "route" because the messages always remain within the "walled garden" of MySpace; (2) MySpace e-messages are not email because they do not use simple mail transfer protocol ("SMTP"); and (3) unlike email addresses, MySpace e-message addresses have no domain part. Defendant's arguments are unsupportable.

First, nowhere does the statute specify the requirements set forth by Defendant. Moreover, arguments as to these requirements are part and parcel of Defendant's position that only traditional ISPs have a right to sue under CAN-SPAM, as these requirements are typically associated with email service provided by traditional ISPs. As discussed above, the Court rejects this position. Furthermore, CAN-SPAM's Congressional findings indicate that exclusion of electronic messages that fall outside the ambit of Defendant's specifications would subvert the legislative intent. Regardless of who has a private right of action under the statute, the overarching intent of this legislation is to safeguard the convenience and efficiency of the electronic messaging system, and to curtail overburdening of the system's infrastructure. See 15 U.S.C. § 7701(a). Limiting protection to only electronic mail that falls within the confines set forth by Defendant does little to promote the Congress's overarching intent in enacting CAN-SPAM.

Nonetheless, Plaintiff has introduced evidence showing: (1) its e-message system uses both a routing method and a domain part, and (2) some MySpace e-messages are transmitted using SMTP. First, according to Plaintiff's evidence, every message must contain routing information letting MySpace servers know where to send that message. (Whitcom Decl., ¶ 4.) While the routing employed by MySpace may be less complex and elongated than those employed by ISPs, any routing necessarily implicates issues regarding volume of traffic and utilization of infrastructure -- issues which CAN-SPAM seeks to address. Similar to an ISP, there is only a finite volume of mail that MySpace can handle without further investment in infrastructure. Second, Plaintiff's evidence shows that each user's mailbox includes a reference to, not only a user name, but also to myspace.com, the Internet domain or domain part. (Ballon Suppl. Decl., Exh.C.2, Whitcom Depo., 71:17-24; Ballon Decl., Tab 4, Wells Decl., ¶ 7.) Finally, Plaintiff's evidence shows that, while most MySpace e-messages are sent using Hypertext Transfer Protocol ("HTTP"), each time an HTTP message is sent by a MySpace user, a companion notification message is sent via SMTP to the recipient's alternative email address. (Whitcom Decl., ¶ 5.) Additionally, MySpace users may send SMTP messages over the Internet from myspace.com when they invite someone who is not a MySpace member to join MySpace. (Whitcom Decl., ¶ 6.) Defendant has not presented any evidence to dispute the evidence set forth above. Therefore, Defendant's argument fails, even under its improperly narrow interpretation of the statute.

Based on the foregoing, the Court finds that Plaintiff has standing to sue Defendant under CAN-SPAM because, as defined under CAN-SPAM, Plaintiff is an Internet access provider whose electronic messages qualify as electronic mail.

3 While the statute references the phrase "domain part," it is clearly not a required element, but merely used to illustrate how an electronic mail address is commonly expressed.

CV-90 (05/04) CIVIL MINUTES - GENERAL
2. **Violation of Section 7704(a)(1)**

Section 7704(a)(1) prohibits the transmission of commercial email that contains false or misleading header information. Under the statute, even if the header information is technically accurate, it is considered materially misleading if it includes an originating email address that was accessed through false or fraudulent pretenses, for purposes of initiating the commercial email message. 15 U.S.C. § 7704(a)(1)(A).

According to Plaintiff's evidence, Defendant's employees created MySpace accounts using false identifying information, including fictitious email addresses and contact information. (Ballon Decl., Tab 8, Fowler Depo., 185:4-21; Ballon Decl., Tab 11, Nelson Depo. 34:4-35:8, 37:16-19, Exh. 2.) Defendant's employees also set up MySpace accounts with the display names, “MySpace Phone,” “Chick,” and “Coppermine.” (Ballon Decl., Tab 3, Kaleel Decl., ¶¶ 7 and 12, Exh. C; Ballon Decl., Tab 10, Mobley Depo., 37:23-38:10.) As indicated by this evidence, the accounts created by Defendant failed to identify the messages as originating from TheGlobe. Based on the plain language of Section 7704(a)(1), Plaintiff's evidence establishes that Defendant violated this provision.

In opposition, Defendant argues that the accounts did, in fact, identify TheGlobe as the originator of the e-messages. To support its argument, Defendant has introduced evidence that a document was used to assist employees in creating MySpace accounts. According to this evidence, the document instructed the employees to use “tgle” in the first name and “phone” as the last name. (Elliot Decl., Exh. 13, Nelson Depo., 34:4-25.) This evidence is unavailing, as it fails to dispute Plaintiff's evidence or otherwise support its proposition. At most, the evidence indicates that, in addition to the false accounts described by Plaintiff's evidence, some of Defendant's other accounts may have had as their account identifiers the words “tgle” and “phone,” the product Defendant sought to market. Even so, this fact is irrelevant because Defendant has not offered any evidence showing that those words are readily associated with TheGlobe or its TGLO Products. As such, the Court finds no triable issue as to Defendant's violation of Section 7704(a)(1).

3. **Violation of Section 7704(a)(2)**

Section 7704(a)(2) prohibits a person from transmitting commercial email containing a subject heading that he or she knows would likely mislead the recipient about a material fact regarding the content or subject matter of the message. Under Section 7706(g)(1), a private right of action under Section 7704(a)(2) is available only when there is a pattern or practice that violates this provision.

It is undisputed that Defendant sent MySpace e-messages with the subject headings, “the new MySpace phone,” “the new phone for MySpace,” and “the new tgle phone for MySpace.” (Ballon Decl., Tab 8, Exh. 33; Ballon Decl., Tab 3, Kaleel Decl., ¶ 4; Ballon Decl., Tab 4, Wells Decl., ¶ 17.) The last heading does not violate the statute, as it references “tgle” in a way that accurately describes the content

---

4 “Header information” means “the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail message, and any other information that appears in the line identifying . . . a person initiating the message.” 15 U.S.C. § 7702(8).

5 In its Opposition, Defendant argues that Section 7704(a)(1) only prohibits sending emails containing header information that makes the email appear to come from an address other than the one from which it actually came. Again, the Court finds Defendant's interpretation far too narrow and unsupported by the provision's plain language.
of the message and implies a product that is separate and distinct from MySpace. In contrast, the first two headings do violate the statute because they imply an affiliation with MySpace, likely misleading the recipient into believing that the marketed product is related to MySpace. In fact, it is undisputed that in late January 2006, an influential technology blogger on Zdnet.com inaccurately reported that MySpace had partnered with TheGlobe. (Ballon Decl., Tab 1, Exh. E; Ballon Decl., Tab 15, Cespedes Depo., 52:1-17, 56:2-24.) Although Defendant was aware of this error, it never sought to correct the misinformation. (Ballon Decl., Tab 15, Cespedes Depo., 58:15-24.) Significantly, the undisputed evidence shows that the subject headings described above were attached to e-messages sent after Defendant learned of the blogger’s inaccurate report. (Ballon Decl., Tab 15, Cespedes Depo., 51:17-52:1-6.) As such, the Court finds that Defendant knew, or should have known, that its subject headings were misleading.

Defendant argues that Plaintiff fails to show a pattern or practice. As to this provision, the Court agrees. The undisputed evidence shows that Defendant’s employees were provided written instructions on how to create MySpace accounts and what content to send through the messaging system. (Ballon Decl., Tab 11, Exh. 2.) The instructions directed the employees to use “Call for FREE fast and easy” as the headline. (Ballon Decl., Tab 11, Exh. 2, D-00003909.) This subject heading is consistent with the email content, and does not violate Section 7704(a)(2). As discussed above, notwithstanding the written instructions, as least a portion of the 399,481 e-messages sent by Defendant contained deceptive subject headings that violated the statute. However, without further evidence as to the number of such e-messages sent by Defendant, it is impossible to determine whether Defendant’s violation of this provision rose to the level of a pattern or practice. Therefore, a triable issue of fact exists as to whether the number of e-messages containing deceptive subject headings is substantial enough to constitute a pattern or practice.

4. **Violation of Section 7704(a)(5)**

Section 7704(a)(5) requires that unsolicited commercial emails contain: (1) clear notification that the message is an advertisement, (2) clear notice of the opportunity to decline receipt of further messages from the sender, and (3) a valid physical postal address for the sender. Again, under Section 7706(g)(1), a private right of action under Section 7704(a)(5) is available only when the defendant has a pattern or practice of violating this provision.

It is undisputed that none of Defendant’s 399,481 e-messages contained clear notice of the opportunity to decline receipt of further messages from the sender, or a valid physical postal address for the sender. (Separate Statement of Uncontroverted Material Facts ("UMF"), ¶¶ 14 and 15; Defendant's Statement of Genuine Issues.) Therefore, Defendant clearly violated this statutory provision.

Again, Defendant argues that its activities do not constitute a pattern or practice, as prescribed by Section 7706(g)(1). However, as stated above, the following is undisputed: (1) Defendant’s employees were given instructions on how to create a MySpace account, what information should be placed in the profiles, and what content to write in the messages (Ballon Decl., Tab 8, Exh. 33.); and (2) through its employees, Defendant created at least 95 MySpace accounts and sent 399,481 unsolicited commercial emails over a course of five months. (Ballon Decl., Tab 4, Wells Decl. ¶ 8; Ballon Decl., Tab 11, Nelson

---

4 In its Statement of Genuine Issues, Defendant attempts to dispute this fact by stating that MySpace provides a mechanism for users to opt out of receiving further messages from a particular sender. However, this fact is irrelevant, as it fails to dispute Plaintiff’s evidence and, in any case, fails to comport with the statutory requirement that clear notice of a recipient’s ability to decline further messages be provided in the original email.
5. **Violation of Section 7704(b)(1)**

Section 7704(b) makes it an aggravated violation to initiate the transmission of commercial email that is unlawful under Section 7704(a) where “the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letter or numbers into numerous permutation.” 15 U.S.C. § 7704(b)(1)(A)(ii).

Plaintiff’s evidence shows that Defendant randomly selected a range of MySpace ID numbers. Defendant then used a script to automatically generate a set of sequential IDs. Once these IDs were generated, the script automatically transmitted Defendant’s messages to those IDs. (Ballon Decl., Tab 8, Fowler Depo., 54:14-57:11) According to the evidence, some of the IDs correlated to MySpace profiles, and some did not. (Ballon Decl., Tab 8, Fowler Depo., 55:1-20) A total of 399,481 messages were sent using this script. (Ballon Decl., Tab 8, Fowler Depo., 170:3-16.) Based on the evidence presented, Defendant violated Section 7704(1)(A)(ii).

In opposition, Defendant argues that it did not violate the statutory provision because the script sent messages in sequence, rather than at random. Defendant further argues that the script sent the messages to a range of MySpace profiles by using a range of user IDs that had already been assigned by MySpace. Defendant’s arguments are unavailing, as it is unclear how these distinctions change the fact that Defendant used “automated means that generates possible electronic mail addresses.” As such, the Court finds no triable issue as to Defendant’s violation of Section 7704(b)(1)(A)(ii).

**B. Section 17529.5 Claim**

Section 17529.5 prohibits email transmissions to or from California email addresses containing “falsified, misrepresented or forged header information” or a subject line that would likely “mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.” Section 17529.5(a)(2) and (3). Under the statute, an electronic mail service provider’s claim may bring an action against a person or entity that violates this section.

It is undisputed that MySpace’s servers, which house all MySpace.com e-message accounts, are located in California. (Ballon Decl., Tab 2, Boster Decl., ¶ 2.) Furthermore, it is undisputed that every time a user logs on to MySpace.com to send, review or reply to an e-message, he or she is doing so by accessing the California servers. (Kaleel Decl., ¶ 3.) Based on this evidence, as well as the evidence and analysis discussed in Section III.A. above, the Court finds no triable issues as to Defendant’s liability for Plaintiff’s Section 17529.5 claim.

---

7 An “electronic mail service provider” is defined as “any person, including an Internet service provider, that is an intermediary in sending or receiving electronic mail or that provides to end users of the electronic mail service the ability to send or receive electronic mail.” Section 17529.1(h).
C. Breach of Contract Claim

To set up a MySpace account, a person must assent to the TOS Contract by checking a box agreeing to its terms. Plaintiff claims that, by setting up 95 accounts and sending its marketing e-messages through those accounts, Defendant breached the terms of the TOS Contract. Furthermore, due to modified terms of the TOS Contract, Plaintiff contends that Defendant must pay $50 for each of its e-messages that were sent after March 17, 2006.

1. Breach of the TOS Contract

It is undisputed that Defendant’s e-messages were sent between January 2006 and May 2006. (Ballon Decl., Tab 8, Fowler Depo., 168:1-15.) During that time, the TOS Contract was modified three times. (Ballon Decl., Tab 2, Boster Decl., ¶¶ 3-6.) All four versions of the TOS Contract contain the following provision: MySpace is “for the personal use of Members only and may not be used in connection with any commercial endeavors except those that are specifically endorsed or approved by the management of MySpace.com. (Ballon Decl., Tab 2, Exhs. A-D.) Also, each version prohibits: (1) content that involves the transmission of ‘junk mail,’ ‘chain letters,’” or unsolicited mass mailing or ‘spamming;’ and (2) “any automated use of the system, such as using scripts to add friends.” Id.

Based on the evidence and analysis discussed in Section III.A above, the Court finds that Defendant used a script to transmit an unsolicited mass mailing to MySpace users for purposes of an unapproved commercial endeavor. This activity violates the terms of the TOS Contract.

Defendant argues that the TOS Contract, as a whole, is entirely unenforceable because every relevant version is a contract of adhesion, such that the terms are unconscionable. This argument is not well-taken.

The doctrine of unconscionability provides that a contract is unenforceable if it is both procedurally and substantively unconscionable. A&M Produce Co. v. FMC Corp., 135 Cal App. 3d 473, 485-486 (1982). Procedural unconscionability focuses on oppression and surprise due to unequal bargaining power. 4 Trend Homes, Inc. v. Superior Court. 131 Cal. App. 4th 950, 957-58 (2005). “Oppression” arises from the inequality of the parties’ bargaining power and an absence of real negotiation or a meaningful choice on the weaker party’s part. Id. at 958. “Surprise” is found when “the terms to which the party supposedly agreed [are] hidden in a prolix printed form drafted by the party seeking to enforce them.” Id. (citations omitted). A contract is substantively unconscionable when its terms are so harsh, oppressive, or one-sided as to shock the conscience. Id. at 961.

A review of the TOS Contract shows that it is, in fact, a standardized contract that gives the subscribing party only the opportunity to adhere to the contract or reject it. (See Ballon Decl., Tab 2, Exhs. A-D.) However, the facts indicate that Defendant had a reasonable alternative or meaningful choice in the matter, in that marketing through MySpace using the method employed was not its only choice. See Freeman v. Wal-Mart Stores, Inc., 111 Cal. App. 4th 660, 668-669 (2003). In fact, Plaintiff’s evidence shows that Defendant had, in fact, considered purchasing advertising space on the MySpace

8 Folded into this analysis is the determination of whether the contract is adhesive. Procedural unconscionability is typically found where there is a contract of adhesion. While an alternative method of analysis calls for an initial determination of whether the contract at issue is adhesive, that determination, by itself, has no legal consequence for purposes of deciding whether a contract is enforceable. The true determining factor is whether the contract is unconscionable. See Graham v. Scissor-Tail, Inc., 28 Cal. 3d 807 (1981).
website. (Ballon Decl., Tab 10, Mobley Depo., 44:19-47:7.) Moreover, the Court finds that the contract is not written prolixly, particularly for an experienced, sophisticated business entity whose area of expertise involves Internet related technology. Even if the TOS contract was procedurally unconscionable, the terms, as a whole, are certainly not so harsh, oppressive, or one-sided as to shock the conscience.

In light of the above, the Court finds that Defendant breached the TOS Contract.

2. **Liquidated Damages Provision**

On March 17, 2006, Plaintiff modified the TOS Contract and included the following provision: “Prohibited activity includes . . . advertising to, or solicitation of, any Member to buy or sell any products or services through the Services. If you breach this Agreement and send unsolicited bulk email, . . . or other unsolicited communications of any kind . . . As a reasonable estimation of such harm, you agree to pay MySpace.com $50 for each such unsolicited email . . . you send through the Services; . . .” *Id.*

Plaintiff asserts that, under this provision, Defendant is liable for liquidated damages in the amount of $50 per message sent after March 17, 2006. Defendant argues that the $50 liquidated damages clause is unenforceable because it is an impermissible contractual penalty. The Court disagrees.

California law provides that liquidated damages clauses are enforceable where: (1) damages from a breach would be impracticable or extremely difficult to determine with certainty; and (2) the amount represents a reasonable estimation of what such damages might be. *Utility Consumers’ Action Network, Inc. v. AT&T Broadband of Southern California*, 135 Cal. App. 4th 1023, 1029 (2006). As stated above, the Court has found that Defendant breached the TOS Agreement by bulk transmission of unapproved, unsolicited commercial e-messages. The costs associated with this activity include not only infrastructure costs, such as additional bandwidth, and monitoring costs, they are also rife with large hidden costs. Such hidden costs include those associated with deterrence (legal fees, software, etc.), depletion of customer goodwill, and liability implications associated with the unlawfully advertised product. Therefore, the damages related to Defendant’s breach are, in fact, impracticable or extremely difficult to determine. As to the amount of liquidated damages, CAN-SPAM sets statutory damages for unsolicited commercial emails at $25-$300 per message. Moreover, while the costs associated with spamming are difficult to definitively assess, the costs listed above are certainly large, and only the tip the iceberg. Therefore, the Court finds $50 per message a reasonable estimation of Plaintiff’s damages.

Defendant further argues that, even if the Court finds the liquidated provision enforceable, the provision should be applied only to those messages that were sent from accounts created after March 17, 2006. Plaintiff contends that, because the TOS contract specifically provides for modification of the agreement, the provision should apply to all messages sent after March 17, 2006, regardless of when the account was created. The Court agrees with Plaintiff.

All four versions of the TOS Contract specifically provide: “MySpace.com may modify this Agreement from time to time and such modification shall be effective upon posting by MySpace.com on the Website. You agree to be bound to any changes to this Agreement when you use the Service after any such modification is posted.” *Ballon Decl., Tab 2, Exhs. A-D* (emphasis added.) For the same reasons stated above, this contractual term is neither procedurally nor substantively unconscionable. Additionally, the Court notes that Defendant created all 95 MySpace accounts, both before and after
March 17, 2006. Therefore, at the time it created its post-March 17 accounts, it knew, or should have known, that all messages, even those sent from pre-March 17 accounts, were subject to the liquidated damages provision. As such, the Court finds that the liquidated damages provision contained in the March 17, 2006 TOS Contract applies to all messages sent by Defendant after March 17, 2006.

IV. EVIDENTIARY OBJECTIONS

To the extent this Court has relied on evidence to which the parties object, those objections are overruled.

V. CONCLUSION

In light of the foregoing, Defendant’s Motion for Partial Summary Judgment is denied, and Plaintiff’s Motion for Partial Summary Judgment is granted in part. Specifically, the Court finds summary judgment in favor of Plaintiff as to the following:

(1) Count I: Violation of 15 U.S.C. §§ 7704(a)(1), 7704(a)(5) and 7704(b)(1)(A)(ii);
(2) Count III: Violation of Section 1729.5;
(3) Count VI: Breach of Contract; and
(4) Liquidated Damages of $50 per e-message sent after March 17, 2006.

The Court finds a triable issue of fact as to Plaintiff’s claim that Defendant violated 15 U.S.C. § 7704(a)(2).

IT IS SO ORDERED.

Initials of Preparer

[Signature]

656
PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

OMEGA WORLD TRAVEL,
INCORPORATED; CRUISE.COM,
INCORPORATED; GLORIA BOHAN;
DANIEL BOHAN,

Plaintiffs-Appellees,

v.

MUMMAGRAPHICS, INCORPORATED,
d/b/a Webguy Internet Solutions,
d/b/a Webguy.net, d/b/a
SucaSpammer.com,

Defendant-Appellant,

and

MARK W. MUMMA, in his individual
capacity,

Defendant.

No. 05-2080

Appeal from the United States District Court
for the Eastern District of Virginia, at Alexandria.
Leonie M. Brinkema, District Judge.
(CA-05-122)

Argued: September 21, 2006
Decided: November 17, 2006

Before WILKINSON and DUNCAN, Circuit Judges, and
Richard L. VOORHEES, United States District Judge for the
Western District of North Carolina, sitting by designation.

Affirmed by published opinion. Judge Wilkinson wrote the opinion,
in which Judge Duncan and Judge Voorhees joined.
COUNSEL

ARGUED: Kelly O. Wallace, WELLBORN & WALLACE, L.L.C., Atlanta, Georgia, for Appellant. James P. Hodges, Leesburg, Virginia, for Appellees. ON BRIEF: Richard S. Toikka, METROPOLITAN LEGAL SERVICES, L.L.C., Rockville, Maryland, for Appellant. Thomas J. Powell, Fairfax, Virginia, for Appellees.

OPINION

WILKINSON, Circuit Judge:

Countless commercial e-mail messages, known colloquially as "spam," pass through the Internet every day, inspiring frustration, countermeasures, and — as here — lawsuits. Based upon eleven commercial e-mail messages, Mummographics, Inc., a provider of online services, seeks significant statutory damages from Omega World Travel, Inc., a Virginia-based travel agency ("Omega"); Gloria Bohan, Omega’s president and founder; and Cruise.com, Inc., a wholly owned subsidiary of Omega (collectively, "appellees"). Mummographics alleges that Cruise.com sent the messages in violation of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. §§ 7701 et seq., as well as Oklahoma law.

The district court awarded summary judgment to the appellees on all of Mummographics’ claims and we affirm. The CAN-SPAM Act preempts Mummographics’ claims under Oklahoma’s statutes. In addition, Mummographics failed to allege the material inaccuracies or pattern of failures to conform to opt-out requirements that is necessary to establish liability under the CAN-SPAM Act. The CAN-SPAM Act addresses "spam" as a serious and pervasive problem, but it does not impose liability at the mere drop of a hat.

I.

Appellant Mummographics, Inc., d/b/a Webguy Internet Solutions, is an Oklahoma corporation with its only place of business in Okla-
Omega World Travel v. Mummographics, Inc.

Inoma City. According to Mark Mumma, the company's president, Mummographics hosts web pages, registers domain names, designs web pages and logos, and sets up computer servers. Mummographics also operates websites devoted to opposing "spam" messages including "sueaspmmer.com." In addition, Mummographics runs a website, "OptOutByDomain.com," that lists Internet domain names — roughly seventy of 347 of which are operated by Mummographics — whose owners have indicated that they do not wish to receive unsolicited commercial e-mail messages. Mummographics owns the domain name webguy.net and uses the e-mail account inbox@webguy.net for company purposes.

Cruise.com operates a website selling cruise vacations and sends e-mail advertisements — dubbed "E-deals" — to prospective customers. It sent eleven "E-deals" containing travel offers to inbox@webguy.net between December 29, 2004 and February 9, 2005. Each message contained a line of text on which the recipient could click in order to be removed from future mailings, and each message also said that the recipient could opt-out of future e-mails by writing to a postal address contained in each message. Each message also contained a link to the Cruise.com website and a toll-free phone number for the company.

Mummographics claims that the messages contained several inaccuracies. First, each message stated that the recipient had signed up for the Cruise.com mailing list, but Mummographics alleges that it had not asked that inbox@webguy.net receive the company's offers. Second, while each message listed Cruise.com as the sending organization, each also included the address "FL-Broadcast.net" in its header information, even though Mummographics alleges that "FL-Broadcast.net" is not an Internet domain name linked to Cruise.com or the other appellees. In addition, the messages contained the "from" address cruisedeals@cruise.com, even though Cruise.com had apparently stopped using that address.

When Mark Mumma noticed the Cruise.com e-mails that inbox@webguy.net had received, he did not use the electronic opt-out link to remove the address from the Cruise.com e-mail list, but instead called John Lawless, Omega World Travel's general counsel, to complain. Mumma told Lawless that he had not asked to receive
the "E-deal" messages. He told Lawless that he refused to use e-mail opt-out mechanisms because "only idiots do that," and he believed opt-out mechanisms just led to more unwanted messages. Mumma told Lawless that his preferred removal procedure was to sue for violations of Oklahoma law. Lawless asked Mumma for his e-mail address, but Mumma did not provide it. Instead, he asked Lawless to remove from all future mailings every address containing a domain name listed on Mummographics' "OptOutByDomain.com" website. Lawless said he was "gonna take them down right now," but Omega's technical support division indicated that removing all the addresses would require considerable effort, and the addresses were not immediately removed.

On January 20, 2005, the day after speaking with Lawless, Mumma received another "E-deal" message at inbox@webguy.net. He sent a letter dated January 25, 2005 to Daniel Bohan of Omega World Travel, saying that he had received six unsolicited "E-deal" messages from Cruise.com, Omega's subsidiary, but again not specifying the e-mail address at which he had received the messages. The letter claimed that the messages violated federal and state laws and said that Mumma intended to sue Bohan's company for at least $150,000 in statutory damages unless Bohan settled the matter for $6,250. Mumma attached the Cruise.com e-mails to his letter, and after John Lawless noticed that the messages appeared to have been sent to inbox@webguy.net, he directed that the address be removed from the Cruise.com mailing list. The company subsequently removed the address.

After Omega World Travel failed to pay Mumma, postings on one of Mumma's "anti-spam" websites accused Omega, Cruise.com, and Daniel and Gloria Bohan of being "spammers" who had violated state and federal laws. The website posted a photo of the Bohans that had evidently been copied from the Omega website and described the couple as "cruise.com spammers." On the basis of these postings, Omega World Travel, the Bohans, and Cruise.com sued Mumma and Mummographics in federal court, claiming defamation, copyright infringement, trademark infringement, and unauthorized use of likeness. The district court granted Mummographics summary judgment on all these claims except the libel action, on which all the plaintiffs except Daniel Bohan, who is no longer a party, expect to proceed to trial.
Mummagraphics raised counterclaims against the appellees under Oklahoma and federal law, which are the only claims now before this court. Mummagraphics alleged, *inter alia*, that the Cruise.com e-mails contained actionable inaccuracies and that the appellees failed to comply with federal and state requirements that they stop sending messages to recipients who opted out through specified procedures. Both parties sought summary judgment on Mummagraphics' counterclaims, and the district court granted the appellees' motion. The court held that the CAN-SPAM Act preempted Mummagraphics' claims under Oklahoma's statutes. It further held, *inter alia*, that the appellees had not violated the CAN-SPAM Act because the alleged e-mail inaccuracies were not material and the appellees had not violated the opt-out provisions. Mummagraphics now appeals.

II.

A.

We turn first to the district court's determination that the CAN-SPAM Act preempted Mummagraphics' claims under Oklahoma's statutes regulating commercial e-mail messages. The basic principles of preemption are well settled, and we need not belabor them here. Our inquiry into the scope of a preemption clause is shaped by "two presumptions." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996). First, under our federal system, we do not presume that Congress intends to displace state law," *Maryland v. Louisiana*, 451 U.S. 725, 746 (1981), and "that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress," *Medtronic*, 518 U.S. at 485 (citations omitted). Second, from this departure point, we address preemption issues in accordance with the "oft-repeated comment . . . that "[t]he purpose of Congress is the ultimate touchstone' in every preemption case." *Id.* (alteration in original) (citation omitted). Instead of imposing the narrowest possible construction on preemptive language when read in isolation, we seek "a fair understanding of congressional purpose," looking to "the language of the pre-emption statute and the statutory framework surrounding it," while also considering "the structure and purpose of the
statute as a whole." *Id.* at 486 (emphasis, citations, and internal quotations omitted).

B.

Mummographics argues that it is entitled to damages because such damages are authorized by Oklahoma law and lie outside the CAN-SPAM Act's preemptive scope. The CAN-SPAM Act provides, in part,

This chapter 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 portion of a commercial electronic mail message or information attached thereto.

15 U.S.C. § 7707(b)(1). The principal Oklahoma provision under which Mummographics seeks damages provides:

It shall be unlawful for a person to initiate an electronic mail message that the sender knows, or has reason to know:

1. Misrepresents any information in identifying the point of origin or the transmission path of the electronic mail message;

2. Does not contain information identifying the point of origin or the transmission path of the electronic mail message; or

3. Contains false, malicious, or misleading information which purposely or negligently injures a person.

Okla. Stat. tit. 15, § 776.1A.¹

¹Mummographics also alleged that the appellees violated an Oklahoma provision requiring senders of unsolicited commercial e-mails to comply
Oklahoma courts appear not to have construed the state provision, but the language seems to reach beyond common law fraud or deceit. By its terms, the statute is not limited to inaccuracies in transmission information that were material, led to detrimental reliance by the recipient, and were made by a sender who intended that the misstatements be acted upon and either knew them to be inaccurate or was reckless about their truth. Cf. Rogers v. Meiser, 68 P.3d 967, 977 (Okla. 2003) (requiring those elements for Oklahoma fraud action); see also Restatement (Second) of Torts § 525, § 538 (1977).

The district court held that the Oklahoma statutes were preempted insofar as they applied to immaterial misrepresentations, and that this ruling disposed of Mummagraphics’ Oklahoma statutory claims. Mummagraphics does not challenge the district court’s reading of Oklahoma law or Mummagraphics’ complaint, but it argues that the district court was incorrect to hold actions for immaterial error to be preempted because the CAN-SPAM Act permits states to "prohibit[] falsity or deception." See 15 U.S.C. § 7707(b)(1).

Whatever the precise scope of the Oklahoma provision might be, we cannot agree that Mummagraphics' action for immaterial errors survives preemption. To begin with, the language in the exception to the federal preemption provision upon which Mummagraphics relies is hardly as straightforward as the company suggests. The exception, as noted, allows states to prohibit "falsity or deception" in commercial e-mail messages. Those terms are not defined in the statute. However, "deception" requires more than bare error, and while "falsity" can be

with certain opt-out requests. See Okla. Stat. tit. 15, § 776.6E. We agree with the district court that this provision was preempted because it bears no arguable relationship to the subject matter excepted from preemption in the CAN-SPAM Act. See 15 U.S.C. § 7701(b)(1). Finally, Mummagraphics alleged that the appellees violated the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, §§ 751 et seq., by violating Oklahoma’s commercial e-mail laws. See id. § 776.1C. Since we find that Mummagraphics did not raise a cognizable cause of action under Oklahoma’s commercial e-mail laws due to federal preemption, the alleged violations cannot give rise to further claims under the Oklahoma Consumer Protection Act.
defined as merely "the character or quality of not conforming to the truth or facts," it also can convey an element of tortiousness or wrongfulness, as in "deceitfulness, untrustworthiness, faithlessness." Webster's Third New International Dictionary Unabridged 820 (1971); see also Oxford English Dictionary Vol. V 697 (2d ed. 1989) (defining false as "erroneous, wrong," but also as "mendacious, deceitful, treacherous," and "[p]urposely untrue"); see also Black's Law Dictionary 635 (8th ed. 2004) (defining "false" as "untrue" but also as "deceitful; lying").

Since the word "falsity" considered in isolation does not unambiguously establish the scope of the preemption clause, we read "falsity" in light of the clause as a whole. Reading "falsity" as referring to traditionally tortious or wrongful conduct is the interpretation most compatible with the maxim of nascitur a sociis, that a word is generally known by the company that it keeps. See, e.g., Jarecki v. G.D. Searle & Co., 367 U.S. 303, 307 (1961); Neal v. Clark, 95 U.S. 704, 708-09 (1877). The canon applies in the context of disjunctive lists. See Neal, 95 U.S. at 706, 709; Jarecki, 367 U.S. at 304 n.1, 307. Here, the preemption clause links "falsity" with "deception" — one of the several tort actions based upon misrepresentations. Keeton et al., Prosser and Keeton on the Law of Torts § 105, at 726-27 (5th ed. 1984) (defining deceit as species of false-statement tort). Restatement (Second) of Torts § 525 (describing elements of deceit). This pairing suggests that Congress was operating in the vein of tort when it drafted the preemption clause’s exceptions, and intended falsity to refer to other torts involving misrepresentations, rather than to sweep up errors that do not sound in tort.

Other sections of the CAN-SPAM Act do not support a bare-error reading of "falsity." In the portion of the Act that created a civil cause of action, Congress affixed the title "[p]rohibition of false or misleading transmission information" to a section that prohibits only "header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1) (emphasis added). While "the heading of a section cannot limit the plain meaning of the text," it can "shed light on some ambiguous word or phrase." Bhd. of R.R. Trainmen v. Baltimore & Ohio R.R. Co., 331 U.S. 519, 529 (1947); see also Almendarez-Torres v. United States, 523 U.S. 224, 234 (1998). Moreover, the "normal rule of statutory construction" provides that "identical words
used in different parts of the same act are intended to have the same meaning." *Gustafson v. Alloyd Co.*, 513 U.S. 561, 570 (1995) (internal quotations omitted). Whether linked with materiality, *see* 15 U.S.C. § 7704(a)(1), or "deception," *see id.* § 7707(b)(1), we can find nowhere in the statute that Congress meant to apply falsity in a mere error sense.

There are good reasons for this. Congress did not intend "falsity" to encompass bare error because such a reading would upset the Act’s careful balance between preserving a potentially useful commercial tool and preventing its abuse. The Act’s enacted findings make clear that Congress saw commercial e-mail messages as presenting both benefits and burdens. Congress found that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail," *id.* § 7701(a)(2), but also that e-mail’s "low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce," *id.* § 7701(a)(1). Congress noted that states had sought to regulate commercial e-mails, but it found that the resulting patchwork of liability standards had proven ineffective:

Many States have enacted legislation intended to regulate 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 disparate statutes they are required to comply.

*Id.* § 7701(a)(11).

Congress implemented these findings by creating a national standard that would be undermined to the point of near-irrelevancy by Mummagraphics’ interpretation of the preemption clause. Rather than banning all commercial e-mails or imposing strict liability for insignificant inaccuracies, Congress targeted only e-mails containing
something more than an isolated error. The CAN-SPAM Act made it a crime to "materially fals[e] header information in multiple commercial electronic mail messages and intentionally initiate[ ] the transmission of such messages," but it attached no criminal sanction to non-material errors. 18 U.S.C. § 1037(a)(3). The Act created civil causes of action relating to error, but attached requirements beyond simple mistake to each of them. It permitted lawsuits based upon "materially false or materially misleading" header information. 15 U.S.C. § 7704(a)(1) (emphasis added). The Act made it actionable for a 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 . . . ." Id. § 7704(a)(2) (emphasis added). In sum, Congress' enactment governing commercial e-mails reflects a calculus that a national strict liability standard for errors would impede "unique opportunities for the development and growth of frictionless commerce," while more narrowly tailored causes of action could effectively respond to the obstacles to "convenience and efficiency" that unsolicited messages present. Id. § 7701(a).

Mummagraphics' reading of the preemption clause would upend this balance and turn an exception to a preemption provision into a loophole so broad that it would virtually swallow the preemption clause itself. While Congress evidently believed that it would be undesirable to make all errors in commercial e-mails actionable, Mummagraphics' interpretation would allow states to bring about something very close to that result.

The ensuing consequences would undermine Congress' plain intent. As we have noted, Congress found that because e-mail addresses do not specify recipients' physical locations, it can be difficult or impossible to identify where recipients live and hence to determine the state laws that apply. Id. § 7701(a)(11). Moreover, commercial e-mails are a bulk medium used to target thousands of recipients with a single mouse-click, meaning that the typical message could well be covered by the laws of many jurisdictions. As a result, law-abiding senders would likely have to assume that their messages
were governed by the most stringent state laws in effect. The strict liability standard imposed by a state such as Oklahoma would become a de facto national standard, with all the burdens that imposed, even though the CAN-SPAM Act indicates that Congress believed a less demanding standard would best balance the competing interests at stake. Because Mummagraphics' reading of the "falsity or deception" exception would thus permit an exception to preemption to swallow the rule and undermine the regulatory balance that Congress established, Mummagraphics' reading of the exception is not compatible with the structure of the CAN-SPAM Act as a whole.

C.

By giving the preemption provision its proper scope, we avoid the need to resolve a difficult constitutional question concerning the compatibility of Oklahoma's commercial e-mail provisions with the dormant commerce clause. Congress' power to regulate interstate commerce implicitly prohibits states from passing any law that "discriminates against or unduly burdens interstate commerce and thereby 'imped[es] free private trade in the national marketplace.'" Gen. Motors Corp. v. Tracy, 519 U.S. 278, 287 (1997) (alteration in original). Whether a nondiscriminatory law unduly burdens interstate commerce turns upon whether it serves a "legitimate local purpose," and, if so, "the nature of the local interest involved, and . . . whether it could be promoted as well with a lesser impact on interstate activities." Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970).

This is not a simple case because important interests lie on both sides of the Pike analysis. We have previously deemed it relevant that one state's Internet laws may impose compliance costs on businesses throughout the country, because it is difficult for businesses to determine where Internet users are located. See PSINet, Inc. v. Chapman, 362 F.3d 227, 239-41 (4th Cir. 2004) (relying upon extraterritorial implications in finding statute criminalizing Internet dissemination of material harmful to minors violated dormant commerce clause). Moreover, courts have long recognized that civil liability for false statements can burden even innocent speech. See, e.g., New York Times Co. v. Sullivan, 376 U.S. 254, 270-73 (1964). The deterrent effect on commercial speech would be particularly great under a statute that authorizes enormous statutory damages — $25,000 for each
day of violations. Okla. Stat. tit. 15, § 776.2C; Okla. Stat. tit. 15, § 776.7C. On the other hand, false and misleading content on the Internet is a serious problem, see 15 U.S.C. § 7701(a), and even innocent inaccuracies can impose costs that states may view as a proper object of redress, State v. Heckel, 24 P.3d 404, 409-411 (Wash. 2001). We avoid a difficult balancing analysis by giving Congress' preemption clause its proper scope. See Jack L. Goldsmith & Alan O. Sykes, The Internet and the Dormant Commerce Clause, 110 Yale L.J. 785, 818-23 (2001) (describing arguments).

III.

We turn next to Mummagraphics' claims that the Cruise.com e-mails violated the CAN-SPAM Act. Mummagraphics first argues that the Cruise.com e-mails violated the Act's requirements concerning the accuracy of header information in commercial e-mails. The Act provides, "It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message . . . that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). The Act further explains,

2Giving the preemption clause its proper scope also allows us to avoid deciding whether such a stringent liability statute exceeds even the states' wide latitude to regulate false or misleading commercial speech. See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (stating that for commercial speech to be protected under the First Amendment "it at least must . . . not be misleading"); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985) (plurality) (allowing presumed and punitive damages for false and damaging credit report that did not involve matters of public concern and constituted speech "solely in the individual interest of the speaker and its specific business audience").

3We shall assume without deciding that Mummagraphics qualifies as an Internet Access Service Provider entitled to bring a claim under the CAN-SPAM Act. See 15 U.S.C. § 7706(g) (creating private right of action for providers of Internet access service); 47 U.S.C. § 231(e)(4) ("The term 'Internet access service' means a service that enables users to access content, information, electronic mail, or other services offered over the Internet . . . ").
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.

Id. § 7704(a)(6). Mummographics alleges that the senders of the Cruise.com e-mails violated this provision because the messages' header information incorrectly indicated that the e-mails originated from the server "FL-Broadcast.net," and because the messages' "from" address read cruisedeals@cruise.com, although that e-mail address was apparently non-functional.

We agree with the district court that these inaccuracies do not make the headers "materially false or materially misleading." Id. § 7704(a)(1). The e-mails at issue were chock full of methods to "identify, locate, or respond to" the sender or to "investigate [an] alleged violation" of the CAN-SPAM Act. Id. § 7704(a)(6). Each message contained a link on which the recipient could click in order to be removed from future mailings, in addition to a separate link to Cruise.com's website. Each message prominently displayed a toll-free number to call, and each also listed a Florida mailing address and local phone number for the company. Several places in each header

4The statute also provides that particular actions not alleged in this case render a message materially misleading. 15 U.S.C. § 7704(a)(1). There is no evidence that any Cruise.com messages "include[d] 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 . . . ." Id. § 7704(a)(1)(A). Nor is there evidence that any Cruise.com message "fail[ed] to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly use[d] another protected computer to relay or retransmit the message for purposes of disguising its origin." Id. § 7704(a)(1)(C).
referred to the Cruise.com domain name, including one line listing Cruise.com as the sending organization.

These references come as little surprise, because the "E-deal" messages were sales pitches intended to induce recipients to contact Cruise.com to book the cruises that the messages advertised. Since the "E-deal" messages and their headers were replete with accurate identifiers of the sender, the alleged inaccuracies in the headers could not have impaired the efforts of any recipient, law enforcement organization, or other party raising a CAN-SPAM claim to find the company. If the alleged inaccuracies in a message containing so many valid identifiers could be described as "materially false or materially misleading," we find it hard to imagine an inaccuracy that would not qualify as "materially false or materially misleading." Congress' materiality requirement would be rendered all but meaningless by such an interpretation.

We also reject Mummagrams' claim for alleged violations of the CAN-SPAM Act's e-mail removal provisions, because Mummagrams cannot sustain such a claim without evidence that could establish a "pattern or practice" of violations. The CAN-SPAM Act requires that the commercial e-mails it covers include

a functioning return electronic mail address or other form of Internet-based mechanism, clearly and conspicuously displayed, that . . . 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 . . . .

Id. § 7704(a)(3)(A). Senders must honor requests for removal made using these mechanisms within ten business days. Id. § 7704(a)(4)(A). While the Act permits Internet access service providers to bring suit under these provisions, they may do so only for "a pattern or practice" that violates the requirements. Id. § 7706(g)(1). In this case, Mummagrams merely alleged that the appellees failed to remove inbox@webguy.net from the "E-deals" mailing list within ten days of Mark Mumma’s call to Omega’s general counsel. It does not allege
that the appellees failed to comply with any other removal request. As a result, Mummographics has not alleged facts sufficient to survive summary judgment on its opt-out claim. This holding makes it unnecessary to address the district court’s ruling that Mummographics’ evidence did not point to even a single violation of the CAN-SPAM Act’s opt-out provisions.

IV.

Lastly, Mummographics claims that Cruise.com’s e-mail messages amounted to trespass to chattels under Oklahoma law. While the CAN-SPAM Act does not preempt the application of state tort laws that are not specific to e-mail messages, id. § 7707(b)(2)(A), the district court correctly granted summary judgment on this claim because Mummographics has not offered evidence that Cruise.com’s e-mails caused the company more than nominal damages. Trespass to chattel is a common law tort that "may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another." *Woodis v. Okla. Gas & Elec. Co.*, 704 P.2d 483, 485 (Okl. 1985) (quoting *Restatement (Second) of Torts* § 217). However, trespass to chattel claims may be brought against a trespasser only if

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

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

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

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

*Mummographics cites the law of multiple jurisdictions on this subject but does not contest the appellees’ assertion that any trespass to chattels claim arises under the laws of Oklahoma, where Mummographics’ computers are located.*
Restatement (Second) of Torts § 218. We proceed with particular caution in this area because Oklahoma courts appear never to have recognized this tort based upon intangible invasions of computer resources. In fact, the Woodis court described "intermeddling" with a chattel as meaning "intentionally bringing about a physical contact with the chattel." 704 P.2d at 485 (quoting Restatement (Second) of Torts § 217 cmt. e (1965)) (emphasis added).

Even if Oklahoma law were to make trespass against chattels available for computer intrusions, Mummgraphics' claim cannot survive summary judgment because the courts that recognize trespass to chattels based upon computer intrusions do not allow "an action for nominal damages for harmless intermeddlings with the chattel." Intel Corp. v. Hamidi, 71 P.3d 296, 302 (Cal. 2003) (quoting Restatement (Second) of Torts § 218 cmt. e (1965)). Because Mummgraphics failed to submit any evidence that the receipt of eleven commercial e-mail messages placed a meaningful burden on the company's computer systems or even its other resources, summary judgment was appropriate on this counterclaim.

V.

We respect the fact that unsolicited commercial e-mail has created frustration and consternation among innumerable users of the Internet. The proper treatment of mass commercial e-mail has provoked controversy since perhaps the first such message was sent. See Adam Hamel, Note, Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-Mail?, 39 New Eng. L. Rev. 961, 965 (2005) (dating "spam" to 1994 advertisement sent to approximately 6000 Internet discussion groups, provoking online outcry). Our role is not to determine the best way of regulating such messages, but merely to implement the balance that Congress struck. The CAN-SPAM Act prohibits some material misstatements and imposes opt-out requirements, but it does not make every error or opt-out request into grounds for a lawsuit. The e-mails in this case are not actionable under the Act. Nor can the messages be actionable under Oklahoma's statutes, because allowing a state to attach liability to bare immaterial error in commercial e-mails would be inconsistent with the federal Act's preemption text and structure, and, consequently, with a "fair understanding of congressional purpose." Medtronic, 518 U.S. at 486 (emphasis omit-
ted). Since we agree that summary judgment was warranted on Mummagraphics' various claims, the judgment of the district court is

AFFIRMED.
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 placed 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 “pop-up” 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.

Opponents of new legislation 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. Supporters of new legislation believe that current laws are inadequate, as evidenced by the growth in spyware incidents.

In the first session of the 109th Congress, debate resumed, and the House again passed two bills (similar to the two passed in the 108th Congress): H.R. 29 and H.R. 744.1 In the Senate, three bills were introduced: S. 687, S. 1004, and S. 1608. S. 687 and S. 1608 were ordered reported from the Senate Commerce Committee during 2005. Legislative action during the 109th Congress on these bills is discussed later in this report.

A June 2006 report on spyware enforcement by the Center for Democracy and Technology (CDT) summarizes active and resolved spyware cases at the FTC and the Department of Justice, and in individual states.2

What is Spyware?

The term “spyware” is not well defined. Jerry Berman, President of CDT, explained in testimony to the Subcommittee on Communications of the Senate Commerce, Science, and Transportation Committee in March 2004 that “The term

1 The 108th Congress debated spyware legislation, and two bills passed the House, but neither cleared Congress. A summary of legislative action in the 108th Congress is included at the end of this report in the Appendix.

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.” More recently, in June 2006, the Anti-Spyware Coalition (ASC) issued a paper that defined spyware as “technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.”

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

---


4 The ASC is dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics, and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies. Its members include AOL, Cyber Security Industry Alliance, McAfee, Microsoft, SurfControl, US Coalition Against Unsolicited Commercial Email, and Yahoo. A complete list of the group’s members is available online at [http://www.antispyswarecoalition.org/about/index.htm].

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 keylogging software has been available for some time.\(^6\) 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.\(^7\)

Spyware remains difficult to define, however, in spite of the work done by groups such as the ASC and government agencies such as the Federal Trade Commission (FTC).\(^8\) As discussed below, this lack of agreement is often cited by opponents of legislation as a reason not to legislate. Opponents of anti-spyware legislation argue that without a widely agreed-upon 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, do, in fact, have legitimate uses. The question is whether the user has given consent for it to be installed.

**Prevalence of Spyware**

In October 2004, America Online (AOL) and the National Cyber Security Alliance (NCSA)\(^9\) released the results of a survey of 329 dial-up and broadband

---

\(^6\) 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.

\(^7\) 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.

\(^8\) The FTC has a spyware information page on its website, [http://www.ftc.gov/spyware](http://www.ftc.gov/spyware). Further, a report from the FTC's April 2004 workshop on spyware is available online at [http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf](http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf). This report contains a discussion on the difficulties of defining spyware.

\(^9\) According to its website [http://www.staysafeonline.org](http://www.staysafeonline.org), 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.
computer users regarding online threats, including spyware. According to the study:

- 80% of the computers they tested were infected with spyware or adware, and 89% of the users of those computers were unaware of it;
- the average infected computer had 93 spyware/adware components on it, and the most found on a single computer was 1,059; and
- 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.

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.

**FTC Advice to Consumers**

The Federal Trade Commission (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. The FTC alert listed the following clues:

- a barrage of pop-up ads;
- 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.

---


11 Spyware Infiltration Rises in Corporate Networks, but Webroot Survey Finds Companies Still Neglect Threat. PR Newswire, October 27, 2004, 06:00 (via Factiva).

12 Available at [http://www.ftc.gov/bcp/online/pubs/alerts/spywarealert.htm].
• 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.spywarewarrior.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 Beale, summarized the workshop at a hearing before the Subcommittee on Telecommunications and the Internet of the 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 affect [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.

---


14 The transcript of the workshop is available at [http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf].
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.\(^{15}\)

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.\(^{16}\) 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 actions to stop spyware practices. FTC Chairwoman Deborah Platt Majoras summarized the FTC’s activities at an October 5, 2005 hearing before the Subcommittee on Trade, Tourism, and Economic Development of the Senate Commerce, Science, and Transportation Committee.\(^{17}\)

**State Laws**

In March 2004, Utah became the first state to enact spyware legislation (although a preliminary injunction prevented it from taking effect, and the Utah legislature passed a new law in 2005 amending the 2004 act).\(^{18}\) In testimony to a House Energy and Commerce subcommittee in April 2004, then-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.”\(^{19}\)

---


\(^{16}\) An FTC press release, and a link to the report, are at [http://www.ftc.gov/opa/2005/03/spywarerpt.htm].

\(^{17}\) Ms. Majoras’ statement is available at [http://commerce.senate.gov/pdf/majoras-spyware.pdf].

\(^{18}\) 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).

In 2006, at least 18 states have considered spyware legislation and at least three have enacted/adopted that legislation: Hawaii, Louisiana, and Tennessee. Detailed listings of spyware legislation from 2004, 2005, and 2006, are available on the National Council for State Legislature’s website.20

Issues for Congress

The first session of the 109th Congress continued to debate the spyware issue. Two bills passed the House: H.R. 29 (Bono) and H.R. 744 (Goodlatte). Three bills were introduced in the Senate: S. 687 (Burns-Wyden), S. 1004 (Allen), and S. 1608 (Smith). S. 687 and S. 1608 were ordered reported from the Senate Commerce Committee in 2005. All the bills from the 109th Congress, 1st session, are summarized later in this report. Legislation from the 108th Congress is summarized in the Appendix.

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.21 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 (see CRS Report RL31953). 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 is true for spyware.

Several subcommittee or full committee hearings on spyware were held in 2004 and 2005 at which witnesses from the government, industry, and consumer groups laid out their various points of view:

- Senate Commerce, Science, and Transportation Committee, Subcommittee on Communications, March 23, 2004
- House Energy and Commerce Committee, Subcommittee on Telecommunications and the Internet, April 29, 2004
- House Energy and Commerce Committee, January 26, 2005
- Senate Commerce, Science, and Transportation Committee, May 11, 2005

**FTC's Position.** At the October 5, 2005 Senate Commerce subcommittee hearing, FTC Chairwoman Deborah Platt Majoras offered the FTC's formal position on the need for new spyware legislation for the first time. Ms. Majoras called spyware a "serious and growing problem" and reviewed FTC actions to protect consumers from it. She said that in the past year the FTC had initiated five law enforcement actions, and has ongoing investigations. She said that the FTC supports legislation that would enhance its ability to investigate and prosecute spyware distributors that are located abroad or who use foreign intermediaries. She specifically endorsed S. 1608, which was introduced by the subcommittee’s chairman, Senator Smith. She also said the FTC could support legislation giving it authority to seek civil penalties against spyware distributors. Further, she said that the FTC would continue to coordinate with federal and state partners in bringing law enforcement actions under existing law, and to educate consumers about the risks of spyware and anti-spyware tools. She also noted, however, that technological solutions are needed.

Absent a formal FTC position, two commissioners, Orson Swindle and Mozelle Thompson, previously had offered personal views on the spyware issue. Both have since left the Commission. Neither supported new legislation at the time of their statements. Mr. Swindle 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

---


23 Ms. Majoras offered similar statements in a February 9, 2006, speech at the Anti-Spyware Coalition public meeting, available online at [http://www.ftc.gov/speeches/majoras/060209editspyware.pdf].

24 FTC Chairwoman Majoras' statement is available at the Senate Commerce Committee's website at [http://commerce.senate.gov/pdf/majoras-spyware.pdf].
definition of the term. 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, 26 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 April 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.”

**Industry Positions.** At the March 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 March 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. 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 April 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 January 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.28

At the May 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.”29 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.”30 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 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.”31

30 Hughes, May 11, 2005 Senate Commerce Committee testimony, Ibid.
31 Testimony of C. David Moll, Webroot Software, to the Senate Commerce, Science, and (continued...
The Information Technology Association of America (ITAA) reportedly supports H.R. 744.32

Meanwhile, in January 2006, an industry coalition launched a website — [http://www.stopbadware.org] — to gather data from consumers about their experiences with spyware and other “badware” programs. The website describes itself as a “neighborhood watch” type of organization, and a clearinghouse for research on “badware and the bad actors who spread it.” The industry coalition includes technology companies Google, Lenovo, and Sun Microsystems.

**Consumer Groups and Others.** At the March 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 three other hearings.

More recently, CDT issued a report on spyware enforcement that summarizes active and resolved spyware cases at the FTC and the Department of Justice, and in individual states.33

**Legislation in the 109th Congress, 1st Session**

Two bills passed the House on May 23, 2005 — 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). Three bills were introduced in the Senate — S. 687 (Burns), which is similar to legislation that was considered in 2004, but did not reach the floor (S. 2145); S. 1004 (Allen); and S. 1608 (Smith). S. 687...

---

31 (...continued)
