# E-COMMERCE DEVELOPMENTS: ACROSS E-COMMERCE LAW ON HORSEBACK*

**By**

**Jere M. Webb****

Prepared for Oregon Law Institute
Business Law Seminar
February 25, 2005


* The allusion, intended to be tongue-in-cheek, is to Karl Llewellyn's seminal work "Across Sales on Horseback," 52 Harv L Rev 725 (1939).

** The author acknowledges valuable assistance from Lewis & Clark Law School third-year law student Joshua W. Smith in preparing this article.

# Table of Contents

## 1. Introduction

What follows are snippets from the world of e-commerce law. Some are hot off the press, such as the first two items reporting on significant e-commerce legislation signed into law by President Bush in the final hours of the last session of Congress (extending the Internet tax moratorium and penalizing providing false domain registration information), California's direct marketing disclosure statutes which went into effect last month, and the recent release by the European Union of contractual provisions that qualify businesses for safe-harbor treatment when collecting and sending to the United States personal data on European Union citizens.

Some are not so new, but still not discovered by the majority of U.S. online businesses, such as the decision by the European Union to tax online services and downloaded software sold by U.S. businesses to residents of the now 18 countries of the European Union, and California's adoption of its Online Privacy Protection Act, which will require revision of most online privacy policies for any business collecting personal data from a California resident.

Some report on continuing controversies in which the courts are split, such as how to treat use of another's trademarks in metatags or to trigger banner ads or pop-up ads, and what online activities will subject a website owner to jurisdiction by foreign courts.

All are developments that every online business should know about.

Enjoy the ride.

## 2. Congress Extends Internet Tax Moratorium

In December 2004, Congress extended the Internet Tax Freedom Act, which prevents new state taxes on Internet-based transactions and services, but does not impact existing state laws, including existing state sales tax laws. The act is now extended for three additional years. The new legislation was delayed in Congress because of concern by many states that it would prevent collection of taxes from telephone companies with respect to telephone calls transmitted over the Internet. As a compromise, Congress eliminated that concern by allowing states and cities to continue to collect taxes on telephone services, even if the calls are made over the Internet.

Note that this law does not prevent application of existing state tax laws to online transactions, and states are mobilizing to tax online sales.

## 3. Congress Passes Fraudulent Online Identity Sanctions Act

In December 2004, President Bush signed into law the Fraudulent Online Identity Sanctions Act as part of the Intellectual Property Protection in Courts Administration Act. This legislation provides stiff penalties for providing false domain name registration information. Specifically, it amends the Lanham and Copyright acts to provide that a trademark or copyright infringement violation will be considered "willful" if the violator knowingly provided misleading or false contact information in making, maintaining, or renewing registration of an Internet domain name. In addition, it adds a new criminal provision, 18 USCA § 3559 (2000 &

Supp 2004), that requires judges to double, or boost by seven years, the sentence for a felony offense that involved the use of a falsely registered Internet domain name.

False domain name information is very common. Virtually every online scam artist and most spam senders provide false registration information. If enforced, the new law will significantly curtail this practice. At a minimum, doing something online of questionable legality while maintaining false domain name contact information, will become much more hazardous.

**4. New California Direct Marketing Disclosure Statute Will Impact Most Online Sellers**

Effective January 1, 2005, California's new direct marketing disclosure statute will impact all online sellers who collect or have collected, in connection with a business transaction, personal information from consumers residing in California. Such businesses are required to provide notice to California consumers of their rights under the statute and how they can obtain information on personal information provided to third-party direct marketers. There are several authorized notice options, but the easiest one is to modify the company's online privacy policy to notify the consumer of his or her rights and to designate an address or toll-free number that the consumer may use to request specified information, including the identity of third parties who have been provided personal information within the last year.

This statute will require most online sellers to revise their privacy policies. Note that the statute does not regulate disclosure of personal information, but rather merely provides a mechanism by which consumers may obtain information about a company's personal information disclosure practices.

With limited exceptions, the statute covers any disclosure to a third party of personal information about a California resident. "Third party" is defined broadly in the statute and includes an affiliate of the disclosing party, if the affiliate is a separate legal entity. There are exclusions for certain disclosures to third parties in connection with implementing a transaction with a California resident, such as third parties who provide data administration or customer service, as long as those third parties do not use or disclose the information for their own "direct marketing purposes." In addition to direct solicitations, "direct marketing purposes" is defined to include selling, renting, exchanging, or leasing personal information to other businesses.

Businesses subject to the new law are those that during the prior calendar year have disclosed "personal information" to "third parties," when the business knew or reasonably should have known that these third parties used the personal information for their own direct marketing purposes. "Personal information" includes any information that identifies an individual, including name, residence address, email address, age or date of birth, number of children, telephone number, information regarding products purchased, payment history, debit or credit card information, and medical information.

Businesses subject to the new law will need to amend their privacy policies and to set up a procedure for providing the required notice to California residents and to provide required information in response to consumer requests.

## 5. New Identity Theft Penalty Enhancement Act

In July 2004, President Bush signed legislation passed by Congress in response to the growing problem of identity theft as more and more Americans use the Internet to shop and manage their personal finances. The Identity Theft Penalty Enhancement Act amends the federal criminal code to establish penalties for aggravated identity theft in addition to the existing punishments for related felonies. The act adds two years to prison sentences for "knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person" during and in relation to specified felony violations. It also adds five years to the sentences of violators who use false identification in the commission of "terrorist acts."

In 2003, identity theft topped the list of consumer fraud complaints to the Federal Trade Commission (FTC). There were 214,905 reported cases of identity theft that year, and the FTC estimates that as many as 27.3 million Americans have been victims of identity theft in the last five years. The FTC published a report in September 2003 estimating that identity theft cost U.S. businesses and consumers $53 billion annually. Betsy Broder, assistant director for the FTC's Division of Planning and Information, claims that the new law will increase the likelihood of thieves being prosecuted, because prosecutors are more likely to bring a case if the law provides for serious jail time.

## 6. European Commission Issues New Set of Standard Contract Clauses for Compliance with European Union Data Directive

On January 7, 2004, the European Commission (EC) issued new standard contract clauses that businesses can use to demonstrate compliance with the European Union (EU) Privacy Directive. The new clauses do not supersede earlier standard contract clauses issued in 2001. Both sets are still fully applicable. The EC issued the second set in response to negotiations with the business community to develop alternative standard clauses that are more "business-friendly." The changes include "more flexible auditing requirements" and "more detailed rules on the right of access." Another change in the contract language is the treatment of third-party beneficiary rights. Data exporters must now be more involved in resolving the complaints of data subjects, through an obligation to contact any data importer and compel it to comply with the contract.

These new clauses are designed to help companies meet their obligations under the Privacy Directive (95/46/EC), which imposes upon member states a duty to block the transfer of personal data outside the EU unless the data importer provides for "adequate protection" of that data. Although the EU has determined that certain countries, such as Canada and Argentina, provide for adequate protection, data importers in other countries, including the United States, must rely on other means to demonstrate compliance.

## 7. California Online Privacy Protection Act

On July 1, 2004, the California Online Privacy Protection Act took effect. It requires that website operators who collect "personally identifiable information" from California residents comply with certain requirements, including posting a privacy policy that tells consumers the types of information collected about users of the site, third parties to whom such information may be disclosed, how consumers can request corrections or changes to their personally

identifiable information, how they will be notified of changes to the privacy policy, and the policy's effective date.

This is the only legislation of its type in the United States. Violation of the act exposes the operator to a civil lawsuit under California's Unfair Business Practices Act.

The act applies only to "commercial" websites but does not define "commercial." The privacy policy must be posted "conspicuously," and the Act provides specific requirements for what constitutes conspicuous posting.

This new law will be a pitfall for unwary website operators and online service providers. Most website operators now have a posted privacy policy, but many do not comply with the act's requirements, meaning that all such policies will have to be reviewed and revised. A cottage industry will almost certainly spring up, composed of lawyers filing suits under the new act. Scarier still, if other states adopt similar legislation, there will be the risk of inconsistent requirements from state to state. This would likely cause Congress to adopt national Internet privacy legislation, which it has been considering for several years.

**8. Beware of Fair and Accurate Credit Transactions Act**

Congress passed this law (commonly called "FACT") in 2003, as an amendment to the Fair Credit Reporting Act of 1970, but its impact is just now filtering down to the business community. It contains two provisions of interest to online sellers: first, it extends the provisions of the Fair Credit Reporting Act to users of credit information, not just credit bureaus and providers of information to credit bureaus; and, second, it contains procedures for responding to cases of identity theft. Since identity theft now occurs largely online or via email, the law's provisions are of particular interest to online sellers.

The law requires users of credit information to comply with notice requirements in connection with taking any "adverse action" based on credit information. An entire cottage industry of lawyers has sprung up to pursue these claims. If you think the potential liabilities are not a big deal, think again. A jury in a federal case in Oregon awarded $5.3 million against TransUnion, one of the three national credit bureaus, for willfully violating the Fair Credit Reporting Act by failing to correct errors in the plaintiff's credit report. It is obvious that juries are extremely sympathetic to the mishandling of credit information. The law also prohibits use of medical information to determine eligibility for credit.

The Federal Trade Commission has recently settled claims against both Sprint and AT&T for allegedly violating FACT's adverse-action notification provisions by using credit scores to deny service to or place conditions on individuals seeking telephone service.

The lesson here is that not just credit bureaus and those providing information to credit bureaus need to be concerned about complying with the Fair Credit Reporting Act. Now, everyone who obtains and uses a credit report has compliance obligations.

The identity theft provisions of FACT took effect on December 1, 2004. The law blocks businesses notified of identity theft from providing information to credit bureaus and also prohibits transfer or placement for collection of identity theft debt. Also, no user of a consumer

credit report that includes a fraud alert may establish a new credit plan, extend credit, or grant an increase in credit limit unless the user implements reasonable policies and procedures designed to confirm the actual identity of the person making the request.

Like the adverse-action notice requirements, the identity theft provisions of FACT are likely to be the subject of many lawsuits, including class actions. Online sellers will need to implement appropriate compliance procedures.

**9. European Union Value-Added Tax on E-Commerce**

In case you haven't heard, the European Union (EU) has extended its value-added tax (VAT) to cover e-commerce; that is, electronically supplied services to consumers located anywhere in the European Union. Is this a big development? You bet.

First, VAT are steep, ranging from 25 percent in Denmark to 15 percent in Luxembourg. Second, lots of U.S. businesses are going to be subjected to the new tax. For many, it will come as a surprise.

The new regime went into effect on July 1, 2003. Before that, VAT was applied based on the residence of the supplier. Under the old regime, EU-based businesses charged for covered services that were exported outside the EU, but businesses outside the EU did not have to charge VAT on covered services supplied to EU customers. Under the new regime, VAT will be applied based on the residence of the customer, not that of the supplier, meaning that U.S. businesses supplying software updates, website hosting, website creation, electronic data, distant learning, online subscriptions, or other electronic services, will, for the first time, be subject to VAT.

The law will have a major impact on U.S. exporters of electronic services. What remains to be determined is how the various taxing authorities in the EU member countries will determine when taxable transactions have occurred and how they will enforce the laws against foreign companies.

**10. Metatags and Initial-Interest Confusion**

The debate over metatags and the trademark doctrine of "initial-interest confusion" continues. Initial-interest confusion occurs when use of another company's trademark, or something confusingly similar to the trademark, leads a prospective purchaser to an unintended seller, but the purchaser discovers the mistake before making a purchase. A plain vanilla initial-interest confusion case exists when the seller intentionally uses another's mark to create the initial confusion, then exploits the situation by selling the misdirected customer competing products. An often cited example would be Burger King's putting up a freeway sign reading "McDonald's – Next Exit." The driver responds to the sign by taking the next exit, only to find Burger King rather than McDonald's. The customer then purchases a hamburger from Burger King.

The initial-interest confusion doctrine is controversial enough when applied in the physical world (after all, the purchaser was not confused as to source when he or she decided to

buy a hamburger, just misled as to the proper freeway exit). When applied to the Internet, the doctrine leads to interesting results that are the subject of heated debate.

The trend in case law is in the direction of holding that use of another's trademarks in metatags does not constitute initial-interest confusion, particularly when the metatag user is not selling competing goods, or if it has a "legitimate" connection with the trademark owner, such as selling or servicing the trademark owner's products or providing after-market replacement parts.

A recent example of this approach to metatag usage is *Bijur Lubricating Corp. v. Devco Corp.*, 332 F Supp 2d 722 (EDNJ 2004). In that case, the defendant used the plaintiff's "BIJUR" trademark in metatags as a method of advertising the defendant's sale of Bijur-manufactured replacement parts and after-market replacement parts for Bijur products. An Internet search for "BIJUR" would produce a list of hyperlinks, including a link to the defendant's site. The court held that this usage constituted "fair use" and did not infringe the plaintiff's trademark rights.

There is a split in the case law on this issue; however, the *Bijur* approach seems to represent the dominant trend. Courts are becoming increasingly sophisticated with respect to search engine methodology and Internet surfing practices and tactics, and are undoubtedly influenced by the fact that any confusion in such cases is fleeting and innocuous. As one court has noted, the prospective purchaser "'would realize in one hot second that she was in the wrong place and either guess again or resort to a search engine to locate [the intended site].'" *Nissan Motor Co. v. Nissan Computer Corp.*, 378 F3d 1002, 1019 (9th Cir 2004) (citation omitted).

Following this approach, the Second Circuit has recently held that the initial-interest confusion doctrine requires a finding of intent and deception, a holding that will doom most initial-interest confusion cases. Similarly, in *Savin Corporation v. Savin Group*, 391 F3d 439 (2d Cir 2004), the court upheld a district court's dismissal of a trademark infringement claim based on the initial-interest doctrine, because the plaintiff failed to demonstrate intentional deception. In evaluating the *Polaroid* eight principal factors to determine the likelihood of confusion, the district court also included an "'Internet initial interest confusion factor'" in the balancing test. *Id.* at 448 (citation omitted). The court agreed that "[b]ecause consumers diverted on the Internet can more readily get back on track than those in actual space, thus minimizing the harm to the owner of the searched-for site from consumers becoming trapped in a competing site, Internet initial interest confusion requires a showing of intentional deception." *Id.* at 462 n 13.

### 11. More on Internet Jurisdiction: Ninth Circuit Holds No Jurisdiction over Anti-Nazi French Companies Suing Yahoo! In France

The Internet insinuates its tentacles all over the world, making it difficult to apply traditional principles of personal jurisdiction, which usually require some pretty significant contact with the forum state. In *Yahoo! Inc. v. La Ligue Contre le Racisme*, 379 F3d 1120 (9th Cir 2004), the U.S. Court of Appeals for the Ninth Circuit held that Yahoo! could not obtain personal jurisdiction in California over two French companies that had sued Yahoo! in France and obtained a judgment there, based merely on the French companies' having sent demand letters to Yahoo! in California and having used the U.S. Marshall Service to serve process on Yahoo! in California for the French lawsuit.

The lawsuit arose out of Yahoo!'s having Nazi-related content on its U.S.-directed website, including auctions of Nazi-related memorabilia and materials. Yahoo! maintained a separate website directed to French citizens, from which such materials had largely been removed, in compliance with French law. Faced with a judgment against it in French courts and substantial daily fines until the materials were removed from its U.S. website, Yahoo! sued for declaratory judgment in federal court in California. The French companies moved to dismiss for lack of personal jurisdiction. The trial court upheld personal jurisdiction and granted summary judgment for Yahoo!, holding that the French court's judgment violated Yahoo!'s First Amendment rights and was not enforceable in the United States. The Ninth Circuit reversed, finding that the French companies had insufficient contacts with California to sustain personal jurisdiction.

Whether sending a demand letter, and related activities, can trigger personal jurisdiction in a declaratory judgment action filed by the recipient in its home state is a tricky issue. In this case, the Ninth Circuit applied the test set forth by the U.S. Supreme Court in *Calder v. Jones*, 465 US 783 (1984), in which the Court upheld jurisdiction in California by a California-based actor in a defamation lawsuit against a reporter and editor of a Florida tabloid newspaper. The Ninth Circuit noted that *Calder* "'cannot stand for the broad proposition that a foreign act with foreseeable effects in the forum state always gives rise to specific jurisdiction'" and that "'something more'" is required in the nature of "'express aiming' at the forum state." 379 F3d at 1131 (citation omitted).

The only clear lesson to be drawn from these cases is that fine lines need to be drawn and that the outcome of individual cases is often unpredictable.

### 12. California Adopts Notice Requirement for Data Security Breaches

California adopted a new law, effective July 1, 2003, that requires businesses to notify consumers whenever hackers gain access to a database containing credit card numbers, Social Security numbers, or other personal information of California consumers.

The new law is expected to cause companies to beef up their computer security systems rather than risk having to provide notice of embarrassing lapses in security. The genesis of the new law was a hacker attack on a State of California payroll database that yielded access to hundreds of thousands of Social Security numbers of state employees.

The new law could have a significant impact on mail-order and online merchants, to the extent that they have California customers. Any person, firm, or government agency that maintains personal information on California residents is subject to the new law.

### 13. Defamation on the Internet: Risks of Getting Hauled into Court in Distant Locations

In the United States, we are used to expansive First Amendment protections that allow great latitude in expressing opinions and generally taking jabs at companies and individuals. Even if what you say turns out to be false and defamatory, in many situations there will be no liability absent proof of "actual malice" or some other heightened proof standard designed to protect speakers, publishers, and the free flow of information.

But what if you make your communication on the Internet? Before you hit the "Enter" button on that Internet posting or publication, you might want to pause to reflect on the facts that your publication will be available worldwide and that many countries have stringent laws against false or defamatory publications.

A good example of this pitfall is the decision issued by the High Court of Australia in *Dow Jones & Co. v. Gutnik*. You can read the opinion at www.4law.co.il/582.htm. The court held that Dow Jones could be sued in Victoria, Australia based on content that appeared in the online version of a *Barron's* magazine article. The article, titled "Unholy Gains," made several disparaging references to the respondent, Joseph Gutnik, who lives in Victoria.

The principal issue in the case was whether publication could be deemed to have occurred in Victoria. Dow Jones argued that the articles published in Barron's Online were published in South Brunswick, New Jersey when they became available on servers located there, and that if someone decided to access those servers and download the articles to a computer in a foreign country, that did not constitute publication in a foreign country. Dow Jones tried to rely on a distinction between the passive role of a Web publisher and the more active role of a newspaper publisher or a radio or television broadcaster. It also argued for the desirability of a single law governing publication of material on the World Wide Web. The High Court of Australia rejected these arguments and found that the article had been published in Victoria. This means that Dow Jones will have to defend the case there, under Australia's stringent defamation laws.

The lesson of this case is that material published on the Internet can result in the unanticipated application of foreign laws and the possibility of being hauled into court in distant locations. You may take some comfort in the fact that, three days after the decision by the High Court of Australia, the U.S. Court of Appeals for the Fourth Circuit issued its opinion in a similar case and held that two Connecticut newspapers that had published articles accessible electronically via their websites, which articles allegedly defamed a Virginia prison warden, could not be sued in a Virginia court. The court said, "[W]e hold that a court in Virginia cannot constitutionally exercise jurisdiction over the Connecticut-based newspaper defendants because they did not manifest an intent to aim their websites or the posted articles at a Virginia audience." The case is *Young v. New Haven Advocate*, 315 F3d 256, 258-59 (4th Cir 2002).

Even more recently, the U.S. Court of Appeals for the Fifth Circuit held that Columbia University and a Harvard professor who made an allegedly defamatory posting on a Columbia-maintained Web-based bulletin board, could not be sued in Texas by an FBI agent who resides there. The article was about the Reagan administration's alleged complicity in the bombing of Pan Am flight 103 over Lockerbie, Scotland. The court found that the article did not "'manifest an intent to target and focus on'" Texas residents and therefore could not support personal jurisdiction over the defendants in Texas. The opinion can be found at *Revell v. Lidov*, 317 F3d 467, 475 (5th Cir 2002) (citation and emphasis omitted).

The bottom line is that although the United States has constitutional protections that both protect speech and protect against being hauled into court in distant locales, you cannot rely on such protections being available under the laws of other countries.

## 14. Company Held Liable for Employee Redistribution of Subscription Email

Can your company be held liable if an employee redistributes an electronic subscription within or outside of the company, in violation of your subscription agreement? You bet.

A federal court in Maryland recently so held in a case in which an employee posted a subscription email report to a company intranet. The employer had paid for a single email subscription, and the subscription agreement restricted further distribution. The court found the employer liable for copyright infringement. The case is *Lowry's Reports, Inc. v. Legg Mason, Inc.*, 271 F Supp 2d 737 (D Md 2003).

Electronic subscriptions are rapidly replacing hard-copy periodicals, and electronic publishers realize that there is lots of money to be made by strict enforcement of subscription agreements. For instance, some publishers take the position that you cannot even copy and circulate the table of contents from a publication without the publisher's permission (and they may be right if the table of contents contains sufficient creative content). Many electronic subscription agreements prevent making and distributing even a single hard copy of the publication, and posting a limited-subscription publication on a companywide intranet obviously violates the subscription agreement and infringes the publisher's copyright. And forget about arguing that the subscribing company did not authorize the distribution (or even, as here, expressly prohibited it) and is innocent of any wrongful intent. In general, copyright laws impose strict liability. "Innocent" infringers are still infringers, and employers are responsible for their employees' acts, authorized or not, that occur within the scope of their employment.

Can you defend the copyright infringement claim if you merely email an electronic publication to a coworker who does not download it, but only reads it in random-access memory and then deletes it? Yes, you can be held liable under those circumstances. Several courts have held that such "ephemeral" copies are sufficient to trigger copyright infringement.

This case is a good illustration of the need for periodic audits to ensure copyright compliance.

## 15. Doing Business on the Web: Jurisdiction over Interactive Websites

The global reach of the Internet raises the possibility that online activities can subject businesses to the jurisdiction of courts in far-flung places. The rules for Internet-based jurisdiction are still being spelled out by U.S. courts. The general rule emerging is that operation of an active Web site, where one actually transacts business through the Web site, is sufficient to confer "general jurisdiction" over the site's owner; that is, to subject the site's owner to all lawsuits of any sort, whether or not related to the Web site's activities. The theory of general jurisdiction is that the defendant is constructively present in the state by reason of doing business with that state's citizens, albeit from a distant locale.

At the other end of the continuum are passive Web sites, which only advertise or provide information to online visitors. Most courts have held that passive Web sites do not provide a basis for jurisdiction. But what about Web sites that provide some limited level of interactivity, such as allowing email exchanges or allowing or requiring visitors to submit personal information?

A court recently answered this question and held that such limited interactivity is not sufficient to confer jurisdiction. In *Hurley v. Cancun Playa Oasis International Hotels*, No. Civ.A. 99-574, 1999 WL 718556 (E.D. Pa. Aug. 31, 1999), the plaintiff, a Pennsylvania resident, was injured while staying at a hotel in Cancun, Mexico. He sued the U.S. agent for the hotel, a Georgia corporation, in the plaintiff's home state of Pennsylvania.

The defendant moved to dismiss based on lack of personal jurisdiction. In the ruling on the motion to dismiss, the court said that Web sites fall under three categories: (1) those that actually conduct business over the Internet, (2) those that allow exchange of information with the Web site, and (3) those that merely post information or advertisements.

The court held that jurisdiction generally exists in the first category and does not exist in the third. However, in the second category, whether jurisdiction exists "is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site." *Id*. at *2 (citation omitted).

The court examined the particular site's level of interactivity and the extent of its contacts with Pennsylvania residents and held that these contacts were not sufficient to confer general jurisdiction. The site accepted and confirmed reservations online, advertised a toll-free number for telephone reservations, and allowed email exchanges with the site's owner. The court found no evidence in the record that these interactive contacts with Pennsylvania residents were sufficiently "continuous, systematic, and substantial" to support general jurisdiction. *Id*. at *3.

Note that this case might have come out differently had the plaintiff's claim arisen out of his contacts with the Web site, but the court was not called upon to reach this issue, because the plaintiff had never visited the defendant's site. What if the plaintiff had booked his reservation on the site? What if he had read the on-site ads and then called the toll-free number to book his room? Answers to questions such as these will have to await future cases.

For two other cases involving limited-interactivity Web sites, see *Molnlycke Health Care AB v. Dumex Medical Surgical Products Ltd.*, 64 F. Supp. 2d 448 (E.D. Pa. 1999) (no jurisdiction in patent infringement case where defendant advertised his products on site and allowed purchases directly from site, but no evidence of significant sales in Pennsylvania), and *Mink v. AAAA Development LLC*, 190 F.3d 333 (5th Cir. 1999) (no jurisdiction over copyright infringement case where defendant's site advertised allegedly infringing software code but had made no sales into Texas).

The application of Internet jurisdictional rules to defamation cases is equally interesting and equally controversial. *See* Jere M. Webb, "Defamation on the Internet: Risks of Getting Hauled into Court in Distant Locations," *at* http://www.stoel.com/resources/articles/ebusiness/developments/ebiz_6.shtm). In *Alternate Energy Corp. v. Redstone*, 328 F. Supp. 1379 (S.D. Fla. 2004), the court held that the sale of online subscriptions was not a sufficient basis to create personal jurisdiction in online libel cases. The court applied the Internet jurisdiction test set forth in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997), which held that engaging in commercial activity over the Internet constitutes sufficient minimum contacts to satisfy due-process requirements, but that posting information on the Internet does not. In *Alternate Energy*, the court noted that "the Fifth Circuit has held that selling subscriptions to view an informational

website does not constitute sufficient commercial activity to invoke jurisdiction under *Zippo* for a defamation action, when the cause of action[ ] arises out of the information posted on the site. *Revell v. Lidov*, 317 F.3d 467 (5th Cir. 2002). The [*Revell*] court held that because the cause of action did not arise out of the solicitation of subscriptions, the defendant's solicitation activity could not give rise to jurisdiction." 328 F. Supp. 2d at 1382. The court held that "selling subscriptions to an internet site to an unknown, relatively small number of Florida residents, without more, does not constitute carrying on a business in Florida. . .and does not constitute the commission of a tortious act in Florida . . . ." The case law is split on the proper test for jurisdiction in Internet-based defamation cases. This issue is of considerable importance, because if simply publishing on the Internet triggers jurisdiction in any country where content is read, Web site owners and Internet publishers will need to "dumb down" their content in order to satisfy the laws of the most stringent jurisdictions or else face lawsuits that could lead to judgments that would put them out of business.

For now, the lesson is this: If you operate an interactive Web site, you are submitting yourself to the possibility of having to defend lawsuits in distant jurisdictions, both in the United States and abroad.

**16. New SPAM Rules: FTC Postpones "Primary Purpose" Effectiveness**

The Federal Trade Commission (FTC) has postponed the date by which email must comply with rules it issued on December 16, 2005, under the federal CAN-SPAM law. Initially, the FTC announced that the new regulations would become effective on February 18, 2005, but the revised effective date is now March 28, 2005. The agency has blamed the delay on a determination made by the Office of Information and Regulatory Affairs that the regulations constitute a "major rule" under the Small Business Regulatory Enforcement Fairness Act and can't take effect until 60 days after they are published in the Federal Register and submitted to Congress.

The CAN-SPAM Act imposes requirements on the use of commercial email messages and provides for civil and criminal enforcement authority to combat unwanted and/or deceptive commercial email. A commercial email message is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service." The FTC has recently issued rules that attempt to define when an email with both a commercial and noncommercial message will be subject to the law. There is an exemption for pending transactions, but it is narrowly drawn such that most existing "relationships" do not qualify.

Any subject email must: (1) contain a functioning return address or Internet equivalent for communication with the sender, (2) contain an opt-out mechanism and notice of how to stop further emails, (3) not contain false or misleading header information or subject line, and (4) be labeled as an advertisement. This last requirement will be a thorn in the side of many businesses, and it is not clear where the label must appear in the email.

The good news is that state email laws are preempted (except as to false header or other false or misleading information). The bad news is that what types of emails are covered is unclear and penalties are severe.

## 17. Utah Appellate Court Holds That Utah Has Personal Jurisdiction over Nonresident Defendant Who Caused a Single Unsolicited Email to Be Sent to Plaintiff in Violation of State Spam Law

In a matter of first impression, the Utah Court of Appeals held that the exercise of personal jurisdiction over an out-of-state company that sent a single email was appropriate because the email represented sufficient contact within Utah. In *Fenn v. MLeads Enterprises*, 103 P3d 156 (Utah App 2004), an action was brought by a Utah resident alleging that the nonresident corporation had failed to comply with Utah's email statute by not identifying unsolicited email sent to her as an advertisement, that the corporation had directed its marketing agent to solicit business by email, and that the marketing agent had sent email to the resident. According to the court, the nonresident corporation could "reasonably anticipate" being haled into state court, and the interests of the state and resident in prosecuting the action outweighed any burden on the corporation in defending against it.

## 18. New York Court Holds That Email Satisfies Statute of Frauds

A New York court has held that an email sent by a defendant accepting the plaintiffs' offer to purchase real property, in which email the defendant had typed his name, satisfies the requirement of the statute of frauds that contracts for the transfer of an interest in real property be evidenced by a writing. Nevertheless, the court dismissed the plaintiffs' claim because the emails the parties had exchanged failed to contain all the essential terms of a contract for the sale of real property.

In *Rosenfeld v. Zerneck*, 4 Misc 3d 193, 776 NYS2d 458 (2004), the plaintiffs made a cash offer to purchase the defendant's house. The defendant responded by email, in which he accepted the plaintiffs' offer, set a date by which the sale must close, and stated that the offer was not subject to any financing contingences. A written contract of sale was to follow. At the bottom of the email, the defendant typed his name. On the defendant's motion for summary judgment, the court held that his email satisfied the requirements of the statute of frauds that contracts for the sale of real property be evidenced by a writing signed by the party to be charged.

An open issue appears to be whether an email sent by an individual from a computer, using software programmed to automatically list his or her name and contact information in the email, would also satisfy the statute of frauds.

## 19. Federal Circuit Provides Potentially Controversial Relief from Stringent Digital Millennium Copyright Act Provisions

In a closely watched case concerning the Digital Millennium Copyright Act (DMCA), the U.S. Court of Appeals for the Federal Circuit recently affirmed a district court's summary judgment ruling in favor of a manufacturer of a universal garage door opener whose transmitter was able to bypass the access control software used on a competitor's garage door opener. In *Chamberlain Group v. Skylink Tech., Inc.*, 381 F3d 1178 (Fed Cir 2004), the court held that the use of the universal transmitter manufactured by the defendant, Skylink Technologies, was not a violation of the antitrafficking provisions of the DMCA. This was a matter of first impression. In reaching its conclusion, the court reasoned that the DMCA does not create a new property right for copyright owners. Instead, the anticircumvention and antitrafficking provisions of the

DMCA merely create new grounds for liability. Therefore, a copyright owner seeking to impose liability on an accused circumventor must demonstrate "a reasonable relationship between the circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization—as well as notice that authorization was withheld." *Id.* at 1204.

The conclusion in *Chamberlain* is in tension with prior decisions in similar cases. The Federal Circuit, however, is not alone in expressing some discomfort with the strictures of the DMCA's broad provisions. Congress has also recently considered clarifying some of the provisions, but no amendments have been adopted. The proposed legislation would have provided that certain defenses against traditional copyright infringement liability are also defenses to alleged violations of the DMCA. Regardless, the *Chamberlain* decision seems likely to mean that in the near term courts will follow the Federal Circuit's lead by inferring policy-based rules for the practical details of DMCA implementation. How far such doctrines can develop and whether Congress will act remains to be seen.

**20. Online Privacy Laws Create New Risks**

Other than the Graham-Leach-Bliley Act (which only covers banks, insurance companies, and other "financial institutions," broadly defined), and the Children's Online Privacy Protection Act (which applies only to personal information collected from children under 13 years of age) in the United States there is no generally applicable federal statute regulating online privacy. Such legislation has been proposed in each of the last several sessions of Congress, but none of these bills have become law. The same is not true in other countries; for instance, the European Union has stringent online privacy rules. See item six, above. The Federal Trade Commission has considered adopting a trade regulation rule covering online privacy, but has decided to follow a "wait and see" approach to assess the need for such nationwide regulation. If many states adopt privacy statutes with differing approaches to regulation, Congress or the FTC may need to step in and preempt the field, much as Congress did with regulation of SPAM.

The FTC currently regulates privacy under its general authority to prohibit unfair or deceptive acts or practices in interstate ecommerce. One of the quickest ways to get in trouble with the FTC is to violate your own privacy policy as many companies have found. Another way is to change your privacy policy without notifying customers and giving them an opportunity to "opt out" of the new policy.

Gateway Learning Corporation recently faced both issues and has agreed to settle Federal Trade Commission (FTC) charges that it violated federal law. The FTC alleged that Gateway Learning rented consumers' personal information to direct marketing companies in contravention of explicit promises made in its privacy policy. The FTC also alleged that, after collecting consumers' information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or gaining consent. This is the first FTC case to challenge deceptive and unfair practices in connection with a company's material change to its privacy policy. The proposed settlement bars Gateway Learning from making deceptive claims about how it will use consumers' information and from retroactively applying material changes in its privacy policy. It also requires that the company give up money it earned from renting the data.

The FTC charged that "(1) Gateway Learning's claims that it would not sell, rent, or loan to third parties consumers' personal information unless it received the consumers' consent, and that it would never share information about children, were false; (2) Gateway Learning's retroactive application of a materially changed privacy policy to information it had previously collected from consumers was an unfair practice; and (3) Gateway Learning's failure to notify consumers of the changes to its privacy policy and practices, as promised in the original policy, was a deceptive practice." The agency charged that the practices violated section 5 of the FTC Act.

The lessons here are: (i) know what is in your privacy policy and follow it; (ii) if you change the policy, give consumers the right to "opt out;" (iii) don't forget to cover transferring such information if you sell your company; and (iv) finally, don't forget about state and foreign privacy laws.

### 21. Google Announces Partnership with Major Research Libraries to Scan 20 million Books for Inclusion in Google's Search Database

Google has announced a partnership with major research libraries to scan 20 million books for inclusion Google's search database. For works that are in the public domain, the full text will be available. For works still possibly under copyright, only portions will be seen. The project has the potential to bring about dramatic changes in the nature of research. The excitement generated by Google's plan, however, has been offset by difficulties in tracking down copyright holders of older works. Google is finding it extremely difficult to determine the property rights for older, out-of-print works. For example, in 1930, there were 10,027 books published in the United States. In 2001, 174 of those books were still in print. That leaves 9,853 books out of print, but presumably still protected by copyright. Before 1978, published work had to have a copyright notice in order to retain copyright protection and then renewed in order for the author to enjoy a full copyright term. At least half of all works published historically never took the first step; almost 90% never took the second. Google faces the challenge of verifying the status of each of the 20 million individual works.

### 22. Lawmakers Target P2P Networks

Congress has recently stepped up efforts to regulate peer-to-peer (P2P) software that enables users to easily share music or video files with each other. P2P networks gained notoriety when Napster established a popular website that facilitated the exchange of music downloads between individuals. The website was eventually shut down through court challenges from the music industry. Since then, many legislators have sought to rein in promoters of other P2P networks, through various forms of legislation. One recent endeavor combines consumer education and criminal penalties.

The U.S. House of Representatives recently passed the Piracy Deterrence and Education Act of 2004. The act requires the U.S. Attorney General to establish a new program, entitled the "Internet Use Education Program," to educate the general public on the value of copyrighted works and to publicize the effect of improper file sharing on the creators of those works. The program would inform consumers about other risks associated with file sharing, including the transmittal of viruses and spyware. Finally, the act would establish a voluntary compliance program administered by the Attorney General, in cooperation with Internet service providers, to

send warning letters to infringers and would outlaw the illegal copying of films at movie theaters. The proposed legislation must still pass the Senate and overcome other legislative hurdles in order to become law. The White House has not yet indicated whether it would support such a measure.

### 23. District Court Holds Amazon Is Entitled to DMCA Safe-Harbor Defense to Infringement Claims Arising out of Activity by Third-Party Vendors

In *Corbis Corp. v. Amazon.com, Inc.*, No. CV03-1415L, 2004 WL 3092244 (WD Wash Dec. 21, 2004), the court held that Amazon met the requirements for invoking the service-provider safe-harbor defense to infringement claims under the Digital Millennium Copyright Act (DMCA). The Plaintiff alleged direct and vicarious copyright infringement based on photographs distributed by a third-party vendor on Amazon's "zShops" platform. The court first held that Amazon satisfied the threshold requirements for the safe-harbor defense: Amazon is a "service provider" under the DMCA, Amazon "adopted and reasonably implemented" a user policy, and Amazon "accommodates and does not interfere with standard technical measures." *Id.* at *7.

Having satisfied the threshold conditions, the court explained that Amazon "must still meet the three conditions for liability protection set forth in [17 USC] § 512(c)(1)(a)-(C)." *Id.* at *14. First, Amazon demonstrated that "it does not have actual or apparent knowledge that material on its network is infringing." *Id.* Second, Amazon showed that "it does not receive a financial benefit directly attributable to any infringing activity that it maintains the right and ability to control." *Id.* Finally, Amazon showed that "it has expeditiously removed or disabled access to allegedly infringing material for which it has received appropriate notice under [17 USC] § 512(c)(3)." *Id.* Having met the three requirements, the court concluded that Amazon "is immune from all monetary relief and, save the limited relief in 17 U.S.C. § 512(j), all forms of injunctive relief for any copyright infringement committed by zShops vendors on the Amazon site." *Id.* at *18.

### 24. Digital Sampling Illegal; Sixth Circuit Adopts Bright-Line Test

In *Bridgeport Music, Inc. v. Dimension Films*, 383 F3d 390 (6th Cir 2004), the court held that even if a sample portion of a song is "de minimis" and the resulting work is not substantially similar to the sample recording, there is still copyright infringement. The court adopted the plaintiff's argument that in sampling cases, no finding of substantial similarity is necessary and even de minimis copying amounts to infringement. With respect to musical *compositions*, however, substantial similarity is still required in order to find infringement, and de minimis copying does not result in substantial similarity. The court felt that it was important to adopt a bright-line test for digital-sampling cases. An editor's note points out that this ruling is unprecedented, so an appeal to the U.S. Supreme Court is a possibility. This case involved 1.5 seconds digitally sampled from the plaintiff's record into the defendant's rap song.