

## MISCELLANEOUS CONCERNS

---

### LINKING

Easy movement from one web site to another is available through “links” between web sites. Hypertext links are the highlighted text, pictures, or logos on a website that, when selected by a user, connect to another web page. Deep linking occurs when a web site provides a hyperlink to another web site, but instead of going to the other web site’s home page, it goes to another page deep within the web page hierarchy. The effect of this practice is that the linking site’s advertising revenues may be enhanced by providing content from another web site, often avoiding any of the advertising on the other web site.

Litigation in this area has focused on three main areas: copyright, trespass and trademark infringement. In *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 U.S. Dist. Lexis 12987 (D.C. Cal. August 10, 2000), Tickets.com linked to internal Ticketmaster pages and compiled that information on its own site to provide to its own customers. The court ruled that there was no infringement, however, because the activity fell within the fair use doctrine and the “hot news” exception. Likewise, finding that there was insufficient interference with the Ticketmaster web site, the court ruled that the physical harm requirement for trespass was not satisfied.

In contrast to the Tickets.com case, the court in *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000) found that trespass to a company’s web server was a valid theory and granted a motion to enjoin Bidder’s Edge from accessing eBay’s servers. eBay is an auction site that lists millions of auctions each day.

Bidder's Edge developed software that searched eBay's server and retrieved information about the auctions. The court found the software effectively diminished the performance of eBay's servers and qualified as a physical harm under trespass law.

These cases show that Internet linking is an evolving area of Internet law that may implicate a variety of intellectual property concerns. Some businesses have actually entered into agreements to allow for, and control, such links between web sites. The American Bar Association has published a guide entitled *Web-Linking Agreements: Contracting Strategies and Model Provisions*, which is available for purchase at <http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5070311>. The advice of counsel may also help a business evaluate the potential risks involved in linking and possible use of a web-link agreement.

## FRAMING

Framing is another approach to keeping a particular business in the mind of a viewer. It allows the content of one site to surround or "frame" the content of a "framed" site, thus enabling a web site to bring up the content of the other website within its own display borders. Web users can surf through multiple sites within a frame in this manner, while the frame site continues to be displayed. Although there are legitimate uses for such a web page design, if the use of the frame incorrectly suggests to consumers that the information within the frame is somehow associated with the information outside the frame, then unfair confusion may result and liability may follow. In fact, with regard to unfair competition concerns, framing may be more objectionable than linking. See *Hard Rock Cafe Int'l v. Morton*, 1999 U.S. Dist. Lexis 8340 (S.D.N.Y. 1999) (noting that framing, unlike linking, combines the websites into "a single visual presentation").

In addition to unfair competition, copyright and trademark infringement may be implicated with regard to framing. In *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2001), the Ninth Circuit Court of Appeals found that a company's use of an image search

engine that returned thumbnail-sized images was fair use but found that inline linking and framing violated copyright laws when applied to full-sized images. Thumbnail photographs are smaller versions of a full-sized image that have lower resolution than the full-sized image. Arriba developed a search engine that scoured the Internet to find images. The results page included thumbnails of the images. The court found that this action was merely a tool to improve access to images on the Internet. Because of the low resolution in the thumbnails, the court reasoned that the images would not be displayed in the same manner as the original. In contrast, the court found that the resultant full-sized images were not merely a means to access information, but rather, were the end product themselves. As such, the court ruled that it was not fair use and enjoined Arriba from further displaying the full-sized images.

## **DEFAMATION**

Defamation is a major issue on the Internet, largely because of its widespread reach and its ability to conceal anonymous users. The basic issues underlying defamation on the Internet are almost identical to other areas such as television and the newspaper. Internet publication takes place when and where the offending material is accessed. Because defamation is determined by state law, the elements vary by jurisdiction. Generally, to prove defamation, a plaintiff must demonstrate (1) the statement was published; (2) the statement referred to the plaintiff; (3) the statement was defamatory; (4) the statement was false; (5) the defendant was either (a) negligent in publishing the statement and the publication was a direct cause of actual damage to plaintiff's reputation or (b) clearly and convincingly shown to have published the statement with knowledge of its falsity or with reckless disregard for its truth or falsity.

There are several areas where defamation can emerge on the Internet, including: (1) e-mail (including one to one e-mail, mailing lists and newsgroups) which can be forwarded to others, and (2) through the world wide web, including web pages and web sites.

E-mail from employees can be a concern for a business in which the company's name appears in the employee's e-mail address ([employee@abc-co.com](mailto:employee@abc-co.com)). A plaintiff may be more likely to sue the business, since it has deeper pockets than the employee.

The law to date has dealt primarily with service provider liability, in part due to their deep pockets. For a good overview of defamation issues involving the Internet, see *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998). This case involved a statement published in the "Drudge Report," available through America Online, accusing White House Advisor Sidney Blumenthal of covering up abuse of his wife. The court granted America Online's Motion to Dismiss because, as an Internet service provider, it was shielded from defamation liability. According to § 230C of the Communications Decency Act, "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," 47 U.S.C. § 230 (c)(1). This case contains an interesting discussion of defamation concerns arising from publication on the Internet and makes a clear distinction between the original party responsible for posting defamatory messages and the Internet service provider who may serve as nothing more than a conduit for the dissemination of the information.

Two prominent pre-Communications Decency Act cases dealing with service providers are *Cubby Inc. v CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991), and *Stratton Oakmont Inc. v Prodigy Services Co.*, 1995 N.Y. Misc. LEXIS 229, 23 Media L. Rep. 1794 (Sup. Ct. N.Y. 1995). In *Cubby*, defamatory material was published on a forum provided by CompuServe. The Court held that CompuServe would not be liable, because it acted as a distributor of a forum edited by another party and not as a publisher of the statements. CompuServe argued in *Cubby* that it had no opportunity to review the contents of the publications before they were uploaded onto the computer. It is important to note that a distributor generally must have some knowledge of the contents of defamatory material which it distributes before it will be held liable for defamation. The test laid

down by the Court in *Cubby* was whether the provider “knew or had reason to know of the alleged defamatory statements.”

In *Stratton*, defamatory material was again published on the Internet and the service provider was sued for the information posted by its subscribers. Here, the Court found Prodigy liable as a publisher, not a mere distributor, because Prodigy exerted some form of editorial control of the information posted on its bulletin boards and it utilized an automatic software screening program. Unlike *Cubby*, the Court said that Prodigy was clearly making active decisions regarding the content of information published on bulletin boards. Prodigy was not successful at arguing that it simply could not control 60,000 daily messages posted through its service. The case is distinguishable from *Cubby* and post-Communications Decency Act cases however, in that it involved use of a former employee’s unretired access code. As such, Prodigy could arguably be liable under negligence theory.

The parameters of defamation claims relating to material posted by individuals on the Internet are still a largely unsettled area of law, particularly as defendants are often difficult to locate, thus deterring many potential lawsuits. As such, this area of the law involves uncertain rights and potential liabilities for individuals and businesses.

## **CENSORSHIP AND FREE SPEECH**

It is no secret that pornography is freely available on the Internet. The Internet has also been used to distribute “hate speech.” The question of the availability of pornography and the distribution of hate speech on the Internet is no less vexing than the question of pornography and hate speech in the off-line world.

In reaction to the issue of children’s access to pornography on the Internet, Congress passed the Childrens’ On-line Protection Act (“COPA”), which was to go into effect on November 29, 1998. See 47 U.S.C. § 221. One day after COPA became law, a lawsuit was filed by the American Civil Liberties Union along with web site operators and content providers challenging the constitutionality of COPA. This challenge pits the First Amendment’s constitutional

protection of freedom of speech against the desire to protect children from exposure to pornography. It follows an earlier attempt by Congress to regulate content on the Internet through the Communications Decency Act of 1996 (“CDA”) which attempted to regulate, among other things, the access of minors to “indecent” and “patently” offensive speech on the Internet. According to the CDA, it is a crime to transmit a “communication which is obscene, lewd, lascivious, filthy, or indecent with intent to annoy, abuse, threaten or harass another person.” Portions of the CDA were invalidated by the Supreme Court in *ACLU v. Reno*, 117 S. Ct. 2329 (1997) as violative of the First Amendment. The invalidated portion made it a crime to send any “obscene or indecent” material on the Internet knowing that it could be seen by someone under eighteen. COPA is an attempt to cure the constitutional defects of the CDA. In this second lawsuit, *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999), the plaintiffs contended that COPA will have a chilling effect on what can be communicated via the Internet and that COPA:

- (1) violates the right to constitutionally protected speech,
- (2) is not the least restrictive means available to satisfy the government’s interests in protecting children,
- (3) is overbroad,
- (4) prohibits even useful information,
- (5) restricts anonymous communications,
- (6) is too vague.

The district court agreed with the ACLU’s contentions, granting a preliminary injunction against enforcement of COPA. On appeal, the Third Circuit affirmed, *ACLU v. Reno*, 217 F.3d 162 (3d Cir. 2000). The U.S. Department of Justice filed a petition for writ of certiorari requesting review by the United States Supreme Court. On March 2, 2004, the United States Supreme Court found COPA unconstitutional. See *Ashcroft v. ACLU* 124 S.Ct. 2783 (2004)

discussed in the section Advertising and Children.

Efforts to regulate speech on the Internet face tough constitutional barriers because of the extreme difficulty involved in narrowly tailoring restrictions so as to avoid imposing overbroad limits on legal types of speech.

One option that has been proposed is adoption of a “kids” top level domain, in which adult-only sites would be prohibited from operating, and an “xxx” top level domain where pornography and other adult sites would be available. Registrations in the “kids” top level domain are already offered through the New.net Registry, although no measures are in place to keep adult-content out of websites offered at these addresses.

For more information see the following web sites of the organizations involved in the lawsuit against COPA; American Civil Liberties Union (<http://www.aclu.org>), Electronic Frontiers Foundation (<http://www.eff.org>), and Electronic Privacy Information Center (<http://www.epic.org>).

## **GAMBLING**

Internet gambling violates provisions of federal law under 18 U.S.C. § 1084. This section prohibits the foreign or interstate transmission of bets or wagers or information on bets or wagers by use of a wire communication. For example, operating an off-shore sports betting operation that utilizes the telephone system within the United States is illegal, *United States v. Blair*, 54 F.3d 639 (10th Cir. 1995). As Internet transmissions are conducted over telephone lines, this is a potential area of liability for gambling service providers.

Internet gambling services are also illegal in Minnesota. Such activities include sporting events, lottery tickets, and simulated casino games. Generally, it is unlawful in Minnesota to sell or transfer a chance to participate in a lottery, Minn. Stat. § 609.755(2). Sports bookmaking is defined as “the activity of intentionally receiving, recording or forwarding within any 30-day period more than five bets, or offers to bet, that total more than \$2,500 on any

one or more sporting events,” Minn. Stat. § 609.75, Subd. 7.

Engaging in sports bookmaking is a felony. Finally, intentionally receiving, recording, or forwarding bets or offers to bet in lesser amounts is a gross misdemeanor, Minn. Stat. § 609.76, Subd. 1(7).

The Minnesota Court of Appeals upheld jurisdiction against an out of state Internet gambling service provider in *State of Minnesota v. Granite Gate Resorts, Inc.*, 568N.W.2d 715 (Minn. Ct. App. 1997). The Court found that because the provider had advertised on the Internet on-line gambling services and had developed from the Internet a mailing list that included one or more Minnesota residents, the provider had purposefully availed itself of the privilege of conducting commercial activities in Minnesota to an extent that maintenance of an action in Minnesota did not offend traditional notions of fair play and substantial justice. Therefore, the provider was subject to personal jurisdiction in Minnesota.

There is also a potential for individual bettor liability in Minnesota. In Minnesota it is unlawful to make a bet through Internet gambling organizations. Minnesota law makes it a misdemeanor to place a bet unless done pursuant to an exempted, state-regulated activity, such as licensed charitable gambling or the state lottery, Minn. Stat. §§ 609.75, Subd. 2 - 3; 609.755(1). As Internet gambling organizations are not exempted, any person in Minnesota who places a bet through one of these organizations may be committing a crime. Further, Minnesota law provides for forfeiture provisions related to unlawful gambling activity. It is the Minnesota Attorney General’s position that a computer that is used to play a game of chance for something of value would be subject to forfeiture under Minnesota law. For the Minnesota Attorney General’s position on the legality of gambling, see <http://www.jmls.edu/cyber/docs/minn-ag.html>.

## **FILE SHARING**

Since the personal computer was developed, computer owners have traded files amongst themselves through a variety of means. With the advent of hard disk technology capable of downloading and storing large files, music files such as MP3s became one of the

most popular subjects of file sharing. File sharing technology, of course, allows easy transfer and replication of all files in the MP3 format, including those comprised of copyrighted material.

In the first file sharing case to reach a court of appeals, the Ninth Circuit found music sharing pioneer Napster liable for contributory and vicarious copyright liability as well as for assisting online users to download copyrighted music, *A&M Records v. Napster*, 239 F.3d 1004 (9th Cir. 2001). Napster was developed as a software program that ran on a central server as well as on individual computers. Users who downloaded the software were able to search music files on others' computers, transfer those copies, and store exact copies on their hard drives.

In *MGM Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154, 1160, (9th Cir. 2004) the Court concluded that, unlike *Napster*, these peer to peer file sharing services could not control activities of users and therefore were not liable. The Court also found that the Grokster service was capable of substantial non-infringing uses.

On June 27, 2005 the United States Supreme Court issued a long awaited ruling concerning the peer-to-peer networks that allowed millions of individuals to download copyrighted music via the Internet. In *MGM v. Grokster* 544U.S.903 (2005) the Supreme Court found that manufacturers and providers of software or technology that allows others to copy songs may be held liable for the infringing acts of others who use their software for such infringing activities. The Supreme Court determined that it was not sufficient for the provider of the peer-to-peer network technology to demonstrate that the software was capable of non-infringing use. Even if capable of non-infringing uses defendants who operate such peer-to-peer networks can now be held liable for the infringing acts of individual end-users if the defendants acted with the intention or objective of promoting use of the technology to infringe copyright. The Court found evidence in this case that Grokster had taken steps to actively induce and encourage copyright infringement and was therefore liable for infringement. It remains an open issue as to whether a peer-to-peer network with

substantial non-infringing uses and that is not actively promoted as a way to pursue infringing activities will be deemed a legitimate and legal program.

The *Napster* and *Grokster* cases provide guidance to businesses that are using file-sharing technology on the Internet. Software should not be designed primarily for infringing purposes. Businesses must also recognize that they have some duty in protecting a copyright holder's rights. These steps will legitimize file sharing and will allow companies the ability to share and exchange ideas in real-time. Neither of these cases suggest that the actions of individuals who download and copy music or film are not infringers and the recording industry has more aggressively gone after individuals.

## **SECURITY HACKING AND COMPUTER CRIMES**

As the Internet grows into a serious business tool, security has become a major issue.

There are many security systems and products which can be put in place to ensure that hacking and other security breaches do not occur. In addition, businesses can limit unauthorized access and hacking by employees by implementing security policies regulating the use by employees of the company's network.

The first federal computer crime statute was the Computer Fraud and Abuse Act of 1986 ("CFAA") (amended in 1996). This act imposes penalties for the intentional "access" into "federal interest computers" for the purpose of committing certain types of criminal conduct. The statute criminalizes seven types of computer activities:

- (1) the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or advantage a foreign nation;
- (2) the unauthorized access of a computer to obtain protected financial or credit information;

- (3) the unauthorized access into a computer used by the federal government;
- (4) the unauthorized interstate or foreign access of a computer system with an intent to defraud;
- (5) the unauthorized transmission of program information, code or command, intentionally causing damage, or the unauthorized access of a protected computer which causes or recklessly causes damage;
- (6) the fraudulent trafficking in computer passwords affecting interstate commerce; and
- (7) the intentional transmittal of any threatening communication in interstate or foreign commerce for purposes of extortion.

*Any* computer used in interstate or international commerce in the commission of the offense would be covered by this provision.

Amendments to the CFAA have been added to deal with the problem of “malicious code” - computer viruses, computer worms, and other computer programs that are specifically and intentionally designed to alter, damage or destroy files or computer programs. Federal law also protects the integrity or confidentiality of electronic communications. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to expand federal jurisdiction and to criminalize the unauthorized interception of stored and transmitted electronic communications. There are some exceptions to the ECPA, which provide business owners and individuals access to stored communications. The entity providing the electronic communications service is allowed to access stored communications and the user of the service is allowed access if they were either the originator or intended recipient of the electronic communication at issue. In addition, the ECPA does not prohibit conduct which is authorized by the party providing the e-mail (business owner) and for certain governmental or law enforcement activities.

Minnesota has its own computer crime statute, Minn. Stat. § 609.87 et. seq. The statute is based upon the federal computer crime statute and provides that:

- Whoever intentionally and without authorization damages, destroys, alters, or distributes a destructive computer program with the intent to damage or destroy any computer, computer system, computer network, computer software, or any other property is guilty of computer damage;
- Whoever (a) intentionally and without authorization or claim of right accesses or causes to be accessed any computer, computer system, computer network or any part thereof for the purpose of obtaining services or property; or (b) intentionally and without claim of right, and with intent to deprive the owner of use or possession, takes, transfers, conceals or retains possession of any computer, computer system, or any computer software or data contained in a computer, computer system, or computer network is guilty of computer theft; and
- A person is guilty of unauthorized computer access if the person intentionally and without authority attempts to or does penetrate a computer security system.

## **EXPORT CONTROL COMPLIANCE**

Since doing business on the Internet may involve global electronic transactions, it is important for businesses to be aware of federal export control regulations and to implement procedures to assure compliance. An individual should be designated with responsibility for monitoring federal export control regulations and communicating such information to the relevant staff. Distribution or license agreements should include provisions requiring compliance with the federal export control regulations.

Of particular interest are the United States government's regulations on encryption software. Encryption allows for the protection of information by converting plain text into unreadable

ciphertext. While the use of encryption may aid companies in protecting things such as trade secrets and confidential company records, the extent to which encryption provides such protection is great, and the protected information can all together be lost if the decryption key is ever misplaced.

The Export Administration Regulations (“EAR”), implemented by the Federal Department of Commerce, impose certain restrictions on the export of non-military encryption goods. Generally, one must obtain a license from the Bureau of Export Administration prior to exporting encrypted goods. EAR addresses the specific issue of exporting encryption products over the Internet. Under EAR, downloading, or causing downloading, outside of the United States, of encrypted source and object code software constitutes export. While the government maintains that the purpose of encryption laws is to safeguard national security and aid in the investigation and prosecution of crime, they have been challenged by some as burdensome, anti-business, and in a recent case, *Bernstein v. U.S. Department of Justice*, 176 F.3d 1132 (9th Cir. 1999), the Ninth Circuit Court of Appeals found that encryption software was speech protected by the First Amendment and restricting its export was an unconstitutional prior restraint. The Court of Appeals, however, recently withdrew the *Bernstein* opinion and granted a rehearing in the case. Such action is a prime example of the uncertainty and change in this area of law, like others involving regulations that change from time to time, and may require the counsel of experts who are knowledgeable in the most current government position. For up-to-date information and assistance, you can contact the United States Department of Commerce, Minneapolis Export Assistance Center at 612.348.1638.

## **PRESERVATION OF THE ATTORNEY-CLIENT PRIVILEGE ON THE INTERNET**

Among other things, the attorney-client privilege prevents an attorney from testifying against his or her client’s interest based upon information provided to the attorney by the client. This privilege only protects private, not public, communications

between the attorney and client. It is the obligation of the attorney to not knowingly reveal a confidence or secret of his or her client.

How is the attorney-client privilege maintained when e-mail is used for such communications? According to the Minnesota Lawyers Professional Responsibility Board, the attorney does not violate the rule against knowingly revealing a client's confidences by using e-mail without encryption to transmit and receive confidential client information. Most states have similar standards, though many suggest or require obtaining client permission prior to using e-mail for sensitive information, and others suggest encryption. The American Bar Association Standing Committee on Ethics and Professional Responsibility recently issued a formal opinion that a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct. It is still a wise business practice to obtain client consent before using e-mail and to use encryption whenever particularly sensitive information is to be transmitted via the Internet.

## **COOKIES**

As you surf the Internet, you may unwittingly leave information about yourself at each site you visit. Your e-mail address, type of computer used, and the URL (Universal Resource Locator) of the site from which you traveled is information that can be captured by each site that you visit. From these visits, a host server can identify certain information about an individual. This information or "cookie" allows the web site server to obtain information about the visitor's preferences. The use of cookies has obvious appeal to online businesses that can derive valuable marketing information from anyone who visits their web sites.

DoubleClick is one example. The company received a patent on a "method of delivery, targeting, and measuring advertising over networks" from the United States Patent and Trademark Office. This patent relates to the process of depositing cookies onto a user's computer and relaying consumer information back to

DoubleClick. DoubleClick is enforcing its patent against alleged infringers. Meanwhile, several defendants argue that the practice of collecting personal information is an invasion of privacy. Amid the controversy, the Federal Trade Commission concluded that the company did not violate its privacy policy with its data collection practices.

Businesses who use marketing services such as DoubleClick should be aware of a new privacy standard called Platform Privacy Preferences (P3P). The technology is part of Internet Explorer 6 and allows web surfers the ability to configure their browsers to automatically determine whether a web site collects personal information. The software differentiates “first-party” cookies and “third-party” cookies. First-party cookies are set from the site being visited. Third-party cookies are set by marketers or ad networks to track consumer preferences. P3P requires that marketers and ad networks develop and post privacy policies that can be read by the browser or they may not be able to use cookies.

Although new technology is on the horizon to allow a user to set preferences, businesses should be careful when volunteering their personal information when visiting web sites. Completing the ubiquitous on-line questionnaire, they may not realize the extent to which this information may then be used and sold for marketing and other purposes. There currently are no specific laws and regulations prohibiting the use of cookies on the Internet. However, potential plaintiffs may argue their cases using the Electronic Privacy Act, the Wiretap Act or the Computer Fraud and Abuse Act.

## **SECURITIES TRANSACTIONS**

The securities industry has already been profoundly affected by the Internet. The Securities and Exchange Commission (SEC) now allows publicly traded companies to submit financial information electronically. See [www.sec.gov](http://www.sec.gov). The Electronic Data Gathering Analysis and Retrieval System (EDGAR) is a system that supports this on-line filing process. The SEC even makes available

information on class action securities and fraud litigation. The Internet has also become a forum allowing potential investors to investigate and obtain information on companies. Actual stock purchases are now possible on the Internet. There is even discussion of possibly creating an entirely on-line stock exchange.

The benefits of easy access and the ability to process financial data on a global basis in real-time are enormous for those involved in the securities industry. Unfortunately, the Internet's ability to enable many people to publish and distribute information regarding securities and potential investments also results in easy access to false information. The flow and availability of information on the Internet is also difficult to monitor. There is increasing concern by federal regulators such as the Federal Trade Commission about on-line credit scams and deceptive trade practices as well as on-line investment fraud. There are also new technologies trying to address the situation.

One such technology is a Smart Card. Smart Cards are credit card-size pieces of plastic that contain an embedded micro controller chip. The cards are attached to a personal computer and contain software and hardware security features and can run executable code. With this technology, users of the cards are able to encrypt data within the public-key infrastructure. Businesses dealing with secured transactions should consider such a technology to prevent multiple-user access to a single account.

## **ACCESSIBILITY-AMERICANS WITH DISABILITIES ACT**

In one of the first court decisions to consider the applicability of the American With Disabilities Act (ADA) to websites, a federal judge rejected a lawsuit contending that a Southwest Airlines website violated the ADA because it was not accessible by blind users. The judge ruled that it was up to Congress to specify by legislation that websites were a "place of public accommodation." *Access Now, Inc., v. Southwest Airlines, Co.*, 227 F.Supp.2d 1312 (SD Fla. 2002).