TRENDS IN INTERNET LITIGATION

By

Paul C. Van Slyke
Philip T. Golden

Locke Liddell & Sapp
3400 Chase Tower
600 Travis Street
Houston, Texas 77002
(713) 226-1200

Presented to
Houston Bar Association
Legal Seminar
September 16, 1999

TABLE OF CONTENTS

TRENDS IN INTERNET LITIGATION

I. Introduction

Internet usage has exploded since its inception less than a decade ago, and promises to continue to grow at a remarkable rate into the next millennium. Nowadays, even the most clandestine company maintains an informational Website, while other more aggressive companies take advantage of the burgeoning e-commerce market by offering goods or services for sale over their Websites. As the Internet has developed and expanded, however, it has become a breeding ground for litigation.

Because cyberspace is seemingly infinite and its global reach vast, courts have struggled with various legal issues such as domain name disputes, copyright infringement, and First Amendment issues. Likewise, the courts have attempted to apply earthbound consumer protection laws, advertising rules, warranties, debt collection statutes, securities laws, and contracting protocols to the virtual world and especially to Internet-based transactions.

This paper attempts to address some of the recent trends in Internet litigation as they arise in privacy cases, personal jurisdiction, spam mail, domain name disputes, trademark and unfair competition litigation, copyright infringement, First Amendment issues, and electronic commerce.

II. Trends in Privacy Cases

The Internet provides countless opportunities for distributing personal information with ease and speed. As a result, the possibility for conflicts involving privacy rights and the Internet is quite substantial. Profiles of individuals can be compiled from Internet activities and then distributed to commercial entities, without the individual ever learning that this activity has occurred. Traditionally, American law has provided more extensive protection from governmental invasions of privacy than from invasions made by individuals or commercial entities. The Internet, however, may cause a shift in the privacy area as laws change to accommodate the growing number of privacy invasions by non-government parties via the Internet. Several representative case are outlined below.

A. McVeigh v. Cohen, *983 F. Supp. 215 (D.D.C. 1998)*

Timothy McVeigh, a U.S. Naval Officer, brought this action to enjoin the United States Navy from discharging him under the statutory policy commonly known as the "Don't Ask, Don't Tell, Don't Pursue" policy. McVeigh contended that while investigating his sexual orientation, the Navy violated his rights under the Electronic Communications Privacy Act ("ECPA"), the Administrative Procedure Act, Naval policy, and the Fourth and Fifth Amendments of the U.S. Constitution. The discharge proceedings were based upon information that a Navy paralegal had gathered from American Online without first obtaining a warrant and issuing a subpoena, as required by the ECPA. The court granted McVeigh a preliminary injunction and decided that the Navy had "impermissibly embarked on a search and 'outing' mission." The court decided that information gained via the Internet was not "credible information" under the Navy's policy because "particularly in the context of cyberspace, a medium of 'virtual reality' that invites fantasy and affords anonymity, the comments attributed to McVeigh do not by definition amount to a declaration of homosexuality."

B. Jessup-Morgan v. America Online, Inc., *20 F. Supp. 2d 1105 (E.D. Mich. 1998)*

A subscriber to American Online, Inc. ("AOL") sued the electronic communication service provider alleging violation of the Electronic Communication Privacy Act, breach of contract, breach of express and implied warranties, negligence, fraud and misrepresentation, and invasion of privacy arising out of the provider's disclosure of her identity pursuant to a subpoena. The subscriber allegedly posted a sexually explicit message meant to harass and injure a third party. The third party served a civil subpoena on AOL for information which would identify the AOL member who authored the injurious message. In compliance with the subpoena, AOL sent a two-page summary containing basic identity information on the AOL account from which the sexually explicit message originated. The summary revealed that Jessup was the holder of the account. She then sued AOL for various damages in excess of $47 million. The court, however, granted AOL's various motions for judgment on the pleadings or for summary judgment.

C. Liu v. DeFelice, *6 F. Supp. 2d 106 (D. Mass. 1998)*

Upon receiving a copy of her credit report, Mary Liu discovered that Gerard Defelice accessed privileged credit information relating to her without her authorization. She brought suit against him in Massachusetts for violations of federal and state consumer credit reporting acts and state consumer protection laws. DeFelice, a New York resident, unsuccessfully moved to dismiss for lack of personal jurisdiction.

D. Zeran v. America Online, Inc., *129 F.3d 327 (4th Cir. 1997)*

Kenneth Zeran brought a lawsuit against American Online, Inc. ("AOL") arguing that AOL unreasonably delayed in removing defamatory messages posted on an AOL bulletin board by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter. The postings described the sale of T-shirts featuring offensive and tasteless slogans related to the April 18, 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, that also included death threats. Zeran sued AOL for negligence, claiming that allowing the notices to be posted and remain on the board constituted negligent conduct. The Fourth Circuit upheld the lower court's dismissal of the case on the ground that Section 230 of the Communications Decency Act, which addresses protection for the private blocking and screening of material, confers immunity on Internet Service Providers with respect to information posted on their sites by third parties.

III. Trends in Personal Jurisdiction Issues

While personal jurisdiction is a topic that is broader than intellectual property law, many personal jurisdiction cases involving the Internet are based on intellectual property causes of action. Thus, although the personal jurisdiction issue is important to all attorneys, the issue is particularly important to intellectual property attorneys. This section of the article summarizes several recent or significant personal jurisdiction decisions regarding the Internet.

From the case law, a framework is emerging for determining the type of on-line activities that may be within the reach of state long-arm statutes and comport with the notions of due process. Although the reach of long-arm statutes vary, they typically cover those defendants who either transacted business within the forum state; committed a tortious act within the forum state; or committed a tortious act outside the forum state that resulted in harmful consequences suffered within the forum state when coupled with additional requisites, such as either a persistent presence in the forum, a regular solicitation within the state, or a reasonable expectation of being haled into the forum state's courts. Although courts have generally been successful in applying the traditional notions of personal jurisdiction to most Internet-related cases, they have faced several problems along the way.

One problem that has arisen between traditional personal jurisdiction principles and Internet-based lawsuits involves the traditional expectation that defendants with the means to conduct commerce in multiple states should be expected to have the means to be subject to litigation in multiple states as well. The Internet allows entities to conduct business simultaneously and continuously in a potentially unlimited number of locations. However, every person who conducts business over the Internet cannot afford to litigate lawsuits in a possibly unlimited number of locations. Thus, the principle stated above likely fails when applied to Internet situations.

A second problem involving the Internet and personal jurisdiction concerns the constitutional requirement that a defendant's entry into the forum territory to do business must involve "purposeful availment." According to the United States Supreme Court, a defendant may only be sued where he has "purposefully established 'minimum contacts'" via "some act by which [he] purposefully avails [himself] of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of the laws." *Burger King v. Rudzewicz,* 105 S.Ct. 2174, 2183 (1985). In a transaction over the Internet, the two actors involved potentially may never know each others physical location or identity. Therefore, an Internet actor may enter a jurisdiction without actually having notice of doing so. Courts are then faced with the dilemma of deciding whether or not such an actor has "purposefully availed" himself of the protection of the laws of that jurisdiction.

The landmark decision in this area, *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), discussed below, established three general categories or levels of Internet "presence" for Web sites to which personal jurisdiction over a non-forum defendant is considered to be proper or improper: active; interactive; and passive. Some court decisions describe "active" sites that usually involve a defendant transacting business with persons in the forum state over the Internet, sending goods, transmitting software, or performing services intended to be used or delivered in the forum state. Other decisions involve Websites accessible to users in forum states, but where the Web site holder did not actually transact business with persons in the forum states. These cases involved "passive" Websites, where the Webhost only advertised its goods or services. The final set of cases relates to so-called "interactive" Web sites that involve users who obtain and transmit information via the Website. However, in these cases, the parties did not actually transact any independent business, and did not ship goods or services, other than the exchange of information.

A. Personal Jurisdiction Held Proper

1. *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997)

Zippo, is cited as the preeminent example of a court's exercise of jurisdiction over an Internet defendant. In *Zippo*, the defendant was an Arizona company that offered an Internet news service on the World Wide Web. On the "Zippo Dot Com" page, a customer who wants to subscribe to the service need only visit the Website, fill out an application, and pay by credit card over the Internet or by telephone. The plaintiff was a Pennsylvania manufacturer of cigarette lighters, who sued the defendant for trademark infringement. The district court found that the exercise of jurisdiction over Zippo Dot Com was proper because of the defendant's repeated and conscious choice to process Pennsylvania residents' applications. The court highlighted the defendant's solicitation of business in Pennsylvania, noting that:

> We are not being asked to determine whether Dot Com's *Website alone* constitutes the purposeful availment of doing business in Pennsylvania . . . [rather] we are being asked to determine whether Dot Com's *conducting of electronic commerce* with Pennsylvania residents constitutes the purposeful availment of doing business in Pennsylvania.

Id. at 1125-26 (emphasis added). Therefore, based on the defendant's approximately 3,000 individual subscriptions and seven access provider agreements in Pennsylvania, the court found that the defendant had "purposefully availed" itself of doing business in the Commonwealth, thereby allowing the proper exercise of jurisdiction.

In its opinion, the court set out what has been identified as the beginnings of the personal jurisdiction/Internet framework through establishing a spectrum against which to measure Websites.

"If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. *E.g., CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996). At the opposite end are situations where a defendant has simply posted information on an Internet Website that is accessible to users in foreign jurisdictions. A passive Website that does little more than make information available to those who are interested in it is not ground for the exercise of personal jurisdiction. *E.g. Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295 (S.D.N.Y. 1996). The middle ground is occupied by interactive Websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Website. *E.g., Martiz, Inc. v. Cybergold, Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996).

2. *Hasbro, Inc. v. Clue Computing, Inc.*, 994 F. Supp. 34 (D. Mass. 1997)

The United States District Court for the District of Massachusetts found the exercise of personal jurisdiction proper over a Colorado defendant. The Massachusetts plaintiff sued the Colorado defendant for trademark infringement based on the defendant's domain name "clue.com." The relevant portion of the Massachusetts long-arm statute requires tortious acts committed elsewhere which cause harm within the Commonwealth to be coupled with either regular solicitation of business, continuing contacts, or the derivation of substantial revenue from the Commonwealth. The court found that the Website was created for the sole purpose of broadening the company's customer base. Additionally, the site was accessible 24 hours a day, seven days a week and included a statement that the company would provide services to any customer site. Further, the Website boasted Digital Equipment Corporation ("Digital"), a Massachusetts company, as a client, presumably to benefit from their name recognition. Combining these elements, the court found that the defendant did regularly solicit business in Massachusetts, therefore placing the defendant within the reach of the Commonwealth's long-arm. The court found due process to be satisfied based on several facts. First, the court noted that the defendant had directed advertising to all states without attempting to avoid Massachusetts. Further, the defendant had knowingly worked for Digital and Digital provided a third to one-half of the defendant's annual income in one year. Finally, the court noted that the Website was interactive in that it provided the capability to E-mail the company directly from the site.

3. *Telco Communications v. An Apple a Day*, 977 F. Supp. 404 (E.D. Va. 1997)

A Virginia plaintiff sued a Missouri defendant for among other things, defamation in Internet press releases from which the plaintiff's stock prices suffered. The Virginia long-arm reaches tortfeasors whose extraterritorial actions result in injury within Virginia when that tortfeasor regularly conducts or solicits business from the Commonwealth, engages in any other persistent course of conduct, or derives revenue from services or goods sold in the Commonwealth. The court held, and the defendant admitted, that the press releases were advertisements, and therefore, a solicitation of business over the Internet. Internet access 24 hours a day, seven days a week, proved sufficient regularity. The court also noted that the acts amounted to torts committed in the Commonwealth because without the Internet service providers and users in Virginia, the alleged tort would not have occurred in Virginia. The court held the exercise of jurisdiction to comport with due process since the defendant knew the statements would be damaging to the plaintiff and was aware of the location of the plaintiff in Virginia. Therefore, the defendant could have reasonably expected to be haled into a Virginia court.

4. ***Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn. App. Ct. 1997)**

The State of Minnesota sued a Belize defendant for deceptive trade practices, false advertising, and consumer fraud based on the defendant's operation of an on-line betting service, WagerNet. Although the long-arm sets forth specific prongs, Minnesota precedent stretches the long-arm reach to the Constitutional limit and the court jumped directly to the due process analysis. In its decision, the court held that "minimum contacts" were established because the site was available 24 hours a day, seven days a week to Minnesota residents and was, in fact, accessed by residents of the forum state. Further, the court held that the site, which included toll-free numbers for further information, existed to solicit subscribers. Finally, the court noted this was not a billboard just over the state line, but more pervasive and invasive as "WagerNet tells its prospective customers WagerNet may sue them in the customer's home forum or Belize at WagerNet's option."

5. ***Cody v. Ward*, 954 F. Supp. 43 (D. Conn. 1997)**

The United States District Court for the District of Connecticut found personal jurisdiction proper over a California defendant. The Connecticut plaintiff brought action against the California defendant for fraudulent misrepresentations made to potential investors via the Internet regarding stock. The court held that the Connecticut long-arm reached the defendant as committing "a tortious act within the state." Connecticut case law, unlike New York's, does not require that the defendant be physically present in the state when the tort is committed. Instead, the court held that the Internet statements made their way into the state based on state precedent finding that "false representations entering Connecticut by wire or mail constitute tortious conduct in Connecticut." In holding due process satisfied, the court found it reasonable that the defendant anticipated being haled into a Connecticut court based upon the allegations of fraudulent misrepresentations made through a series of telephone calls and E-mail messages.

6. ***Heroes, Inc. v. Heroes Foundation*, 958 F. Supp. 1 (D.D.C. 1996)**

The U.S. District Court for the District of Columbia found personal jurisdiction proper in a trademark infringement case brought by a Washington, D.C. plaintiff against a New York defendant. The D.C. long-arm extends to those who transact business in the District and those who cause harm in D.C. by an act committed outside the District when the actor either regularly does business in the forum, engages in persistent conduct, or derives revenue from the forum. The court found a newspaper advertisement in the Washington Post for the defendant's charity to both constitute transacting business in the forum and causing harm in the forum from outside the forum. It was the defendant's Internet Webpage that proved to be evidence of the defendant's "persistent conduct" in the forum state. Solicitation of donations on-line established the requisite "minimum contacts." The court noted that because the defendant's home page was not the only contact, the court did not need to decide whether the defendant's Website by itself subjected the defendant to personal jurisdiction.

7. *Panavision Int'l, L.P. v. Toeppen*, 938 F. Supp. 616 (C.D. Cal. 1998)

A California plaintiff sued an Illinois defendant, a "cybersquatter," for trademark infringement and dilution. The California long-arm, expressly written as reaching the full due process limit, sent the court directly to looking for purposeful availment. Because the defendant registered the plaintiff's mark with the intent to affect the plaintiff's business, the tort was found to be clearly directed at the plaintiff and therefore at the forum state. The court went on to find a sufficient nexus between the defendant's actions and the cause of action by stating that "but for" the defendant's actions the plaintiff could have easily registered a site under their own trademark. Finally, the court found it reasonable that the defendant anticipate being haled into a California court since his actions were aimed a California company.

8. *Maritz Inc. v. Cybergold Inc.*, 947 F. Supp. 1328 (E.D. Mo. 1996)

This case is perhaps an example of an "interactive" Website, for which the court found personal jurisdiction proper over a California defendant after a Missouri plaintiff sued for trademark infringement and unfair competition, based on the defendant's domain name. The relevant prong of Missouri's long-arm reaches tortfeasors who commit a tortious act within the State. The court followed precedent extending that prong to a defendant corporation where the sole basis for jurisdiction was an extraterritorial act of tortious interference with a contract that produced an effect in the State and held jurisdiction proper under the long-arm "even assuming Cybergold's allegedly infringing actions were wholly outside Missouri." The Internet Website, soliciting to sign up users on an advertising mailing list and accessed more than one hundred times by forum state residents, satisfied due process.

9. *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996)

Patterson, the defendant, was a Houston, Texas-based attorney and software developer who subscribed to CompuServe, an Ohio plaintiff that sued Patterson for trademark infringement and unfair competition. The *CompuServe* court held that the defendant "transacted business" within the meaning of the long-arm through transmitting files to the plaintiff's service that was then available for downloading by the plaintiff's subscribers. The court held due process was met by the defendant's file transmissions, others accessing the software via the plaintiff's system, the defendant's advertising and selling products through the plaintiff's system, and an existing ongoing relationship between the parties, which included a contract. The court held the above actions were directly related to the cause of action and that the defendant therefore could reasonably expect to be haled into an Ohio court.

10. Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996)

A Connecticut plaintiff sued a Massachusetts defendant for trademark infringement based on the use of the Internet domain name “www.inset.com” and a toll-free number on a Website. The Connecticut long-arm extends to causes of action arising out of business solicitations in the state if the defendant repeatedly solicited business whether orders or offers relating to the solicitation were accepted within or without the state. The U.S. District Court for the District of Connecticut held advertising via the Internet as solicitation of sufficient repetition to satisfy that prong of the long-arm. The court likened that activity to multiple advertisements over a period of time in a local newspaper. Continuously directing advertisements via the Internet and the toll-free number on the site toward all states established purposeful availment

11. *Thompson v. Handa-Lopez, Inc.*, 998 F. Supp. 783 (W.D. Tex. 1998)

A federal district court sitting in San Antonio held that it had jurisdiction over a California corporation that operated a casino arcade site on the Internet. The lawsuit was brought by a Texas resident who sued for the winnings owed him by the casino. The *Thompson* court, in going through the *Zippo* analysis, concluded that the Website was sufficiently interactive to justify the imposition of specific jurisdiction.

B. Personal Jurisdiction Held Improper

1. *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 (2d Cir. 1997)

This case typifies the jurisdictional analysis for defendants who maintain a “passive” Internet presence. In *Bensusan*, the defendant operated a Webpage out of Columbia, Missouri, which advertised information about the “Blue Note” club in Columbia. The site did not solicit commercial transactions across the Internet, but rather provided phone numbers so that interested persons could call to ask about upcoming shows. The plaintiff was the New York-based operator of a cabaret called “The Blue Note.” The plaintiff held a federal trademark for “The Blue Note,” and sued King for infringement of that mark. The court found that the exercise of jurisdiction was improper in this case because the activity giving rise to the lawsuit - including the authorization and creation of the Website and the use of the “Blue Note” name and logo - were performed by persons in Missouri and not in New York. The court concluded that because the defendant did not solicit business in New York, it cannot be amenable to jurisdiction based on an informational Website.

2. *Cybersell, Inc. v. Cybersell, Inc.,* 130 F.3d 414 (9th Cir. 1997)

The Ninth Circuit affirmed that an exercise of personal jurisdiction by an Arizona court over a Florida defendant based on passive Web contact alone would be improper. The Arizona plaintiff, the owner of the federally registered trademark "Cybersell," sued the Florida defendant that was operating an Internet Website bearing the allegedly infringing mark "Cybersell." The defendant was using this mark to advertise its Webpage development services. The Arizona long-arm statute permits an Arizona court to "exercise personal jurisdiction over parties, whether found within or outside the state, to the maximum extent permitted by the Constitution of this state and the Constitution of the United States." Ariz. R. Civ. Pro. 4.2(a). The Plaintiff conceded that general jurisdiction is not available in Arizona and therefore argued that specific jurisdiction was applicable. The Arizona courts find "purposeful availment" in a nonresident defendant's "deliberate action within the forum" or "continuing obligations to the forum residents." *Ballard v. Savage*, 65 F.3d 1495 (9th Cir. 1995).

In this case of first impression for the Ninth Circuit, the court looked to the decisions of other jurisdictions for guidance. In recognizing the spectrum from interactive to passive Websites, the court noted that passive Websites alone have not typically been enough to establish specific jurisdiction. *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997). The court also took note of other jurisdictions that looked to the number of "hits" a site received from residents of the forum state. *Heroes, Inc. v. Heroes Foundation*, 958 F. Supp. 1 (D.D.C. 1996). In summary, the Ninth Circuit agreed with the *Zippo* court in recognizing that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet." *Zippo*, 952 F. Supp. at 1124. The Ninth Circuit opinion noted in the *Cybersell* case that the Defendant did not encourage Arizona residents to access their Website; there were no "hits" by Arizona residents to the Defendant's site (except by the Plaintiff); there were no contracts formed; sales or phone calls exchanged; or income or messages received from Arizona residents. As such, the Defendant's actions lacked "purposeful availment" of the laws of Arizona and an extension of specific jurisdiction was held improper.

3. *Weber v. Jolly Hotels*, 977 F. Supp. 327 (D.N.J. 1997)

The plaintiff, a New Jersey resident, booked a hotel room with the defendant, an Italian hotel operator, through a Massachusetts travel agent. The plaintiff, while staying at the defendant's hotel, incurred a physical injury and filed suit against the defendant in a New Jersey court. The defendant maintained advertisements on its own Website, thus the plaintiff sought to establish general personal jurisdiction based on the Website. With New Jersey's long-arm reaching the full constitutional extent, the court looked directly to due process limitations. The court held that no sufficient "minimum contacts" were established because the plaintiff's travel agent was not the sole agent for the hotel and neither the defendant nor the travel agent had specifically targeted New Jersey to solicit business.

4. *Smith v. Hobby Lobby Stores, Inc.*, 968 F. Supp. 1356 (W.D. Ark. 1997)

The U.S. District Court for the Western District of Arkansas found personal jurisdiction improper over a Hong Kong manufacturer of artificial Christmas trees. Plaintiff, an Arkansas resident, brought a wrongful death action against Hobby Lobby Stores, Inc. ("Hobby"), the store that sold an artificial Christmas tree for which a fatal house fire was attributed. Hobby filed a third-party complaint against the Hong Kong manufacturer. The Arkansas Code permits the courts of the State to maintain personal jurisdiction "to the maximum extent permitted by the due process of law clause." Thus, the court looked directly to the due process requirements. The Hong Kong manufacturer maintained an advertisement accessible to Arkansas residents via the Internet. The court found the advertisement "simply insufficient contact" to satisfy due process. The court noted the contact was a mere advertisement and that the company did not contract to sell any goods or services to any Arkansas citizens over the Internet.

5. *Agar Corp., Inc. v. Multi-Fluid, Inc.*, Civ. Act. No. 95-5105 (S.D. Tex., June 25, 1997)

A Texas plaintiff sued the Colorado subsidiary and its Norwegian parent company for patent infringement and unfair competition based on offers for sale appearing over the Internet for allegedly infringing technology. The United States District Court for the Southern District of Texas Houston Division expressly held there were no grounds present for specific or general jurisdiction over either the Colorado defendant or the Norwegian defendant. The Texas long-arm reaches those nonresidents "doing business" within the state. "Doing business" has been interpreted broadly, essentially making a personal jurisdiction question under the Texas long-arm a constitutional question.

The court first analyzed HiTec's (the Norwegian parent company) motion to dismiss for lack of specific jurisdiction. Specific jurisdiction requires that the allegedly tortious activity be "purposefully directed" at the forum. In applying the traditional standard to the modern Internet medium the court looked to the three Website categories established in *Zippo*. The court held that the Website in question was "largely passive" in that customers could not purchase products or set up contractual relationships through the site. Additionally, out of the site's seven pages there were only two "buttons" providing opportunities for feedback and registration. The court held that merely placing an offer for sale on the Internet does not establish specific jurisdiction. Further, the court stated that a passive Website does not seek out a customer but resides in "cyberspace" waiting for a visitor; therefore, the sponsor of such a site cannot purposefully direct the information to any particular jurisdiction. The court went on to state that while the defendant may have reasonably expected Texas residents to visit the site, it surely did not and could not purposefully direct its site at Texans.

In its analysis of general jurisdiction, the court relied on the *Hearst* court's classification of a passive site as a "distribution." Since a distribution is not the equivalent of "doing business" in the Fifth Circuit, the court held that an exercise of general jurisdiction would be improper.

The court considered additional claims for jurisdiction over the defendants based on other activities, but no basis was found.

6. *Hearst Corp. v. Goldberger*, No. 1997 WL 97097 (S.D.N.Y. 1997)

The United States District Court for the Southern District of New York held that personal jurisdiction was lacking under the New York long-arm statute. The New York plaintiff sued the New Jersey defendant for his use of the domain name and Website, "esqwire.com." The defendant used his Website to advertise legal office networking services that he would soon publicly offer for sale. The court found that the defendant had not transacted business in New York because his business was not yet operational, and further that he had not committed a tort in New York because he was not physically present in the State, as required by New York case law. New York's long-arm provision for jurisdiction over tortfeasors whose actions outside the state cause injury within the state requires the plaintiff to establish that the defendant: (a) regularly solicits or does business in the state; or (b) has a reasonable expectation of causing harm in the state and derives substantial revenue from interstate commerce. The court found that they met none of the requisites because the defendant had no product to sell at the time of the alleged infringement. Since they did not establish the requisites, the court did not even consider if a harm was caused within the state. Without the State's long-arm reach, the Constitutional issue was not addressed.

7. IDS Life Insurance Co. v. Sunamerica, Inc., 958 F. Supp. 1258 (N.D. Ill. 1997)

The United States District Court for the Northern District of Illinois found jurisdiction improper in a suit alleging multiple charges including violations of the Lanham Act and Copyright Act, and misappropriation of trade secrets. The Illinois long-arm statute reaches those who commit torts within the state and those doing business in the State. In Illinois, "doing business" is defined by regular activities with "a fair measure of permanence and continuity." Because the plaintiff failed to sufficiently plead that improper solicitation of the plaintiff's employees by the defendant was a tort in the State, the court considered whether the defendant was "doing business" within the State. The court did not find the defendant's Internet advertisements sufficient to establish "regular activities" stating that such a finding would subject any defendant advertising on the Internet to jurisdiction. Besides determining that the Illinois long-arm failed to reach the defendant, the court also commented that such an exercise of jurisdiction would be Constitutionally impermissible as such an exercise would "offend traditional notions of fair play and substantial justice."

8. McDonough v. Fallon McElligott, Inc., 40 U.S.P.Q. 1826 (S.D. Cal. 1996)

The plaintiff, a California photographer, sued the defendant, a Minnesota advertising agency, for copyright infringement, unfair trade practices, and a violation of privacy and publication rights. The defendant used some of plaintiff's copyrighted photographs without permission in advertisements created for a client. While none of the plaintiff's materials were alleged to be on the defendant's Website, the plaintiff argued that the Website established sufficient contact with California. The California long-arm permits an exercise of jurisdiction "on any basis not inconsistent with the constitution of this state or the United States." The court held that the defendant had not availed itself of California benefits merely by advertising on his Website since the advertisement did not draw on California sources, concern California activities, or target California.

IV. Trends in Internet Spam Litigation

Anyone with an Internet E-mail account is familiar with unsolicited "junk" E-mail. In-boxes are packed with these messages from unfamiliar addresses. Most offer some commercial proposition, from benign get-rich-quick schemes to less-innocent advertisements for sexually explicit Websites. For most people, these mass mailings are merely a nuisance. However, there is growing concern that such messages are hogging Internet bandwidth and impeding the Net's continued growth. Others view unsolicited junk E-mail as an invasion of privacy. However the situation is viewed, the solution to the problem of junk advertisements presents a unique challenge to the law.

A large portion of Internet litigation to date has revolved around this unsolicited commercial E-mail, or "spam." Unlike traditional direct junkmail or telemarketing, spam imposes costs on consumer E-mail recipients and the Internet Service Providers who must direct, redirect, and process spam. This is because spam arrives at an E-mail box via the services of "private" actors - Internet service providers, online communities, and networks, at a cost to the recipient (like a collect call). On the other hand, junkmail and telemarketing arrive by way of the postal service or telephone lines, quasi-public means of communication that impose costs on the sender rather than the recipient.

Currently, some are attempting to regulate spam by various nonlegal means. One effort involves reliance on informal guidelines governing behavior on the Net, known as Nettiquette. Such guidelines are largely worthless when dealing with spammers because spammers ignore them. Since Nettiquette is informal and lacks the power of law, spammers can ignore it with impunity. Generally, if someone is sent unsolicited E-mail, he or she could reply to that message asking that he or she not be sent any more. However, many spammers avoid these responses by concealing their identities (*i.e.*, they provide false return E-mail addresses), making such replies unavailing. Because Nettiquette lacks enforcement, it is practically worthless as an anti-spam tool.

Beyond the problems between spammers and Internet users, there is also friction between spammers and the various Internet service providers ("ISPs"), who make E-mail services available for the use and enjoyment of the Internet community. ISPs, who are receiving complaints from their subscribers, are looking for ways to shut down spammers, or at least force them to find another service provider. However, such disputes are likely to be resolved by interpretation of various contractual provisions, at least in the future.

Courts, Congress, and many state legislatures are seeking to, or already have, imposed limits on spamming. There are multiple bills currently pending in Congress and various state legislatures that have the purpose of controlling spam. For example, California enacted two statutes, effective on January 1, 1999, which attempt to restrict and curtail spamming. "The Miller Bill" outlaws cloaking and spoofing and allows Internet Service Providers to recover damages from spammers. "The Bowen Bill" requires spammers to label their bulk E-mail "ADVERTISING" and to provide readers who wish to be removed from bulk mailing lists with the opportunity to have their name deleted. Thus, either an accurate return address or toll-free telephone number for the spammer must be included on the mail message.

Some of the litigation that has arisen from spam involves the large Internet service providers, such as American Online, who have attempted to thwart the most abusive spammers with legal action. Although ISPs have taken the lead in prosecuting such cases, the Federal Trade Commission and state governments have also joined the fray with enforcement actions of their own and by enacting statutes geared to protect consumers and ISPs from the negative aspects of spam.

A. *Cyber Promotions, Inc. v. America Online, Inc.,* 948 F. Supp. 436 (E.D. Pa. 1996)

These consolidated actions present the issue of whether, under the First Amendment of the U.S. Constitution, a private company has the right to spam subscribers of another private online company over the Internet and whether the private online company has the right to block the spam from reaching its subscribers. *Cyber Promotions, Inc. v. America Online, Inc.,* 948 F. Supp. 436, 437 (E.D. Pa. 1996). The court held that without State action, the private online service has the right to block the spam from reaching its subscribers via the Internet. In their opinion, the court decided that although AOL, the private online provider wanting to block the spam, had indeed opened its E-mail system to the public, that was not enough to qualify as the exercise of a municipal power or an essential public service (*i.e.,* state action).

B. *CompuServe, Inc. v. Cyber Promotions*, No. C2-96-1070 (S.D. Ohio)

Following the lead of AOL, in 1996, CompuServe, the large online computer network and access provider, brought suit against Cyber Promotions and Sanford Wallace, its president. CompuServe had apparently been fighting a pitched battle against Cyber Promotions and its spam for months prior to filing suit. After receiving thousands of customer complaints and subscription cancellations over the amount of spam being received by CompuServe subscribers and the effect of that spam on system operations, CompuServe requested that Cyber Promotions cease and desist from sending spam to its subscribers. Instead of complying with this request, Cyber Promotions actually increased the volume of spam it was sending to CompuServe's subscribers. CompuServe then attempted to block Cyber Promotions' spam by installing spam filtering software. Cyber Promotions began to sidestep this technological block by spoofing and reconfiguring its servers to conceal its domain name.

After obtaining a temporary restraining order prohibiting Cyber Promotions from using CompuServe accounts, equipment or services to send or receive E-mail and prohibiting Cyber Promotions from spoofing its spam with CompuServe return addresses, CompuServe moved for a permanent injunction continuing the terms of the temporary restraining order and to bar Cyber Promotions from sending spam to any E-mail address maintained by CompuServe.

In a lengthy opinion granting CompuServe a permanent injunction, Judge Graham, citing the Restatement of Torts, found that Cyber Promotions committed a trespass because, although Cyber Promotions did not take possession of CompuServe's equipment, the spam nonetheless "intentionally intermeddled" with CompuServe's computer systems and that intermeddling resulted in a loss of value to that equipment because the drain on the CompuServe network caused by Cyber Promotions spam reduced the system resources available to CompuServe's subscribers. Moreover, the resultant complaints and cancellation of subscriptions suggested that CompuServe's goodwill and business reputation had also been harmed.

The case settled a few weeks after entry of the Injunction. The terms of the settlement eliminated Cyber Promotions' ability to spam CompuServe's system by providing that Cyber Promotions would not spoof and would not send any E-mail to any CompuServe subscriber unless that subscriber specifically requested such E-mail. In addition, Cyber Promotions paid CompuServe $65,000 in attorneys fees. In return, CompuServe agreed to allow Cyber Promotions to send verifiably requested E-mails and advertise on CompuServe's network.

C. *Seidl v. Greentree Mortgage Co*., No. 97-WY-2087-AJ (D.Colo.)

Since May 14, 1995, Seidl, through his business has owned the registered domain name "localhost.com." Seidl's system uses the administrative address "nobody@localhost.com" to forward E-mail received by the domain to Seidl, the system administrator.

In January 1997, Greentree Mortgage Company, a New Jersey-based entity, through a bulk E-mailer, sent spam to several thousand people, advertising Greentree's mortgage services. Unbeknownst to Seidl, the spam message "spoofed" his domain name - the "from" address on the spam appeared as "nobody@localhost.com" - and the return path, the numeric code which directs undeliverable messages and responses sent using the "reply" function, was also altered to direct such replies to "nobody@localhost.com."

During the days and weeks that followed Seidl's system was overrun by some 7,000 messages using some 31 megabytes of memory. According to the Verified Complaint filed by Seidl, his system was continuously occupied by the task of processing these replies for three days. Early on, Seidl telephoned and requested that the mailing be halted. The defendant admitted being involved with the sending of the spam but refused to take any action to halt the spam or compensate Seidl for his damages.

In his Complaint, Seidl seeks compensatory and punitive damages under various Colorado statutes regulating unfair and deceptive trade practices. Seidl also seeks recovery under theories of trespass, negligence and invasion of privacy alleging that Greentree knew it had no right to "localhost.com" domain name and that Greentree could have easily determined that the domain was registered to Seidl through Internic. The lawsuit is still in litigation.

V. Trends in Internet Domain Name Disputes

The future of commerce on the Internet is intricately connected first and foremost with domain names. Domain names are a company's location, advertising, slogan, and business card all rolled into one. As long as controversy and uncertainty surrounds the issue of domain names, the Internet will not reach its full potential as a medium of commerce.

One of the most famous early domain name controversies involved Adam Curry and MTV. *MTV Networks v. Curry*, 867 F. Supp. 202 (S.D.N.Y. 1994). Adam Curry, an MTV video jockey, registered the name "mtv.com" with the approval of MTV management. When Curry left MTV, MTV sued to recover the domain name "mtv.com." A court never reached the merits of the case, and they ultimately settled the dispute. The court, however, did address pre-trial motions. In a published opinion related to these motions, the court noted that domain names are similar to telephone number mnemonics. Many scholars have taken note of this and analyzed domain name trademark problems in the context of telephone number mnemonic trademark cases.

For example, trademark law allows alphanumeric mnemonic telephone numbers to be used in such a way as to warrant trademark protection. In *Dranoff-Perlstein Associates v. Sklar*, 967 F.2d 852 (3d Cir. 1992), the two parties used almost identical telephone mnemonics. In 1984, Dranoff-Perlstein began using "INJURY-1" as the telephone number for their personal injury law practice. In 1990, Harris Sklar began using "INJURY-9" as the telephone number to identify his law practice. Dranoff-Perlstein filed suit against Sklar for trademark infringement and state trademark dilution. The court held that the alphanumeric combination "INJURY" was generic. The addition of a "1" or "9" to the end of INJURY did not sufficiently change the generic nature of the word. The court remanded the case because they could not determine from the facts whether secondary meaning had been established.

Besides the dispute between Adam Curry and MTV, there have been many other conflicts over the ownership and use of domain names. Princeton Review registered its competitor's probable domain name - "kaplan.com" - and used the site to solicit and list complaints about Kaplan. Joshua Quittner, a writer and reporter, registered the domain name "mcdonalds.com" to get a response from the ultra-sensitive McDonald's Restaurant company. Sprint Communications attempted to register its competitor's domain name "mci.com," but InterNIC discovered the mistake and re-registered it to MCI. While none of these disputes ever made it to court, some conflicts have and are being examined and decided through the court system.

A. *ActMedia, Inc. v. Active Media Int'l, Inc.*, No. 1996 U.S. Dist. LEXIS 20814 (N.D. Ill. July 12, 1996)

In *ActMedia, Inc. v. Active Media International, Inc.* the court reached the merits of a case involving a domain name controversy. ActMedia had been in the advertising and promotional business since 1972. ActMedia used its mark "ACTMEDIA" in association with these services. When ActMedia sought to register the domain name "actmedia.com," they were precluded from registration because Active Media International had already registered the name. The court determined that Active Media International's use of "actmedia.com" violated the Lanham Act, Illinois common law, and the Illinois Anti-Dilution Statute. It is important to note that ActMedia and Active Media International were competing in the same market for presumably the same customers. This made the decision of the Illinois Federal District Court much easier. Nonetheless, this decision is important because it clearly establishes that domain names may infringe upon federal and common law trademarks, and illustrates the use of an anti-dilution statute to hold the infringer liable for an unauthorized use of a mark.

B. *Brookfield Communications Inc. v. West Coast Entertainment*, 174 F.3d 1036 (9th Cir. 1999)

Brookfield Communications Inc. gathers and sells information about the entertainment industry. It markets several products, including software, under the name "MovieBuff." When it tried to obtain the World Wide Webdomain name "moviebuff.com," it learned that West Coast Entertainment had already registered that domain name. It subsequently obtained federal registration of "MovieBuff" as a mark to designate both goods and services. West Coast, a large video rental store chain, had been using the term "Movie Buff" with regard to its services and products for many years.

When West Coast launched its Website at "moviebuff.com," Brookfield filed suit alleging trademark infringement and unfair competition. Brookfield sought preliminary injunctive relief to prevent West Coast from using "Movie Buff" with its Website, including in the domain name and in the site's metatags. ("Metatags" are hidden code or keywords that allow Internet search engines to identify the contents of a Website and direct users to the site.) The trial court rejected Brookfield's request, finding that Brookfield had failed to establish it was the senior user of the "MovieBuff" mark or that West Coast's use of the "moviebuff.com" domain name created a likelihood of confusion. Brookfield appealed.

The court of appeals reversed and remanded, holding that the trial court erred in concluding that Brookfield failed to establish a likelihood of success on its claim of being the senior user or a likelihood of confusion between its mark and West Coast's domain name.

The court found that, although West Coast registered the domain name "moviebuff.com" before Brookfield began using "Moviebuff.com" on its Internet-based products and services, West Coast did not use it with reference to a good or service in commerce until it actually set up its own Website. Registration of a domain name, by itself, does not constitute "use" for purposes of acquiring trademark priority, the court noted. The court also found that West Coast's use of "moviebuff.com" in E-mail correspondence with lawyers and customers was insufficient to establish that the public identified that mark with West Coast. West Coast's first public use of "moviebuff.com" was its widespread and public announcement about the imminent launch of its Website, an event that took place more than two years after its registration of the domain name.

C. *Avon Products, Inc. v. Carnetta Wong*, No. 96-0451 (E.D.N.Y. 1996)

Avon filed suit in the Eastern District of New York (a mere two and a half weeks after the Federal Trademark Dilution Act was signed into law), alleging trademark dilution under the federal statute and seeking to enjoin the use of the domain name "avon.com." The case, however, settled before the court rendered a decision on the merits. As part of the settlement, Avon obtained ownership of the domain name.

D. *Paine Webber Inc. v. Fourtuny*, No. 99-0456-A (E.D. Va., April 9, 1999)

A Virginia federal judge entered a preliminary injunction against a Website that tried to take advantage of a common Internet typographical error to direct users to a pornographic Website. Plaintiff Paine Webber Inc. filed suit against Rafael Fourtuny after it discovered the existence of a Website at wwwpainewebber.com. The domain name excluded the period between "www" and "painewebber." Users who accidentally omit the period ended up at a pornographic Website rather than at Paine Webber's site. The court found that Paine Webber was likely to succeed on the merits of its dilution claim because the mark is famous and would be tarnished by association with a pornographic Website. The court also found that the absence of an injunction would likely cause Paine Webber irreparable harm.

VI. Metatags, Linking, and Framing

A. What are Metatags, Linking, and Framing?

A Webpage is constructed using Hypertext Markup Language (HTML), a basic text coding technique that provides display instructions to a Web browser program viewing the file that generates the particular Webpage. Through these codes, a Web browser is instructed where to implement new paragraphs, line breaks, bolded letters, and other display attributes that determine the way a document is presented to the viewer. Without HTML, a Web browser would display plain text in a continuous block without organization. Although HTML tags are hidden from normal view, most Web browsers enable users to select a viewing option that allows them to see the HTML coding used to generate a given Webpage.

One type of HTML code is the hyperlink, often represented as bolded or underlined text, or as an image. By "clicking" a mouse or other pointing device on a hyperlink, the contents of another Webpage referenced by the hyperlink are then displayed by the Web browser. This "jump" to another Webpage is the essence of the Web. Hyperlinking enables a Websurfer to connect to other Webpages and retrieve information within seconds and without having to perform new searches or other complex tasks. The extensive use of these interconnections between Webpages is why the medium is termed a "web." A Webpage can contain as many or as few hyperlinks as the creator wishes. These branching mechanisms may reference Webpages both within and outside the Website, though it is primarily the linking to outside Webpages that raises intellectual property questions.

Related to hyperlinking, "framing" is an associational tool that provides a means for dividing a Website into separate windows, with optional scroll bars and borders. Each window is displayed in a separate portion of the Webbrowser screen and functions independently to display an individual Webpage. Usually, each Webpage is interlinked by hyperlinks within the framed site, allowing for user interaction without leaving the original framed site or opening a new screen. A user can choose from different topics within one of the individual framed pages within the site by clicking on a hyperlink on one of the framed pages that, in turn, opens a linked Webpage within one of the framed portions of the Website. When used properly, frames can make a viewer's time on a Webpage much more productive.

Search engines also function to organize information on the Web and help users find information. Webusers utilize search engines such as Yahoo!, Webcrawler, HotBot, Alta Vista, Infoseek, and Lycos, to locate Websites that match their particular interest. Like any typical computerized searching mechanism, a user types a keyword query into the search engine, and the program searches its database and returns a list of results. The results returned by search engine programs are a list of hyperlinks to related Webpages. The design of each of these immense databases is unique to the particular search engine. Each search engine does, however, use a specific kind of software, usually called a spider or crawler, to gather the addresses of Webpages available on the Internet. These programs, in turn, index text on the Webpages, thereby enabling the search engines to associate a user's keyword query with the indexed Webpages.

In addition to analyzing the displayed text, the titles, and the addresses of Webpages, search engines make particular use of meta-tag keywords. Meta-tag keywords consist of text coding which is hidden from normal view and placed within a specially designated portion of the HTML code that generates the Webpage. Webpage designers use this hidden HTML code to designate keywords that are communicated to search engine software. This is an important associational tool for the Webpage designer since search engines are often unable to properly index a particular Webpage based on the text of the page. In its cooperation with a search engine, a meta-tag keyword may be thought of as a "pre-hyperlink" since a hyperlink is often created by a search engine in a search results phase when a user performs a search using that keyword. Unfortunately, uses of trademarks in ways that cause search engines to improperly associate Webpages with those trademarks have created allegations of intellectual property violations.

The development of these associational tools has made the Weban even more valuable and efficient resource by logically associating related information. However, as with any new technology, new rules and regulations are never far behind, and the developing law must carefully balance the power and efficiency of these new tools with their potential impact upon intellectual property rights. Some of the litigation that has spawned from these tools follows.

B. Trends in Linking Cases

At the center of litigation surrounding linking is the issue of Website control-- who has the right to access a Website, when and how they may access the site, and to what extent can Website creators protect their sites from others. Most lawsuits in this area have resulted in settlements. Thus, the number of reported cases in the area is small. However, the cases that have been decided have not yet challenged the "right to link" that has been associated with the Internet from its beginnings. Nevertheless, as the amount of commercial activity on the Internet continues to grow, a greater number of parties are beginning to object to links and metatags. Website owners have tried to protect Websites using linking agreements, new technology, trademark, copyright, and unfair competition laws, and by attempting to control the manner in which linking to their sites occur.

1. *TicketMaster Corp. v. Microsoft Corp.*, No. CV 97-3055 (C.D. Cal. filed April 28, 1997)

The recently settled case of *TicketMaster v. Microsoft* addresses the implications of hyperlinking without permission. TicketMaster sued Microsoft in the U.S. District Court for the Central District of California for improperly using TicketMaster's name and logo on their Webpage, "Seattle Sidewalk." The Seattle Sidewalk site describes entertainment and events in the Seattle region. Microsoft placed a convenient link on its site to the TicketMaster page (many levels down) where you could buy tickets. TicketMaster complained that by bypassing its home page, customers were also bypassing any third-party advertising that appears there. Specifically, TicketMaster alleged numerous counts against the software giant including dilution of TicketMaster's trademarks, misrepresentation, unfair competition, unfair business practices, and misleading statements.

Because of the use of "deep" hyperlinks, a user of the Seattle Sidewalk Website could bypass all policies and service information provided on the TicketMaster homepage and go directly to TicketMaster's event listing to purchase tickets. This would not have happened if the hyperlinks from Seattle Sidewalk had been "surface" links linked to the TicketMaster homepage instead of to one of the subsidiary pages within the Website. TicketMaster alleged that due to this direct linking Microsoft has benefited from their trademarks and name. Additionally, TicketMaster alleged that this unlawful use has diminished the advertising revenue available to TicketMaster in return for an increase in Microsoft's advertising revenue

One interesting note in the history of this case is that before the suit began, the companies were in negotiations for having hyperlinks from the Sidewalk Website to the TicketMaster site, perhaps suggesting Microsoft was concerned about the legal bases for their intentions. After the negotiations failed, Microsoft established the links anyway. In addition, after they filed the initial Complaint, TicketMaster filed an Amended Complaint to more specifically reference deep linking, creating an inference that TicketMaster suspects that merely linking to a homepage may not be actionable. Specifically, the new language in the First Amended Complaint stated, "Some of Seattle Sidewalk's links have circumvented the beginning pages of TicketMaster's Website, which display advertisements, products and services of entities with which TicketMaster contracts, and have linked directly to subsidiary pages of the Website." The specific language affirms the theory stated above.

This and similar lawsuits have been settled, and the outcomes suggest that linking agreements between two sites may become common practice. Some sites even post terms and conditions spelling out what kinds of links are permitted. In the absence of any clear agreement, it is wise to link only to the home page of the desired site (as opposed to deep linking). The link should be text - not the logo or other trademark of the linked site. Using the linked site's logo without permission could lead to a claim of trademark infringement or false impression of sponsorship or endorsement.

2. ***Shetland Times, Ltd. v. Wills*, 1997 F.S.R. (Ct. Sess. O.H.), 24 October 1996**

Although considered the first "linking" case, *Shetland Times*, was not a case, as some have reported, challenging the validity of hypertext links. The issue in *Shetland Times* was far narrower - whether "deeplinking" to internal or embedded pages of the Shetland Times' ("Times") Website by the Shetland News ("News") through the use of the plaintiff Website's news headlines was an act of copyright infringement under the United Kingdom's Copyright Designs and Patents Act of 1988. In *Shetland Times*, the plaintiff sought, and received, an injunction precluding such deeplinking. In granting the injunction, the court held only that the plaintiff had presented a prima facie case of copyright infringement under the Act because it could not be said that the Websites at issue were not covered by the Act or that the Times's headlines which the News had used as linking text were not protected under the Act as "literary works." The News appealed this ruling and the matter settled before trial. As part of that settlement, the News agreed to link only through the Times's Website's front page and agreed to include a legend identifying the headlines as from The Shetland Times wherever such headlines were posted on the News' Website.

C. Trends in Metatag Cases

Metatags have also produced Internet related litigation. Search engines index and identify Websites using "metatags," embedded keywords that the Website developer has included behind the Website. "Much like the subject index of a card catalog, the meta tags give the websurfer using a search engine a clear indication of the content of a Website." *Playboy*

Enterprises, Inc. v. Terri Welles, 7 F. Supp. 2d 1098, 1104 (S.D. Cal. 1998). Some Website owners have used the metatag codes from popular sites or trademarked words as metatags, to ensure that search engines will turn up their site in search results more often. *See e.g, Niton Corporation v. Radiation Monitoring Devices, Inc.*, 27 F. Supp. 2d 102, 104 (D. Mass. 1998). Metatags can cause confusion for users searching the Internet, as well as infringe upon and dilute the borrowed trademarks.

1. ***Playboy Enterprises, Inc. v. Calvin Designer Label*, 985 F.Supp 2d 1220 (N.D. Cal. 1997)**

In the first meta-tag case, *Playboy Enterprises, Inc. v. Calvin Designer Label*, the district court issued a preliminary injunction ordering the defendants to cease all use of the plaintiff's registered trademarks in any fashion. In this case the defendant was using the registered trademarks PLAYMATE and PLAYBOY as meta-tag keywords as well as domain names on the Internet and on different Webpages within their sites at Internet addresses "www.playboyxxx.com" and "www.playmatelive.com."

In response to Calvin's use of the Playboy trademarks, Playboy filed a motion seeking a preliminary injunction for trademark infringement, unfair competition and dilution. In granting Playboy's preliminary injunction, the court ruled that Playboy demonstrated a sufficient (1) likelihood of success on the merits of its trademark infringement, unfair competition and dilution claims, (2) showing of irreparable harm if they are not granted a temporary restraining order pending hearing on their motion for a preliminary injunction, (3) balance of hardships tipping in their favor, (4) and the absence of any public interest factors that stand against the issuing of the relief sought by the motion.

In the court's order, Calvin was preliminarily enjoined from, among other things: using the Playboy and Playmate trademarks, any terms similar to these trademarks, or any terms likely to cause confusion within meta-tags, domain names, or Websites; using the trademarks on their goods or services in a manner that is likely to create an erroneous belief that the goods or services are authorized by Playboy; and engaging in any activities that may cause a consumer to believe that the defendant's goods or services are sponsored, authorized, licensed or authorized by the plaintiff.

Although this case seems to shed some light on the potential causes of action concerned with search engines, the plaintiff's infringed marks were also being used as domain names of the defendant's Website. Thus, this decision may not have been decided solely because of meta-tags, but instead on the basis of domain name usage, an area presently being litigated as an issue of trademark infringement.

2. ***Insituform Technologies, Inc. v. National EnviroTech Group*, No. C-97-2064 (E.D. La. filed July 31, 1997)**

Insituform filed a motion for preliminary injunction, claiming trademark infringement and unfair competition. In this case, National EnviroTech, a competitor of Insituform, placed meta-tags within the HTML code for its Website referencing Insituform's registered trademarks INSITUFORM and INSITUPIPE. This designation would lead keyword searches on search engines to return National's Website as well as Insituform's, thereby potentially showing an association between the Insituform and National Websites.

On August 26, 1997, the court signed a final judgment on consent against the defendant National EnviroTech. This final judgment was based on a settlement agreement calling for National to delete Insituform's federally registered trademarks and service marks INSITUFORM and/or INSITUPIPE from the meta-tag section of the National Liner Website, to submit or resubmit the National Liner Website to different Internet search engine companies, and in addition, to send a letter to each of these search engine companies with a copy of the final judgment on consent and the plaintiff's complaint.

Since this recent case was settled by consent agreement, it lacks the judicial direction many Internet users presently seek regarding meta-tag usage. The defendants did, however, agree to the removal of all meta-tag references which may signify either that they feel there may in fact be a cause of action against this kind of meta-tag usage, or that they simply did not wish to commence litigation in an area containing practically no guidance from the courts.

3. *Oppedahl & Larson v. Advanced Concepts*, No. C-97-Z-1592 (D. Colo. filed July 23, 1997)

In the most recent case addressing the use of meta-tags, *Oppedahl & Larson v. Advanced Concepts*, the plaintiff brought an action for federal unfair competition, federal dilution, common law unfair competition, and common law trademark infringement for the defendant's use of the plaintiff's trademark OPPEDAHL & LARSON. In filing the complaint Oppedahl stated that the defendant's Websites contained their trademark numerous times within meta-tags and that when a search report was performed using the Alta Vista search engine, the defendant's Webpages were returned as well as their own. In fact, in the complaint, Oppedahl specifically states that after viewing the returned URLs from the search engine, they noticed no reference to their trademarks and instead were required to look at the "underlying source document" to find the references to their mark.

Although the defendants have removed all references to Oppedahl & Larson on its Websites, since the civil action still proceeded, those seeking an answer to the relevance of meta-tags in an infringement action may have some judicial guidance in the near future.

4. *Playboy Enterprises, Inc. v. Welles*, 7 F. Supp. 2d 1098 (S.D. Cal. 1998)

Playboy Enterprises, Inc. sued Terri Wells, a former Playboy "Playmate of the Year," for trademark infringement, dilution of trademark, and unfair competition after Wells used particular marks, namely "PMOY" as a watermark and "playmate" and "playboy" as hidden metatags on her Website, www.terriwelles.com, which included photos, a fan club posting board, and other information. The court found that Welles use of the "PMOY" watermark and the metatags were fair use because Playboy Enterprises had bestowed upon her the title "Playmate of the Year" and had encouraged her to use the title for self-promotion. The court also found that Welles was not trying to deceive websurfers by using the metatags and watermark, because her site contained a visible disclaimer which clearly stated that the site has no relationship to Playboy. In addition, Welles did not use the bunny logo and her references to Playboy were minimal. Playboy appealed to the Ninth Circuit Court of Appeals and the Appeals Court affirmed the lower court's ruling.

5. *Niton Corp. v. Radiation Monitoring Devices, Inc.*, 27 F. Supp. 2d 102 (D. Mass. 1998)

The Plaintiff, Niton Corporation, manufactured and sold x-ray florescence instruments and software designed to detect the presence of lead in paint. *Niton Corporation v. Radiation Monitoring Devices, Inc.*, 27 F. Supp. 2d 102, 103 (D. Mass. 1998). The defendant, Radiation Monitoring Devices, manufactured a device also designed to detect lead in paint, but using a slightly different technique. *Id.* The defendant's Website contained metatags that were identical to the metatags that the plaintiff's webmaster had created for the plaintiff's Website. In addition, the defendant's metatags included the plaintiff's trademarked name. The court issued a "preliminary injunction subject to modification," which enjoined the defendant from using their Website and means of attracting users of the Internet in any manner likely to mislead consumers into thinking the defendant's Website was actually the plaintiff's Website or that the parties were affiliated in any way.

D. Trends in Framing Cases

Beyond linking, many sites "frame" another site within their borders. Frames provide a means for dividing a Webpage into scrollable portions, or windows, that are viewed in separate parts of the screen simultaneously, while functioning independently. When used properly, frames can make a viewer's time on a Webpage drastically more productive and convenient. This practice is not always welcomed, however, by the framed site and has been the subject of several lawsuits. The owners of the framed sites have complained that their products or services appear to be associated with the company that's doing the framing. In some cases, the visibility of the framed site is reduced and advertising banners may not be displayed. As with linking, framing may be safer when a specific agreement is reached between the two sites.

1. *The Washington Post Co. v. TotalNews, Inc.*, No. CA 97-1190 (S.D.N.Y. filed Feb. 20, 1997)

In *Total News*, the plaintiffs, Washington Post Co., Time Inc., Cable News Network Inc., and Reuters New Media Inc., among others, brought multiple causes of action against the defendants, Total News Inc. and other related parties. Included among the many claims were misappropriation, trademark dilution, trademark infringement, and willful copyright infringement. In a complaint filed in the U.S. District Court for the Southern District of New York, the plaintiffs alleged that the defendants designed a parasitic Website which, instead of having its own material, simply republished the news and editorial content of Websites that already existed so as to unfairly attract both advertisers and users.

On the Total News Website, activation of a hyperlink to an external site opened the associated external page within one of the framed portions of the Total News homepage while leaving the Total News logo, commercial advertisements and URL on the screen surrounding the activated page. The plaintiffs claimed that this method of advertising was the "Internet equivalent of pirating copyrighted material from famous newspapers, magazines or television news programs," and that the defendants' page simply took parts of competitive publications and used them for their own financial benefit.

While many observers were anxious to hear a court speak on the various legal issues presented by this conflict, Total News and the other defendants settled this controversy by, inter alia, agreeing to stop the framing of plaintiffs' Websites. While being far from conclusive, this settlement could suggest that hyperlinking in a framed arrangement could be actionable under at least one of the legal claims asserted in the *Total News* complaint.

VII. Copyright Issues

A. Web Site Content

The Internet has been characterized as the largest threat to copyright since its inception. The Internet is awash in information, a lot of it with varying degrees of copyright protection. Copyrighted works on the Internet include news stories, software, novels, screenplays, graphics, pictures, Usenet messages and even E-mail. In fact, the frightening reality is that almost everything on the Net is protected by copyright law. While some freedom-of-information advocates argue persuasively for a loosening of intellectual property rights in cyberspace, their views have not yet won out. That can pose problems for the hapless Website developer.

What you post on your Website should fall into one of three camps. First, it can be original material that you have created. Second, it can be work that is truly in the public domain. This generally means that all copyrights have expired (such as with the works of Shakespeare), have been abandoned or waived, or never were issued in the first place (such as copyrighted works created by the United States government - for example, the Declaration of Independence). Unfortunately, determining if a work is in the public domain is never easy. Third, the content can be posted with the permission of the owners of the intellectual property rights. (Be prepared to pay for the privilege.) The permission can take the form of a license, a clearance letter, or perhaps general permission posted on a Website.

B. Copyright Infringement Issues for Internet Service Providers

In the past few years, online providers from Internet Service Providers, (ISPs,) to Bulletin Board Services, (BBSs,) to traditional online services have felt like entrapped criminals, left holding the bag for copyright infringers who have used the provider's facilities for their dirty deeds. Copyright owners, looking for deep pockets, have asked courts to hold online providers liable. The providers expected the courts to throw these cases out - after all, they did not post the infringing material and cannot monitor the thousands of user postings for copyright violations. The courts, however, were reluctant to entirely let online providers off the hook. Some of these cases are discussed below.

Since these cases, Congress stepped into the fray several times, first passing the infamous Communications Decency Act (the one with the unconstitutional anti-indecency provisions), which provides some relief for passive service providers, such as when defamatory materials are posted by a user. More recently, Congress amended the Copyright Act with the Digital Millennium Copyright Act ("DMCA"). The DMCA gives service providers limited immunity from user postings that run afoul of copyright laws. Specifically, the Copyright Act was amended to exempt an ISP from liability for claims of copyright infringement based solely on the "provider's transmitting, routing, or providing connections for, material through a system or network controlled" by the ISP or by reason of storage of material in the course of such transmitting or routing if certain conditions are met by the ISP. However, the DMCA so unclearly defines "service provider" that it could easily apply to any Website. If your Website permits user postings - via forums, chat rooms, or similar areas - you may want to take advantage of the DMCA's provisions.

1. ***Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995)**

This case was one of the first to discuss whether the operator of a computer bulletin board service ("BBS"), and the Internet access provider that allows that BBS to reach the Internet, should be liable for copyright infringement committed by a subscriber of the BBS. Religious Technology Center, one of the formal entities constituting the Church of Scientology founded by L. Ron Hubbard, brought a copyright infringement action for the unauthorized posting of portions of their works on the BBS. The court first analyzed and then concluded that Netcom could not be held liable for direct infringement. As for contributory infringement, the court refused to grant a summary judgment stating that there are fact issues as to whether and when Netcom knew that the subscriber was infringing the copyrights of the plaintiff. Last, the court dismissed vicarious liability claims pointing out that the Internet service provider does not create or control the content of the information available to its subscribers nor does it monitor messages as they are posted.

2. ***Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923 (N.D. Cal. 1996)**

This action was initiated after Sega, a major manufacturer and distributor of computer video game systems, received an anonymous tip that Chad Sherman was operating a computer BBS which contained and distributed pirated and unauthorized versions of Sega's video game software. Sega collected evidence of these activities by having a Sega employee gain access to the MAPHIA BBS under a pseudonym, using information supplied by an authorized user who was an informant. Printouts of the data on Sherman's BBS seized pursuant to a court order and on-line data captured from Sherman's BBS show that the uploading and downloading of unauthorized copies of Seta's copyrighted video games were known to Sherman.

Sega contended that Sherman was liable for copyright infringement under direct, contributory, and vicarious liability theories. As for direct liability, the court ruled that Sega has not shown that Sherman himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. As for contributory liability, the court found that Sega had established a prima facie case by proving: (1) that the users of Sherman's MAPHIA BBS directly infringed Sega's copyright, (2) that Sherman had knowledge of the user's infringing activity, and (3) that Sherman induced, caused, or materially contributed to their infringing activity. The court stated that the third prong was met because Sherman "provided the facilities for copying the games by providing, monitoring, and operating the BBS software, hardware, and phone lines necessary for the users to upload and download the games" and because Sherman offered the copying means to facilitate playing the downloaded games.

3. *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993)

This case involved a suit against the operator of a small BBS whose system contained files of erotic pictures. A subscriber of the defendant's BBS had uploaded files containing digitized pictures copied from the plaintiff's copyrighted magazine, which files remained on the BBS for other subscribers to download. The court concluded that the BBS operator was liable for violating the plaintiff's right to publicly distribute and display copies of its work even though the operator himself never uploaded to the BBS, or downloaded from the BBS, any of the Playboy photographs. The court based its holding on the public distribution and display rights available under the Copyright Act, even though the BBS operator was unaware of the copyright infringement. As the court stated, "Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature."

VIII. Trends in First Amendment Issues

There has been substantial litigation concerning First Amendment rights and the Internet, especially surrounding two major issues, freedom of speech and obscenity. The first issue arises from the tension between the freedom of speech in our society and the need to regulate speech for particular reasons (*i.e.*, to protect children from pornography in cyberspace). *See, e.g., Reno v. American Civil Liberties Union*, 117 S. Ct. 2329, 2336 (1997). Secondly, a common issue in these cases concerns the proper standard for obscenity. More specifically, should the most restrictive local standards of obscenity apply to communications over the Internet, or should a more relaxed standard be applied? One possible resolution may be to develop a standard unique to the Internet itself. One point Internet litigation up until now has clearly established is that communications over the Internet are to be afforded the full measure of First Amendment protection given to communications in other mediums. However, because the Internet is a fairly new and unique means of communication, clear guidelines for applying the full First Amendment protection to Internet users are yet to be settled.

A. Ford Motor Company and Robert Lane

A Website that posted secret blueprints and business plans from Ford Motor Co. has gone back online, but without the content that landed its owner in federal court. A federal judge will soon rule whether Robert Lane, a 32-year-old nursing student and Ford enthusiast, violated company trade secrets and copyright law when he posted Ford internal documents on the Website. Lane and his site, www.BlueOvalNews.com, are under a temporary restraining order recently issued ordering him to remove the documents and any material copyrighted by Ford.

U.S. District Judge Nancy G. Edmunds said that she would decide within the next week whether the Dearborn resident can repost any of the 112 Ford documents he claims to have received from anonymous sources. Edmunds said she needed time to research the question, and that few, if any, cases had addressed the issues before. Among the documents is an internal memo detailing problems with the 1999 Mustang SVT Cobra. Ford announced recently that all 5,300 models sold had been recalled to fix exhaust problems that cut as much as 50 horsepower from the 320 horsepower the car is supposed to have.

Lane and his attorney claim Lane is a journalist, and that the limits against BlueOvalNews are an illegal prior restraint. "I don't think Ford wants to discuss the First Amendment, because if they discuss the First Amendment, they'll lose," said attorney Mark Pickrell. Lane testified that he started the site to inform the public about Ford news and share his enthusiasm; he owns four Mustangs. He said the documents were mailed or delivered to his home anonymously. But Lane said some damaging documents were posted in the hope of getting Ford to change some decisions, such as designing a diesel engine that might fail future emissions standards. Other documents included a list of engines for future cars and trucks, and a blueprint of an engine cylinder head.

B. *United States v. Baker*, 890 F. Supp. 1375 (E.D. Mich. 1995), *aff'd sub. nom.*, *United States. v. Alkhabaz*, 104 F.3d 1492 (6th Cir. 1997)

University of Michigan undergraduate Jake Baker was arrested by FBI agents for posting to the alt.sex.stories newsgroup a violent narrative of rape and torture that used the real name of a female classmate for the victim. Baker subsequently E-mailed a friend that "just thinking about it [his fantasies] doesn't do the trick anymore. I need to do it." The university suspended him and a federal judge ordered him held without bail, charged with the federal crime of "transporting threatening material" across state lines.

Some civil liberties groups rushed to the student's defense, arguing that the Constitution guarantees freedom even for repugnant fantasies broadcast worldwide. A federal judge in Detroit implicitly agreed, throwing out the case. While the university acted properly in disciplining the student for his behavior, the judge ruled, there was no cause for a criminal indictment.

Specifically, because prosecution under the federal criminal act involves punishment of pure speech, it necessarily implicates and is limited by the First Amendment. The court quashed the indictment holding that the messages did not meet the First Amendment "true threat" requirement.

C. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 117 S. Ct 2329 (1997)

In *Reno,* the Plaintiffs filed suit in order to challenge the constitutionality of the provisions of the Communications Decency Act of 1996 ("CDA") which seek to protect minors from "indecent" and "patently offensive" materials on the Internet. *Reno v. American Civil Liberties Union,* 117 S.Ct 2329, 2334 (1997). The Supreme Court struck down all or part of these provisions and thus clearly established that Internet communications are entitled to the broadest First amendment protections accorded to traditional forms of communication (*i.e.*, books and newspapers), and not simply the narrower First Amendment protections accorded to the broadcast media. The provisions were held to violate the First Amendment because they were facially over broad and therefore could not be properly analyzed.

D. *Apollomedia Corp. v. Reno,* 19 F. Supp. 2d 1081 (N.D. Cal. 1998)

Apollomedia, like *Reno*, also interpreted the Communications Decency Act of 1996. Apollomedia, a multimedia technology company who operates the "annoy.com" Website, brought a declaratory judgement action to challenge the constitutionality of a criminal provision of the CDA to the extent that it prohibited "indecent" communications "made with the intent to annoy." *Apollomedia Corp. v. Reno,* 19 F. Supp. 2d 1081, 1085 (N.D. Cal. 1998). "Annoy.com" allows Website visitors to view images and articles that present strong views on various issues, send anonymous E-mails to public officials, send electronic postcards, and post messages on an uncensored message board. Apollomedia was concerned that the images and language on "annoy.com" would be considered indecent in some communities. The court held that the challenged provision was not unconstitutional because it only applied to "obscene" communications. Thus, the provision was allowed to stand but its reach was limited to communications deemed to be obscene (but not to communications which are lewd, lascivious, indecent, or filthy). On April 19, 1999, the Supreme Court affirmed the lower court's decision.

E. *American Civil Liberties Union v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997)

A group of Internet users brought an action to challenge the constitutionality of a Georgia state criminal statute that prohibits Internet transmissions that falsely identify the sender or that use trade names or logos that would falsely state or imply that the sender was legally authorized to use them. The Internet user's action was for declaratory and injunctive relief challenging the constitutionality of the Georgia law alleging that it imposed unconstitutional content-based restrictions on their right to communicate anonymously and pseudonymously over the Internet. The district court granted the plaintiff's motion for preliminary injunction stating, among other things, that the users were substantially likely to show that the statute imposed content-based restrictions that were not narrowly tailored to achieve state interest.

F. *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996)

Robert Thomas and his wife Carleen Thomas operated a bulletin board system that included obscene, sexually-explicit images of bestiality, oral sex, incest, sado-masochistic abuse, and sex scenes involving urination. The court confirmed their conviction for federal obscenity charges holding that the allegedly intangible form by which computer-generated images moved from the defendant's bulletin board in one state to a personal computer in another state did not preclude prosecution for interstate transportation of obscene materials.

IX. Trends in E-Commerce

Commercial activity over the Internet is a quickly expanding area. "E-commerce" is the word used to describe a wide range of commercial transactions conducted via the Internet, including the sale of goods and the purchase of services. As more and more entities conduct E-commerce, more litigation involving Internet-based transactions inevitably arises.

A. Contract Disputes

One area of E-commerce litigation deals with contract disputes. Courts face new problems when dealing with contracts entered into over the Internet, especially in the areas of formation, validity of assent, and the authentication of "electronic signatures." For example, if a person orders books electronically from the Website of amazon.com does that method of ordering create an enforceable contract, though no writing or even verbal confirmation completes the transaction, no signature is present, and the order exceeds $500? There are also problems regarding choice of law issues--whose law governs in a cyberspace contracting situation? To address these problems, a new article to the Uniform Commercial Code, Article 2B, was written with the purpose of governing all transactions involving licensing information. However, Article 2B was defeated in April 1999 after extensive debate. The Uniform Computer Information Transactions Act, a new, more narrow set of rules has been proposed and is currently being debated.

B. Use of "Clickwrap" Licenses

Another portion of E-commerce litigation has developed surrounding "clickwrap" licenses, the Internet version of the "shrinkwrap" license. These licenses raise questions concerning the nature of the purchaser's true understanding of the agreement and the possibility of unconscionable terms.

Click-wrap agreements, or point and click agreements, are contracts formed entirely over the Internet. A party posts terms on its Website pursuant to which it offers to sell goods or services. To buy these goods, the purchaser is required to indicate his assent to be bound by the terms of the offer by his conduct -- typically the act of clicking on a button stating "I agree." Once the purchaser indicates his assent to be bound, the contract is formed on the posted terms, and the sale is consummated. No paper record is created nor is the signature of the purchaser required.

Click-wrap agreements derive their name from shrink-wrap agreements, by which most software is sold today. The software vendor offers to sell or license the use of her software according to terms accompanying the software. The purchaser or licensee agrees by his conduct to be bound by such terms. Such conduct typically takes the form of the retention or use of the software after being provided an opportunity to review the contract's terms and return the software for a full refund if they are unacceptable.

Several cases have upheld the enforceability of clickwrap licence agreements. These decisions are well grounded in existing law. Under Uniform Commercial Code §2-204, a "contract for the sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of a contract." Similarly, Section 19 of the RESTATEMENT (SECOND) OF CONTRACTS provides that "[t]he manifestation of assent may be made wholly or partly by written or spoken words or by other action or by failure to act." These provisions provide ample support for the conclusion that a binding contract can be created over the Internet by the act of clicking on an "I agree" button indicating assent to be bound by the offeror's proposed contract terms. Indeed, this rationale was utilized by the Seventh Circuit in support of its decision in *ProCD*.

The fact that click-wrap agreements can be enforced does not mean that any particular agreement is in fact enforceable. Contracting parties must still turn to ordinary contract law principles to determine the enforceability of particular agreements. While beyond the scope of this article, contracts of adhesion are no more enforceable when consummated over the Internet than if consummated in a retail store. "Contracts of adhesion arise when a standardized form of agreement, usually drafted by the party having superior bargaining power, is presented to a party, whose choice is either to accept or reject the contract without the opportunity to negotiate its terms. Such a contract will not be enforced against the weaker party when it is (1) not within that party's reasonable expectations; or (2) is unduly oppressive, unconscionable or against public policy." *AEB & Associates Design Group, Inc. v. Tonka Corp.*, 853 F. Supp. 724, 732 (S.D.N.Y. 1994) (citations omitted). Similarly, various UCC provisions are likely to be applicable to online contractual arrangements. These include UCC §2-316, which requires that for certain warranty disclaimers to be enforceable, they must appear conspicuously in the parties' contract.

1. ***Hotmail Corp. v. Van $ Money Pie, Inc.*, 47 U.S.P.Q. 2d 1020 (N.D. Cal. 1998)**

Plaintiff Hotmail provides free E-mail services to more than 10 million customers under its trade name and service mark "hotmail." To utilize Hotmail's services, one must agree to Hotmail's Terms of Service, which expressly prohibit use of Hotmail E-mail accounts to facilitate the transmission of unsolicited commercial E-mail, otherwise known as spam. Users agree to these Terms of Service via a click-wrap agreement, in which the customer, after being given the opportunity to view the Terms of Service on his computer, clicks a box indicating assent to be bound thereby.

Defendants sent spam which advertised allegedly pornographic materials. Defendants altered the return addresses of this E-mail to falsely indicate that it was sent from a Hotmail account, rather than its true source. This was accomplished by using plaintiff's mark in the E-mail's reply address. Numerous recipients of defendants' spam responded with complaints, which were sent to accounts defendants had set up at Hotmail for the receipt of E-mail.

Hotmail moved to enjoin defendants both from sending "spam" which falsely stated it came from plaintiff's service, and from using Hotmail accounts as mail boxes for "spam" reply. The court held that "the evidence supports a finding that plaintiff will likely prevail on its breach of contract claim." As stated above, this contract was contained in plaintiff's Terms of Service which was breached by defendants' use of Hotmail accounts and the Hotmail mark in their transmission of spam. To reach this conclusion, the Court first had to hold that the plaintiff and defendants were parties to an enforceable agreement. By so doing, the Court indicated its willingness to uphold the validity of a click-wrap agreement, as defendants agreed to be bound by plaintiff's Terms of Service solely by clicking "I agree" after being presented with an opportunity to view the Terms of Service.

Finally, the court found that defendants' conduct was likely to violate the Computer Fraud and Abuse Act, and constituted a trespass on chattel. The former act, 18 U.S.C. § 1030, prohibits persons from knowingly causing the transmission of information that intentionally causes damage to protected computers. Defendants committed the requisite injury to plaintiff's computers by causing spam E-mail to bounce back to plaintiff's computers by use of a false return address. This conduct also caused a prohibited trespass on plaintiff's chattels, namely its computers.

The Court's decision in *Hotmail* accords with two decisions of the Seventh Circuit Court of Appeals, each of which upheld the enforceability of shrink-wrap agreements:

2. *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996)

Defendant purchased CD-Roms which contained compilations of various telephone directories. These CD-Roms were packaged along with a user's manual in a box. Printed on the outside of this package was a notice that use of the CD-Roms was restricted by the terms of an enclosed license. This license, contained both in the user's manual found inside the product's packaging, as well as encoded on the CD-Rom disks themselves, restricted use to non-commercial purposes. In violation of this license, defendant sold the information contained on the CD-Roms to third parties.

In upholding this shrink-wrap agreement, the court determined that ProCD had made an offer to license its product which could only be accepted by conduct - use of the software - after being afforded an opportunity to read the terms of the license. By so using the software, defendant Zeidenberg was bound by the terms of the license. The court held that "shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general (for example, if they violate a rule of positive law, or if they are unconscionable)."

3. *Hill v. Gateway 2000, Inc.*, 105 F. 3d 1147 (7th Cir. 1997)

The Seventh Circuit held that plaintiff's purchase of a computer was governed by contract terms shipped to her along with the computer. Plaintiff had received notice that the terms would govern the parties' relationship unless the computer was returned within 30 days. Plaintiff had failed to return the computer within the allotted time.

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

The Seventh Circuit held that the terms do indeed govern the parties' relationship, validating Gateway 2000's "approve or return" device. The court held that Gateway's offer required acceptance by retaining the computer after receipt of the terms. As such, the parties' contract was not formed until the customer retained the computer for a period of 30 days, and the terms provided with the computer bound the parties.

C. Consumer Fraud and False Advertising

Since its inception, the Internet has brought society an array of opportunities. With those opportunities challenges arise. The Internet advertising arena is no different. The opportunities for companies to use the Internet to reach their target audiences are extraordinary. Because no regulations apply specifically to the Internet and since no agency has the specific task of regulating it, questions are plentiful regarding how and to what extent advertising is acceptable over the Internet.

Once a Website is built, someone in the company will have to fill it with content. All too often the job is relegated to the Webmaster, a human resources staffer, or someone in the IS/IT department. Talented as these folks may be, they are not usually trained in the fine art of corporate communications or legal arcane. That is why you see so many corporate Websites brimming with job postings, product statements, advertising claims, and corporate projections that would never pass legal review, much less find their way into printed corporate literature. "We own this market and control everything from supply to price." "Energetic young white male wanted for shipping clerk position." "Our products are guaranteed not to fail." "Watch for our initial public offering, coming soon!" Basically, if it is illegal on paper, it is forbidden online.

That is why a third type of E-commerce litigation revolves around consumer fraud, including false advertising, unfair and deceptive trade practices, and investment fraud. The Federal Trade Commission, the Food and Drug Administration, the Securities and Exchange Commission, and State Attorney Generals offices have led the bulk of the prosecutions for false advertising or consumer fraud over the Internet so far, many of which are targeted against credit repair schemes, business opportunities, pyramid schemes, and unsubstantiated product claims.

1. *People v. Lipsitz*, 663 N.Y.S.2d 468 (N.Y. Sup. Ct. 1997)

The Attorney General for the State of New York brought an action against Kenneth Lipsitz seeking enforcement of consumer fraud and false advertising laws upon allegations that the business engaged in fraudulent and deceptive consumer sales practices targeting the worldwide Internet audience by methods involving the use, misuse, and abuse of E-mail. Lipsitz, using various assumed business names, was selling magazine subscriptions from a location in Staten Island, New York. In many instances, the magazines never arrived, or if any magazines started to arrive, always after an extremely extended delay, the subscription was shortened, often by as much as half the length of time for which the consumer paid.

In a case apparently of nationwide first impression, the Attorney General was successful in forcing Lipsitz to stop using fictitious "satisfied consumers" extolling the unbeatably low prices and wonderful customer service, using bulk E-mail distribution practices ("spamming"), and using fictitious or anonymous E-mailers ("spoofing"). Lipsitz was also required to post a bond to assure future proper business behavior, make restitution to the aggrieved parties, and pay penalties.

2. *Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W.2d 715 (Minn. App. Ct. 1997)

In this case discussed previously in this paper, the State of Minnesota sued a Belize defendant that was operating an on-line betting service, WagerNet. The state filed a complaint alleging that the defendants had engaged in deceptive trade practices, false advertising, and consumer fraud after a consumer investigator for the Minnesota Attorney General's office spoke with representatives of the defendant who told the investigator that the on-line betting service was legal.

3. *Juno Online Services, L.P. v. Juno Lighting, Inc.*, 979 F. Supp. 684 (N.D. Ill. 1997)

The plaintiff, an online service provider, which had registered the Internet domain name "juno.com," brought an action against the defendant, a lighting manufacturer, which had registered the domain name "juno-online.com." The plaintiff asserted violations of the Lanham Act, state unfair competition laws, and state consumer fraud and deceptive business practices laws. The court dismissed these latter two claims, holding that merely obtaining a domain name, without setting up a Website or E-mail service, is not enough to constitute "trade or commerce" or to create a likelihood of confusion to potential buyers or to the public.

X. Conclusion

The World Wide Web has experienced dramatic growth in recent years, and has transformed the Internet from a primarily passive environment used for E-mail, newsgroups, and mailing lists to an interactive, user-enabled universe filled with vast amounts of information. With the Internet providing a new medium in the search for this information, it has also opened a closet filled with new questions relating to traditional areas of litigation. Each new decision of the courts becomes part of a living and evolving body of law, arising out of the growth and importance of the new Internet environment and its related technologies. In the meantime, in the law of cyberspace, very few issues can be characterized as having been conclusively established.