Protecting Against Liability for On-line Practices in External E-Business

by

M. Jean Connolly, Esq.[1]

One of the greatest strengths of the Internet is its interactivity between users and information as well as between one Web site and other Web sites. Any entity with an Internet presence can be exposed to liability for its data collection and other online practices relating to interactivity. Such potentially liable practices are related to Internet and computer technology which has emerged in the past few years, such as linking and framing; spiders, web crawlers and bots. and metatags. Additionally, the application of such technology to the World Wide Web has made it possible to gather and transmit data, especially data in which a third party possesses proprietary interests, more easily than ever before. As a result, there is now a much greater potential, whether intentional or inadvertent, for infringing such interests of third parties. The impact of such technologies will be discussed as well as how to avoid the liability associated with them.

One caveat must be noted: a great deal of the law in this area is in the formative stages, and the rights of interested parties will be argued in and defined by the courts. A recent court decision summarizes this state of the law aptly: "This is a classic illustration of a new kind of litigation for which nothing in past experience comes even close to preparing trial judges and the advocates appearing before them."[2]

This article will also detail how the law appears to be developing with respect to the various implications of using such technology and in light of such developments, I will

---

[1] *M. Jean Connolly is partner in the Intellectual Property and Corporate, Securities and Finance Groups of Hogan & Hartson L.L.P.*

[2] *Niton Corp. v. Radiation Monitoring Devices, Inc.*, 27 F. Supp. 2d 102, 103, 1998 U.S. Dist. LEXIS 18538 (D. Mass. 1998) (The case addresses the use of metatags, and is discussed later in this text.).

make some practical suggestions of actions that counsel can advise their clients can take, to minimize their liability risks.

I. Linking.

Linking is one of the most important technologies to emerge in this field. It is the underlying basis for the great popularity and efficacy of the World Wide Web for it facilitates an extremely easy, highly efficient and apparently seamless transmission of information from one point to another. Linking involves the use of words, phrases or images, coded in hypertext transfer protocol language, (or, the "http" that prefixes web addresses that are typed into a browser), to form a "hyperlink" or "link" that connects different sets of text or images on another page within a Web site, or connect pages on different Web sites with each other. A person needs only to click on the link to be transported immediately to the connected Web page, text or image.

Although there is not yet much decisional law relating to linking, the use of linking and the associated liability for such use is an aspect of this area of the law that is developing the most rapidly. The cases that are emerging suggest that linking can present a liability risk to the owner of a Web site under copyright law, under trademark laws, or under state common or statutory laws relating to business torts such as misappropriation or unfair competition.[3]

It is important at the outset to differentiate between a "surface" link that merely connects to the first page that appears when one accesses a Web site, the "home page", and a "deep link" that connects to an interior page by drilling down into the Web site beneath the home page. In most cases, a surface link will be protected under the First

[3] Unless otherwise specifically stated, all references to laws, regulations and court decisions are to the laws, regulations and court decisions of the United States of America and/or of its individual states.

Amendment, as it directs an end user to the first page of a particular Web site, which is akin to merely citing a book title.[4]

On the other hand, courts may be inclined to impose liability in the case of an unauthorized deep link on various emerging theories. One such theory is based on the premise that when such a link bypasses the home page, it deprives the Web site owner of advertising income derived from home page "hits" or banner ads. Another theory is that a deep link may result in misidentification of the true source of goods or services demarcated by the Web site owner's trademarks residing on the bypassed pages, and thereby diminishes the value of such marks. Another theory is that deep linking interferes with existing commercial relationships that the Web site owner has with third parties such as sponsors, who derive revenue from advertising or referrals from bypassed pages, thus undermining their value. Yet another theory is that a deep link circumvents legal notices on a Web site, such as the site's contractual terms of use or service, proprietary warnings such as to copyright and trademark ownership, notices and waivers; thereby, undermining a Web site owner's contractual relationship with end users.

The litigation between Ticketmaster and Microsoft a few years ago illustrates some of the liability issues and underlying legal theories that have been articulated with respect to linking.[5] The case arose after Microsoft posted on its Microsoft Network (MSN) Web site pages containing event guides tailored to particular cities. Microsoft called these pages its city "sidewalk" sites. The "sidewalk" pages in question listed schedules of live entertainment events such as concerts, plays and professional sports events for Seattle. Such pages incorporated a deep link connecting to an internal page on Ticketmaster's

[4] Such links will be legally permissible "in most cases", but not all. In the recent DVD de-encryption cases, which will be discussed in more detail in the text, *infra*, a link that facilitates infringement was found to be unlawful.

[5] Case No. 97-3055, U.S. District Court for the Central District of California

site through which a person could purchase tickets to such events directly over the Internet.[6]

Ticketmaster then sued, asserting that Microsoft, by making it possible for visitors to Microsoft's sidewalk sites to access Ticketmaster's live event information and services without Ticketmaster's approval, and by offering such information as a service to end users of Microsoft's web site, was "feathering its own nest" at Ticketmaster's expense, and that Microsoft was, in effect, committing electronic piracy.

Ticketmaster's complaint also asserted that Microsoft's deep linking to the internal pages on Ticketmaster's independent web site misappropriated Ticketmaster's name and trademarks and diluted and diminished their value, thereby violating U.S. trademark law (i.e., the Lanham Act).[7] Ticketmaster argued that an integral part of its services was selling and marketing tickets to entertainment events through use of the Internet, noting that the Ticketmaster's Web site provided listings and ticketing access to more than 25,000 events across the United States, and that Ticketmaster was one of the leading providers of automated ticketing services, with ticket sales for its clients exceeding $1 Billion annually.

Ticketmaster also asserted that Microsoft had committed unfair competition and unfair business practices and made false and misleading statements in violation of California's common law and California's Business and Professions Code,[8] and that by so doing Microsoft had enhanced the value of Microsoft's Web site and business and diluted and diminished the value of Ticketmaster's Web site and business. Ticketmaster further

---

[6] It is interesting to note that Ticketmaster and Microsoft had earlier tried to negotiate a contract that would allow Microsoft to post a link to such information and to Ticketmaster's automated ticket purchase software on Ticketmaster's site, but the parties failed to reach agreement. It was after such negotiations had failed that Microsoft placed the deep link to such information on its MSN Seattle Sidewalk Web site, and the legal battle then followed.

[7] Case No. 97-3055, U.S. District Court for the Central District of California.

[8] The citations to California law were premised on Ticketmaster's having its principal place of business in Los Angeles.

asserted that Microsoft had gained revenue from advertising made a part of Microsoft's site, but deprived Ticketmaster of favorable advertising business and opportunities; presumably, because Ticketmaster's home page, which generated advertising revenue, had been bypassed through the deep link.[9] The complaint also indicated that Ticketmaster had a business relationship with MasterCard requiring Ticketmaster to give MasterCard prominence over other credit cards in any advertising, but that Microsoft's use of Ticketmaster's name in connection with MasterCard did not give MasterCard prominence and thereby diluted the value of Ticketmaster's relationship with MasterCard.

Ultimately, Microsoft settled with Ticketmaster. As part of the settlement, Microsoft agreed that it would link only to Ticketmaster's home page, and not deep link to any of Ticketmaster's interior pages. Although the parties settled before the court could rule on the merits of the respective complaints, the case is nonetheless valuable for its presentation of theories that could prove successful in an action asserting a claim for injunctive relief and for damages based upon unauthorized deep linking to commercially valuable information or services provided by interior pages of one's Web site.

In a somewhat similar case involving Ticketmaster, but with a different outcome, a rival online ticketing service, Tickets.com, extracted data from interior pages on Ticketmaster's site that provided event listings.[10] After extracting such data, Tickets.com then posted it on the Tickets.com Web site. Tickets.com also, however, referred ticket buyers to Ticketmaster's site via a direct hyperlink. The link consisted of the words, "Buy this ticket from another online ticket company". Tickets.com also posted adjacent to the link a disclaimer that stated, "These tickets are sold by another ticketing company.

---

[9] In another case involving Ticketmaster (discussed in text below), the court noted that Ticketmaster received about 3 Million visits ("*hits*") a day on its home page.

[10] *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000), *aff'd without opinion*, 2 Fed.Appx. 741, No. 00-56574, 2001 WL 51509 (9th Cir. Jan. 22, 2001) (Not selected for publication in the Federal Reporter, No. 00-56574).

Although we can't sell them to you, the link above will take you directly to the other company's website where you can purchase them". Despite Tickets.com's efforts to qualify the extraction of data and use of the link, Ticketmaster asserted that Tickets.com's actions constituted misappropriation, false advertising and unfair competition.[11]

It is important to point out here the means by which Tickets.com obtained its event listings information. As the court noted in its Order in response to Ticketmaster's motion for a preliminary injunction, the vast amount of ticket information that Tickets.com provided on its Web site came from Ticketmaster's site, and Tickets.com did not obtain such information in the same way that the general public did. The general public had to follow a circuitous path, starting at Ticketmaster's home page and following a chain of links originating from there to access interior pages before they could read the events listings. Tickets.com, by contrast, monitored Ticketmaster's thousands of interior Web pages[12] by using "webcrawlers" or "spiders", robotic software programs that would scan Web pages of other sites for particular kinds of information, methodically extract such information and then, copy and transmit it back to Tickets.com's fileservers. Tickets.com would then place the information on its own Web pages, formatted in Tickets.com's own style.

Despite Tickets.com's extensive and intrusive data-gathering practices, the court had difficulty accepting many of Ticketmaster's liability theories. In fact, the court rather bluntly stated its view that Ticketmaster was "attempting to find a way to protect its expensively developed basic information from what it considers a competitor."[13]

---

[11] The claims make some sense when Ticketmaster's own business practices are taken into consideration: Ticketmaster often enters into exclusive arrangements with event promoters to be the exclusive vendor for their ticket sales.

[12] Ticketmaster used a large number of interior "event" pages which changed with additions or modifications to as many as 35,000 pages per day.

[13] *Ticketmaster*, 2000 WL 1887522, at *3.

Moreover, the court was precise in pointing out that, under copyright law, facts are not eligible for copyright protection, no matter how much effort or expense is incurred in gathering them. The court cited to the U.S. Supreme Court's 1991 decision in ***Feist Publications***[14] for supporting principles. Indeed, the court noted, Tickets.com had taken "great care" not to use Ticketmaster's format and style expression in publishing the facts that were extracted from Ticketmaster's Web site.

The court also found that the Internet address references (URLs) for the interior Web pages which Tickets.com's spiders copied were not protectable under the copyright law, because the URLs contained only functional and factual elements and not original material. Analogizing to a reverse engineering case[15], the court determined that copying of the URLs was a fair use under the copyright act, because the spiders copied only non-protectable (i.e., factual) data. Nor was the court able to find that the events information of Ticketmaster's site qualified for copyright protection under a "hot news" exception, even though the value of such information was time-sensitive. The court pointed out that Tickets.com referred visitors seeking such information to Ticketmaster's site for purchase of tickets to such events. Such referral thereby diminished any profit motive Tickets.com may have had to exploit such information to Ticketmaster's resulting commercial loss. Indeed, the court found no such loss, but rather a potential gain, from the customers referred to Ticketmaster's site to Tickets.com's site.

The court also found that Ticketmaster's Lanham Act and trademark infringement theories lacked sufficient facts to be supported. The court determined that Tickets.com did not "pass off" itself as Ticketmaster, but instead had "carefully" stated on its Web site that it could not sell the referenced tickets but would refer the buyer to another broker, specifically, Ticketmaster, who could sell the tickets to them. Similarly, the

---

[14] *Feist Publications v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991).

[15] *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).

court found no confusion as to the source or identity of goods and services, because when a potential customer was transported by the link that Tickets.com posted, that potential customer was sent to the Ticketmaster home page, which was distinguished by Ticketmaster's marks and logos. Nor was the court able to find reverse palming off because the disclaimer that Tickets.com posted with its link to Ticketmaster's site made it clear that Tickets.com was not pretending to be Ticketmaster or acting on Ticketmaster's behalf. As for Ticketmaster's false advertising claim, the court found that a few mistakes in phone numbers and other information appeared to be stray errors and did not rise to the level that would merit the court's imposing injunctive relief.

The court did find, however, that two of Ticketmaster's theories demanded serious consideration and might well prove decisive at trial, although the court did not consider them sufficient grounds for the purpose of granting a preliminary injunction.

The first of those theories is copyright infringement. The court pointed out that Tickets.com's undeniable copying of the "electronic bits" which made up Ticketmaster's event pages would violate the copyright act if such copying were not legally justified. Although the court gave reasons why it thought that Tickets.com's copying activities were justified, determination of that issue was not necessary to the purposes before the court (i.e., whether to grant an injunction), and so the court in passing noted that the door was open to another trial court to resolve such issue in some other case at some other time in the future.

Secondly, the court found particular significance in the emerging theory of trespass to chattels applied to the online medium, particularly as expressed in the California District Court's decision in eBay's case against Bidder's Edge.[16] The court pointed out that the question of invasion of Ticketmaster's computers by Tickets.com's spiders, and possible consequent damage to such computers, was not presented in the complaint requesting

[16] *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 2000 U.S. Dist. LEXIS 7287 (N.D. Cal. 2000). The case is discussed in the text, *infra.*

injunctive relief, but the court stated that it found itself to be much in agreement with the opinion in the eBay decision.

Additionally, there is another theory that merits consideration, although the Ticketmaster court dismissed it in its Order. Ticketmaster also asserted that Tickets.com's spidering of Ticketmaster's site was sufficient to support a breach of contract claim, on the basis that Tickets.com's acts violated the terms of use posted on Ticketmaster's Web site. Some commentary suggests that the "click-wrap" contract established by a Web site's terms of use may be more enforceable, and used by more courts in future decisions, than the Ticketmaster court was able or willing to recognize.[17]

These two *Ticketmaster* cases illustrate that because the law is developing in this new area, at this point it is possible for the courts to reach apparently contradictory conclusions. They also indicate that because the state of the law is in such flux, the facts, and particularly the way in which business is conducted over the Internet, may prove decisive.

In contrast to decisions supporting linking, there have been two instances in which linking was determined to be unlawful as a matter of principle. Those cases relate to the "cracking" of the encryption codes for DVD copy protection software, and the dissemination of the cracked code by means of hyperlinked Web sites. Such cases illustrate that the courts may be quite willing to invalidate links when those links intentionally facilitate illegitimate copying or misappropriation of proprietary information.[18]

A few years ago, members of the hacker community in Norway and elsewhere figured out the algorithm and master keys to de-encrypt the motion picture industry's Content

---

[17] See, for example, Mark Grossman, *"Ruling on Deep Linking Proves Less than Deep Thinking"*, LEGAL TIMES, July 21, 2000. (Article also available from law.com).

[18] *DVD Copy Control Ass'n v. McLaughlin*, No. CV786804, 2000 WL 48512 (Cal. Super. Ct. Jan. 21, 2000), *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

Scrambling System (or, "CSS"), a software program that prevents movies recorded on DVDs from being copied electronically, as by a computer. The hackers disseminated the "cracked" code in the form of a de-encryption program they named, "DeCSS", by posting such code for download from various Web sites. They also encouraged others to link to such sites and encouraged the creation of a plethora of "mirror" sites throughout the World Wide Web to make it impossible for the motion picture industry to shut down all sites facilitating such illegal copying and distribution. In a pair of cases, one adjudicated in a State Court in California, the other in a Federal District Court in New York, the courts determined that such dissemination was unlawful, although each on different legal grounds, and enjoined distribution of DeCSS.

The California State court analyzed the case as a trade secret that had been misappropriated in violation of the California Civil Code's version of the Uniform Trade Secrets Act.[19] The court ascertained that the CSS program had likely been de-encrypted by reverse engineering, which was improper under the Civil Code. The court's decision indicates a particular concern that, given the power of the Internet to disseminate information and the defendants' stated determination to do so, the motion picture industry's right to protect its CSS encryption system as a trade secret would "surely" be lost and the protection afforded by the encryption system would become "completely meaningless" if hacking of the CSS program was not enjoined. The court, in fact, was emphatic that despite the wide dissemination of DeCSS by illicit postings on a vast number of Web sites, the trade secret status should not be deemed destroyed. To hold otherwise, the court asserted, would do nothing less than encourage future misappropriators of trade secrets to post the fruits of their wrongdoings on the Internet as quickly and as widely as possible and thereby destroy a trade secret forever. Accordingly, the court sanctioned the defendants' de-encryption and resulting DeCSS program.

---

[19] *DVD Copy Control Ass'n v. McLaughlin,* No. CV786804, 2000 WL 48512 (Cal. Super. Ct. Jan. 21, 2000).

However, the court refused to enjoin the defendants from linking to other Web sites containing the de-encryption program. The court stated that it was particularly concerned about preserving the free flowing nature of the Internet, asserting that, links to other Web sites were the "mainstay" of the Internet and indispensable to a user's ability to conveniently access the World Wide Web's vast repository of information.

In a parallel case, the United States District Court for the Southern District of New York enjoined individuals who owned and operated Web sites (such as, "dvd-copy.com," "krackdown.com", and a site popular with hackers on which was published an online hackers "webzine"), that distributed DeCSS by on-site download.[20] In this case, however, instead of finding a trade secret disclosure, the court found that the defendants violated the anti-circumvention provisions of the Digital Millennium Copyright Act, which prohibits "offering to the public, providing or otherwise trafficking in any technology designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under the Copyright Act."[21]

The defendants argued they were entitled to various defenses afforded under the DMCA, such as reverse engineering, encryption research or security testing exceptions, but the court was not persuaded, and also rejected their claim that they were engaged in a "fair use" of the CSS program. Of particular merit is the court's freedom of expression (i.e., First Amendment**)** analysis. The court found that although there was some expressive content in the DeCSS program, such expressiveness was minimal compared with the program's functional aspect. The court determined that because the principal purpose of the program was to render an encrypted data file on a DVD intelligible to the average end user, the DeCSS program essentially should be regarded as

---

[20] *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

[21] 17 U.S.C. § 1201(a)(2). The DMCA includes in its definition of circumvention the descrambling of a scrambled work, or decrypting an encrypted work

a "virtual machine"[22]. The court found that the predominant character of DeCSS was no more expressive than an automobile ignition key. The court pointed out that the DMCA facilitates the Copyright Act's protective purpose of advancing the public welfare through promoting science and the useful arts, because the DMCA is a tool to protect copyright in the digital age. Consequently, as the security of DVD technology is essential to the continued distribution of motion pictures in DVD format, without effective limits on de-encryption technologies, protection of DVD content by the Copyright Act would become "meaningless," and the continued marketing of DVDs, impractical. The end result could only, therefore, be discouragement of artistic progress and an undermining of the goals of the Copyright Act. Accordingly, on the grounds of such violation of the DMCA, the court prohibited the defendants from not merely posting the offending software on their Web sites, but also from knowingly linking to other Web sites posting the de-encryption software.

Another area of potential liability involves a kind of linking actuated by what is called an IMG or "in-line" link. This kind of link displays text, or more commonly, an image, that appears to be a seamless part of the content of the displaying (or, "parent") Web page, even though such text or image may originate from an entirely different Web site. That is, it is impossible to tell by just looking at it, that the text or image actually originates from another location. The way IMG links work is that they load such off-site content automatically at the same time that the end user's browser loads the content resident on the parent page; the in-line link therefore displays off-site content at the same time that the browser displays the parent Web page.[23] IMG or in-line links can create liability for a Web site owner and operator if they index proprietary content without authorization. Such liability can emanate under the theory that the link violates

[22] *Universal City Studios*, 82 F. Supp. 2d at 222.

[23] IMG links, which display content automatically or passively without any action on the part of the end user, are activated by coding on the Web page itself. Consequently, IMG links function in an opposite way to the more common kind of link, an "HREF" or referential link, which activates linked content only when an end user "actively" clicks on the link.

display or performance rights under the Copyright Act, because the link enables the automatic display of a portion of another Web page's copyrighted content.

One other area of potential liability due to linking is in hyperlinks in EDGAR documents filed by a publicly traded company with the Securities and Exchange Commission. In November 2000, the SEC published on its Web site a "staff guidance" stating the SEC's position that linked documents in a company's reporting materials would not be deemed part of the company's official filing for determining compliance with reporting obligations, but would nevertheless be subject to the civil liability and antifraud provisions of the federal securities laws.[24] Moreover, hyperlinks in the reporting materials to other hyperlinks, which in turn link to yet other hyperlinks, will be treated as conjoined, thus making all the material that the hyperlinks conjoin a constructive part of the reporting materials. Thus, a company could be subject to liability for securities fraud under Rule 10b-5 if its reporting material contain links to other Web sites publishing favorable but materially incorrect information such as might be contained in analyst reports or news articles about the company. Although the "staff guidance" does not have the force of regulation or law, it is significant as the first major statement by a Government agency that comments on a potential liability creating by linking to a third party's site.

II. Framing

Framing is another Internet technology, kindred to linking, that could subject Web site owners and operators to liability. Framing can be described as internal coding on a Web page that enables another Web page (including, a Web page from a different Web site) or content from another Web page to appear within a smaller window on the enclosing page. The leading case on this subject involved an action brought by The Washington Post, Time, Entertainment Weekly Magazine, CNN, the Los Angeles Times, the Wall

[24] EDGAR Filer Information: Electronic Filing and the EDGAR System: A Regulatory Overview. (Published on www.sec.gov, November, 2000)

Street Journal, and Reuters against Total News Inc. Total News operated what the plaintiffs described in their complaint as a "parasitic" Web site.[25] Total News framed on its site news and editorial content it had lifted from the plaintiffs' Web sites without their permission. An end user clicking on a hyperlinked item, indicated by a trademarked logo of one of the plaintiffs in a list of news sources, such as CNN or Time, appearing on Total News's site, would be transported to the corresponding Web site of that plaintiff. The referenced site of the plaintiff, however, appeared within a framed window on Total News's site, rather than filling the entire viewing frame of the end user's browser, as would be the case if the user had accessed an ordinary hyperlink. Moreover, the borders surrounding the frame displayed the Total News name, trademarks and logos, URL and advertisements by Total News's advertisers.

The complaint alleged that such framing pirated the plaintiffs' copyrighted material and trademarks, packaged such material to advertisers as part of a competitive publication, and pocketed the advertising revenue generated by such unauthorized use, thereby misappropriating the plaintiffs' valuable commercial property. Additionally, the complaint asserted that Total News's framing tortiously interfered with plaintiffs' contractual relationships with their own advertisers, because the ads appearing around the frame diverted end users from the plaintiffs' ads, which were obscured by the smaller size of the framed window, interfered with the benefits that plaintiffs' advertisers bargained for when they purchased space on plaintiffs' sites, and rendered plaintiffs' performance of their advertising contracts more burdensome. Plaintiffs also asserted that Total News's conduct constituted unfair competition under common law because it took the entire commercial value of the news reported at each of the plaintiffs' respective Web sites and sold it to others for Total News's profit. Additionally, plaintiffs asserted that Total News's actions diluted the value of plaintiffs' trademarks, constituted false representations and false advertising, and deceptively

[25] *Washington Post Co. v. Total News, Inc.*, No. 97 Civ. 1190 (PKL) (S.D.N.Y. complaint filed Feb. 20, 1997).

caused end users to believe that Total News had an affiliation with the plaintiffs or was sponsored or otherwise approved by them. Although the parties settled before the court could issue a ruling, the case usefully illustrates legal theories that one can expect will form the basis for binding precedent in this area before long.

III. **Spidering, Web Crawling, and Other Uses of Bots**

Spidering, Web-crawling, and related software programs powered by "robots" or "bots" are particularly interesting from a legal perspective because the cases involving the use of these programs have generated a new class of Internet liability theories, namely trespass and trespass to chattels. This cause of action may emerge as the most powerful Internet-related liability theories, particularly as applied to the gathering of data from another party's Web site. A recent case illuminates such theories.

The case involves the use of "spiders" or "web crawlers," which are essentially virtual robots (or, "bots" in cyberspeak) consisting of software programs that sift through Web pages, retrieve data from such pages, and copy and convey it to another site.[26] Such bots are capable of executing thousands of instructions per minute. The defendant, Bidder's Edge, operated an online "auction aggregation site," a site that enabled Internet auction buyers to search through a variety of different on-line auctions without having to visit and search each host site individually. The Bidder's Edge Web site provided access to a database containing information on more than five million items available for auction through more than one hundred online auction sites. Bidder's Edge included in such database information that it had obtained from the Web site of the Internet's largest online auction house, eBay.[27]

---

[26] e*Bay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 2000 U.S. Dist. LEXIS 7287 (N.D. Cal. 2000).

[27] eBay's complaint asserted that querying activities by the Bidder's Edge spiders constituted up to 1.53% of the number of requests that eBay received on its site, and up to 1.10% of the total data transferred by eBay over a period of two months. At the time of the decision, eBay had over 7 million registered users, and more than 400,000 new auction items were added to eBay's Web site

Bidder's Edge compiled its database by having its spiders crawl through such auction sites, harvest relevant information, and bring it back to Bidder's Edge for further analysis and compilation. About 70% of the auction items listed in Bidder's Edge's database originated from listings on eBay's Web site. Moreover, Bidder's Edge spiders accessed eBay's site approximately 100,000 times each day.

eBay moved for a preliminary injunction asserting that the Bidder's Edge spiders caused irreparable harm to eBay's computer system by consuming its processing and storage systems, thereby making that portion of system capacity unavailable to eBay and its authorized users, reducing the performance of eBay's system, and resulting in damage to customer goodwill and a corresponding loss of profits. eBay premised its claim on various theoretical bases, yet, of greatest interest and persuasion to the court, were the trespass theories. The court pointed out that fundamental to the concept of ownership of personal property is the right to exclude others, and drew the following analogy: If eBay were a "brick and mortar" auction house with a limited number of seats, it would be entitled to reserve those seats for potential bidders, refuse entrance to individuals or, as the court punctuated, robots, and seek injunctive relief against non-customer trespassers whom eBay was physically unable to exclude.

The court indicated that under California's law, action based on trespass to chattels would lie if an intentional interference with the possession of personal property had proximately caused injury. The court also noted a recent California decision where trespass to chattels was employed as a tort theory to cover the unauthorized use of long distance telephone lines.[28] The electronic signals generated by the defendants in that case were deemed sufficiently tangible to support a trespass cause of action. Analogously, the court observed that the electronic signals sent by the Bidder's Edge

---

listing every day. Additionally, 600 bids were placed every minute on nearly 3 million items. Thus, bidding for and sales of items were continuously going on in millions of separate auctions.

[28] *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal.App.4th 1559, 54 Cal. Rptr.2d 468 (Cal. Ct. App. 1996).

spiders and bots to retrieve information from eBay's computer system were also likely to be sufficiently tangible to support eBay's trespass cause of action.

The court stated that under California law, for eBay to prevail on a claim for trespass based on accessing a computer system, it had to establish two elements: first, that Bidder's Edge intentionally and without authorization interfered with eBay's possessory interest in its computer system, and second, that the unauthorized use of that system by Bidder's Edge proximately resulted in damage to eBay.

The court was not persuaded by Bidder's Edge's argument that trespass on eBay's site was impossible because the site was publicly accessible. The court asserted that eBay's servers, which were accessed when visitors landed on eBay's Web site, were, in fact, private property and that eBay granted conditional access to them, as indicated in eBay's terms of service for its Web site. eBay's terms of service expressly prohibited the kind of automated access made by Bidder's Edge. The court found that the repeated queries by the Bidder's Edge bots, in any event, had exceeded the scope of the conditional consent to access that eBay granted visitors to its site, and that therefore, Bidder's Edge's use of eBay's system was unauthorized.

Further, the court pointed out that under California law, substantial interference with eBay's possession of its property was not required to establish trespass. Rather, it was enough if Bidder's Edge "intermeddled"[29], or even merely used eBay's property, and such intermeddling or use diminished the value or quality of that property. The court found such diminishment in the appropriation of valuable bandwidth and system capacity by the 80,000 to 100,000 daily search requests made of eBay's computers by the Bidder's Edge bots.[30]

---

[29] *eBay*, 100 F. Supp. 2d at 1070.

[30] Interestingly, the court found irrelevant Bidder's Edge's argument that such search requests represented a negligible load on eBay's system, even if true. The important principle to consider, the court asserted, was that Bidder's Edge had derived eBay of the ability to use that portion of its

One additional observation by the court merits discussion, however, because it identifies the possible grounds on which other courts may later decide that the trespass theory is insupportable with respect to Internet claims. That is the subject of preemption under the Copyright Act.

In the eBay case, Bidder's Edge also argued that eBay's trespass claim and other state law-based claims were preempted by federal copyright law because Bidder's Edge had merely copied eBay's factual (and non-original) auction listings, and such copying was a right permitted under federal copyright law because facts and other content which lacks the statutory modicum of creativity are not copyrightable. Yet, the court in reply stated that a state law cause of action will be preempted under the Copyright Act only if the rights asserted under state law are "equivalent" to those protected by the Copyright Act, and the work involved also falls within the subject matter of the Copyright Act. In order not to be deemed equivalent, the court indicated, the right under state law must have an extra element that changes the nature of the action so that it is qualitatively different from a copyright infringement claim. Based on the facts, the court found that such an extra element did exist, namely, that eBay asserted a right not to have Bidder's Edge use eBay's computer systems without authorization. According to the court such a right, that is, the right to exclude others from using physical personal property, was not equivalent to any rights protected by copyright, and therefore constituted the extra element to make trespass qualitatively different from a copyright infringement claim.

The court in the Bidder's Edge case, however, was careful to point out that the court in the *Ticketmaster v. Tickets.com* decision, which was discussed above, saw matters differently on this subject of preemption. Thus, it is possible that later courts could find the court's reasoning in the Bidder's Edge decision unpersuasive, and decide not to follow it. Surely, developments on the preemption will be keenly watched by the courts and interested counsel in ensuing months and years.

---

personal property for its own purposes, and the law recognized no such right to use another's

IV. **Metatags**

Another important potential area of on-line liability in e-business is in the use of metatags. Metatags are words or phrases written in special hypertext markup language (HTML) and embedded in the software code of a Web page and therefore not visible to end users. Metatags enable search engines to find a particular Web site or page more easily, and correspond to the keyword or words that an end user is likely to type in when submitting a search query to a search engine in order to find a particular Web site. Search engines scan for such keywords in domain names, actual text on a page, and metatags when processing search queries. The presence of such keywords in the metatags of a Web page's coding significantly enhances the likelihood that such page will appear in the list of "hits" that the search engine returns to the end user after processing the end user's query.

The courts have looked to trademark law for guidance when adjudicating disputes in this area. The leading case, *Brookfield Communications, Inc. v. West Coast Entertainment Corporation*,[31] involved one of the largest video rental chains in the U.S., the defendant West Coast, and a software company, the plaintiff Brookfield, that owned an interactive electronic database of entertainment industry-related information.

Brookfield began retail marketing of its database product, named, "moviebuff," on disc in 1993. It began using its Web sites to vend such product and to offer access to a similar Internet-based interactive database, which was also marketed under the "moviebuff" mark in 1997. Brookfield filed an application to register the "moviebuff" word as a trademark and a service mark for software and an on-line database in 1997, and the U.S. Patent and Trademark Office issued a registration of those marks to Brookfield in 1998.

---

personal property.

[31] *Brookfield Communs., Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036 (9th Cir. 1999).

West Coast decided to join in the "dot com" revolution in 1996 when it registered the phrase, "moviebuff.com" as a domain name. However, West Coast did not use "moviebuff" as a trademark in commerce until November of 1998, when it made a widespread public announcement about the imminent launch of its moviebuff.com Web site.[32]

The dispute arose when Brookfield learned of West Coast's intention to launch a Web site at "moviebuff.com" and to market through that site a searchable entertainment database similar to Brookfield's "Moviebuff" products.

West Coast asserted that earlier in 1991 it had obtained a service mark registration of the words, "The Movie Buff's Movie Store" for purposes of retail store and rental services featuring video cassettes and video game cartridges and claimed that it had first used such mark in commerce in 1986. West Coast also claimed that it had been using various phrases including the words "Movie" and "Buff" to promote goods and services in its video stores since 1988. Accordingly, West Coast sought to apply the "tacking" doctrine of trademark law to extend the reach of West Coast's earlier 1986 service mark first use date and tack it onto West Coast's later 1998 first use date of the "moviebuff.com" mark. The "tacking" doctrine is a constructive use theory under U.S. trademark law. If accepted by the court, the doctrine would enable West Coast to claim seniority user status with respect to the "Movie Buff" and "moviebuff.com" marks on the grounds that the marks were so substantially similar to each other that consumers would generally regard them as the same.

The court determined that Brookfield's "moviebuff" mark for software and software related services, and West Coast's "moviebuff.com" and related online products, were "virtually identical", and that it was therefore likely that consumers would be confused

[32] The court determined that merely registering a word or phase as a domain name is not sufficient in itself to qualify as a first use in commerce which would confer seniority usage rights (including privilege to enjoin junior users from employing such marks) under trademark law.

in distinguishing between the two. The court also drew a conclusion that many Web users would be likely to think that the company that made "moviebuff" products and services also operated the moviebuff.com Web site. The court found authority for this conclusion in several earlier but recent decisions, which observed that Web users often assume that the domain name of a particular company will be the company's name followed by "dot com", and that companies attempt to make the search for their respective Web sites as easy as possible by using their corporate name, trademark or service mark as their Web site address.[33]

In its complaint, Brookfield also asked the court to enjoin West Coast from using marks that were confusingly similar to "moviebuff" in metatags and other buried software coding on West Coast's Web sites. In responding to such request, the court determined that if West Coast did use such marks, it would result in "initial interest confusion" in the minds of consumers, which would be damaging to Brookfield. Initial interest confusion occurs when a consumer is diverted by a competitor from obtaining the product of a particular vendor that the consumer initially was interested in and perhaps intended to purchase, and instead is presented with a similar product of the competitor.

The court surmised that using another's trademark in one's metatags was much like posting a sign with another's trademark in front of one's store. To illustrate, the court posited the following analogy:

> "Suppose West Coast's competitor (let's call it 'Blockbuster') puts up a billboard on a highway reading -- 'West Coast Video: 2 miles ahead at Exit 7' -- where West Coast is really located at Exit 8 but Blockbuster is located at Exit 7. Customers looking for West Coast's store will pull off at Exit 7 and drive around looking for it. Unable to locate West Coast, but seeing the Blockbuster store right by the highway entrance, they may simply [choose to] rent there. Even consumers who prefer West Coast may find it not worth the trouble to continue searching for West Coast since there is a Blockbuster right there.

[33] Such presumption or "rule of thumb" was expressed in *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998), and *Beverly v. Network Solutions, Inc.*, No. 98-0337, 1998 WL 320829 (N.D. Cal. Jun. 12, 1998).

> Customers are not confused in the narrow sense: they are fully aware that they are purchasing from Blockbuster and they have no reason to believe that Blockbuster is related to, or in any way sponsored by, West Coast. Nevertheless, the fact that there is only initial consumer confusion does not alter the fact that Blockbuster would be misappropriating West Coast's acquired goodwill."[34], [35]

Extending such analogy to Brookfield, the court deduced that Web surfers looking for Brookfield's "moviebuff" products but were taken by a search engine, due to embedded metatags, to westcoastvideo.com, would find a database similar enough to the "moviebuff" database such that an appreciable number of them would decide instead to purchase the offerings available on the West Coast site to which the search engine led them. Consequently, the court concluded, by using "moviebuff" or "moviebuff.com" in metatags on its Web site, West Coast would improperly benefit from the goodwill that Brookfield had built up in its mark.

Accordingly, the court determined that the Lanham Act barred West Coast from including in its metatags any term that was confusingly similar to Brookfield's mark. The court enjoined West Coast from using or facilitating the use of the "moviebuff" mark or any other terms likely to cause confusion with it, including in buried code or metatags on West Coast's Web site or in connection with the retrieval of data or information on other goods or services. Also enjoined was use of the phrases, "moviebuff.com" and "@moviebuff.com" in such metatags.

Similarly, other courts have enjoined the use of metatags containing marks that were deemed misleading to consumers on the basis that they produced initial interest confusion. For example, in one such case, the defendant, a company named Radiation

---

[34] *Brookfield,* 174 F.3d at 1064.

[35] The court derived its analogy from an actual case, *Blockbuster Entertainment Group v. Laylco, Inc.*, 869 F. Supp. 505 (E.D. Mich. 1994), where the defendant, a video rental store, attracted the initial interest of customers by using a sign confusingly similar to its competitor. The court in that case found trademark infringement.

Monitoring Devices ("RMD") not only used its competitor's trademark in metatags placed on its own Web site, but also copied into such site the metatags and HTML coding that were embedded in the competitor's own Web pages.[36] The competitor and plaintiff was a company named Niton Corporation.

The case emerged when a technician responsible for maintaining Niton's Web site discovered during Web site maintenance procedures that when he ran search engine queries to test the site's metatags, the Web site of Niton rival RMD curiously appeared in the search results. Investigating further, the employee visited RMD's site and used the "View Source" command of his Web browser to reveal the source coding for RMD's site. He discovered that the metatags on RMD's site were identical to those that he had used when creating Niton's Web site. Moreover, he discovered that among RMD's metatags were key words that were relevant to the products that Niton sold, but were not relevant to any of RMD's products.

The technician then performed an Internet search using the phrase, "home page of Niton Corporation", and discovered that only three of the direct "hits" were for pages on Niton's site, but five of the other results listed were references to RMD Web pages. Also investigating the source coding for such pages on RMD's site, the technician was astonished to find metatags stating, "The Home Page of Niton Corporation". He then repeated the search using several other search engines, and received virtually identical results. Lastly, he executed a search query using the search terms, "Niton Corporation" and "Home Page", and discovered that a number of the search result "hits" were Web pages the metatags of which described the pages as being the home page of Niton but which also gave the Web site address (URL) of RMD's site.

Obviously, due to the egregious copying made evident by the facts, it did not take much to persuade the court in this case, and the court enjoined RMD from using RMD's Web

---

[36] *Niton Corp. v. Radiation Monitoring Devices, Inc.*, 27 F. Supp. 2d 102, 1998 U.S. Dist. LEXIS 18538 (D. Mass. 1998)

sites, and means of attracting Internet users, such as by metatags, in a way likely to lead users to believe that RMD was also known as or affiliated with Niton, that RMD made for Niton any product marketed by Niton, or that RMD Web sites were Niton Web sites.

A couple of other metatag decisions merit mention, because they illustrate instances where the use of metatags which were also trademarks of another party were allowed.

One such case involved a model named Terri Welles, and the company that presides over the Playboy Magazine "empire".[37] Ms. Welles had her own Web site and placed metatags in its source code which included the keywords, "playboy" and "playmate". The site advertised the fact that she was a former Playboy Playmate of the Year, but minimized any use of Playboy's trademarks. Her site also contained a number of disclaimers indicating that her site was neither endorsed by nor affiliated with Playboy. Playboy sought to have her enjoined from using the names that it had trademarked as metatag keywords on her Web site, asserting that such uses infringed Playboy's marks.

The court found that Welles used the "playboy" and "playmate" keywords merely as descriptive terms that fairly and accurately described her Web site, rather than as trademarks, and found that her use of such key words in metatags was a good faith attempt to index the content of her Web site for search engines. Accordingly, the court ruled that her use was permissible under applicable trademark laws.

The other case involves an area of the law that, particularly in the U.S., requires courts to exercise caution when responding to requests for injunctive relief. That is the area of constitutionally protected speech and freedom of expression under the First

[37] *Playboy Enters. v. Terri Welles, Inc.*, 78 F. Supp. 2d 1066, 1999 WL 1296101 (S.D. Cal. 1999).

Amendment to the federal Constitution of the United States. The illustrative case here involves an interior designer and a disgruntled client.[38]

The client was so disgruntled with a designer that he had hired that he went to the effort of registering and building a number of Web sites on which he published his caustic criticism of the designer and her interior design services. The pages of such sites included metatags consisting of keywords stating the name of the designer and the designer's business name. The Web sites contained statements, for example, such as, "Welcome to the first web site designed to protect people from the alleged ill intentions of [name of designer and her company]." The sites, however, also contained disclaimers, cautioning visitors that the sites reflected "only the view points and experiences of one Manhattan couple that allegedly fell prey to [the designer and her company]." And the disgruntled client made certain to ensure that the domain names of his Web sites did not reflect the designer's names.

In a long and thoughtful opinion, the court declined to grant the injunctive relief that the designer requested. Among its reasons for denying such relief, the court reasoned that use of the various designer "marks" in metatags was the only way that the designer's disgruntled client could get his message to the public. Moreover, the court found that a broad rule prohibiting the use of such marks in the metatags of Web sites not sponsored by the designer would "effectively foreclose" all discourse and comment about the designer's company, including fair comment. Allowing such foreclosure would overextend the reach of the Lanham Act to such an extent that it would intrude upon First Amendment values. Citing to informed legal commentary, the court emphasized the importance of creating "critical breathing space" for legitimate comment and criticism about products and services. Additionally, the court observed that metatags effectively serve as a cataloging system for a search engine, and that the client had the right to catalog the contents of his own Web sites.

---

[38] *Bihari v. Gross*, 119 F. Supp. 2d 309 (S.D.N.Y. 2000).

Lastly, in response to the designer's claim that her client's disparaging comments had libeled or otherwise defamed her and her company, the court pointed out that under local (New York state) law, speech concerning the business practices and alleged fraud of the designer was arguably within the sphere of legitimate public concern and thereby vested with a heavy presumption of protection under the State's Constitution. Moreover, the court emphasized, the State's law placed a heavy burden upon the designer, as plaintiff, to prove that the disparaging statements were not opinion, which was granted absolute protection under the State Constitution.

V. **Practical Suggestions**

In light of these decisions and the emerging developments in the law and the directions that the law seems to be taking in regard to the Internet, the following are some practical suggestions that counsel can take to protect their clients who conduct their businesses using these new technologies on the World Wide Web:

LINKING

Prohibit "deep linking" in your Web site's Terms of Service/Terms of Use:

Make sure that there is language in your Web site's Terms of Service or Terms of Use that prohibits deep linking by third parties from outside your site to interior Web pages without your written consent.

Do not "deep link" without authorization:

Examine all externally oriented links posted on your Web pages and remove them unless you have a written consent of the connected site's owner, unless you have a strong linking agreement with such owner. (See below.)

When in doubt, link externally only to home pages.

Do not use third party logos, trademarks or service marks on or with any links, unless you have express written authorization from the owner thereof.

Post Link Disclaimers:

Post prominently and immediately adjacent to every externally-connected link on your Web pages, clear language that disclaims any endorsement or affiliation

with the linked site, unless, of course, you do in fact have an agreement that authorizes such affiliation with the other site's owner.

Disclaim any liability for any loss or damage that the visitor may sustain from using such site. For example, ABC Corp. might use the following language: "These sites are not part of ABC Corp. on the Web, and ABC Corp. has no control over their content or availability."

Consider also language emphasizing that use of the linked site is at the visitor's sole and absolute risk, especially if the site has interactive features or sells consumer products.

Be wary of in-line (IMG) links:

Do not use IMG links to externally located, third party-sited text or images which have copyright or other proprietary protection.

Be wary with SEC reporting and materials:

If you are required to make periodic disclosure reporting to the Securities and Exchange Commission, carefully review all documents to be filed electronically under EDGAR, particularly for externally oriented hyperlinks to third party materials (such as analysts' reports and news articles).

If you are in the process of registering an offering with the Securities and Exchange Commission, the issuer's Web site should be reviewed for links to pages or sites containing information that could be construed as an offer to sell.

Additionally, review all links in offering materials posted on the issuer's Web site.

Do not frame or use in-line third party content on your Web site.

If you cannot avoid linking to third party information, prominently post adjacent to each such link a statement disclaiming responsibility for and all endorsement of, the linked information. In such instances, install an intermediate web page on your web site which states that the visitor has departed your site and will be connected to an unaffiliated third party site.

Ensure that your site is DMCA safe-harbor compliant

Make sure that the notice pages of your Web site include all requisite information (including, that regarding your designated agent for receiving

infringement notices) in compliance with the Digital Millennium Copyright Act, and file the appropriate registration form with the Copyright Office, so as to benefit from the liability limitations of the Online Copyright Infringement Liability Limitation Act.

LINKING AGREEMENTS

Describe with precision the placement and appearance the links are to have on the page. For example, their minimum size, color, font, graphic image (if a logo is to be used).

Describe in particular detail the link structures to be used. For example, if frames will be used, describe the content the frames are to contain, what size and where on the page the frame is to appear, the color and nature of borders, etc.

Specify that no changes in the appearance or placement of the link may be made without the prior written consent of the parties.

If the link is to contain a logo or mark in which you have proprietary rights, specify that no changes may be made to it without your prior written consent.

Additionally, reserve the right to have the link removed if certain practices occur that would have the effect of diluting the goodwill in the mark.

Additionally, allow removal of the link if the link becomes non-functional and functionality cannot be readily restored.

The parties should grant mutual licenses to link to each other's site; if marks or logos are reproduced in the link, the party having proprietary rights in them should grant a license covering such use.

Specify who owns what on the respective sites. For example, you should reserve all rights in your logos and marks except for those rights expressly granted by you in the license for their use as stated in the linking agreement.

Specify that the parties are independent contractors and not co-venturers or agents of each other and as such have no power to bind each other with respect to third parties, unless, of course, such is not the case).

Ensure that in your own Terms of Service or Terms of Use for your Web site, you have strong and clear language stating that third parties operating sites hyperlinked to your own have no power or authority to enter into any binding arrangement on your behalf.

Ensure appropriate indemnities against third party claims arising out of the linked site. Also ensure that your own Terms of Service or Terms of Use exclude all liability for any loss or damage your end users sustain by linking to other sites from your site, including, without limitation, consequential or special loss or damages.

Specify a choice of governing law of your state (excluding conflicts of laws provisions), with a forum selection favorable to you.

FRAMING

Do not frame without authorization:

Frame third party sites only if you have the third party's express written consent or written agreement.

Use Java scripting if necessary:

If external third party framing of your proprietary content is of particular concern, consider incorporating anti-framing technology in the source coding of your Web pages, to deny display of such pages in a Web browser.

TRESPASS

Preclude screen scraping

Prohibit in clear emphatic language in your Web site's Terms of Use or Terms of Service all spidering, web crawling, and the use of automated software robots

to gather extract data from your Web pages and all resident databases, without your express written consent.

If scraping is of particular concern (because your content or particular resident databases have significant economic value to your business), consider requiring

an affirmative click-wrap type of consent to such prohibitions (e.g., an "I Accept" button that the end user must click) before allowing entrance to the Web pages containing such content or databases.

Specify a limited right to use your Web site

State in your Web site's Terms of Use or Terms of Service that the visitor has a limited, non-exclusive license, solely for the visitor's personal use, to access your site, and without your written consent (which consent may be withheld in your sole and absolute discretion) may not use the site for any commercial use, republication, distribution, sale, preparation of derivative works or any other unauthorized use.

Specify also that the right to such use is personal to the visitor and non-transferable.

Additionally, reserve all rights in your intellectual property on the site. Preclude also any acquisition of any ownership rights in the site's intellectual property by the visitor's use of the site.

METATAGS

Be wary of using keywords that are competitor marks

Do not use the trade or service marks of competitors in your metatag keywords, unless those words are also factually descriptive of your own business and business practices.

Do not use third party domain names

Refrain from using keywords that index the home page or interior Web pages of your competitors' Web sites.

Run periodic checks

From time to time, run search queries on the major search engines, using your domain and business names as search terms. If the results suggest that a competitor may be embedding your marks in its Web site, examine that site's source code for infringing metatags.