PART ONE

Legal Issues and Considerations

CHAPTER 1

CYBERLAW: THE MAJOR AREAS, DEVELOPMENT, AND INFORMATION SECURITY ASPECTS

DENNIS M. POWERS
Southern Oregon University

INTRODUCTION

As the number of Internet users, Web connections, and personal computers increased exponentially, controversies and legal problems also accelerated in cyberspace without any specific statutes or case law at first to govern the inevitable conflicts. Despite solid preexisting legal foundation, no information medium ever had such an enormous appetite to leapfrog geographic territories and laws, in turn creating intense pressures on that system.

If somebody "ripped off" another's slogan or logo in "pre-Net" California, it was possible that a business located in Chicago would never know the difference. If one person wrote a defamatory article in a local Florida newspaper about someone in Oregon, the defamed person at that time could have died before reading that particular printed statement. Once the Internet came into existence, however, anyone with an Internet connection—whether living in Florida or in France—could stumble across that slogan or posting. Large organizations were caught napping when more nimble entrepreneurs registered their trademarks as domain names and then offered to sell those registrations back for outrageous sums of money. Who could ever have predicted the rise of mass-copying technology such as Napster and Kazaa that bypassed the copyrights of the musicians, composers, and recording studios? Not to mention the countless rogue programmer attacks and security failures of information systems throughout the world.

The wide differences among the laws of wide numbers of states and other countries became quickly evident. Whether entered into by e-mail or not, a contract under certain facts could be fine in Georgia but void in California, and a copyright claim upheld in Japan but not in the United States, with its differing laws and "fair use" exception. Over time, court decisions confirmed that existing legal concepts were applicable to cyberspace, and legislatures enacted specific statutes to fill in the gaps. These basic legal concepts with later refinements proved adaptable to the Internet technology of the new millennium, just as they had during the dawning of new technologies in the past century, and as unfolds during the course of this chapter.

INTELLECTUAL PROPERTY

The rise of the Internet and its conflicts highlighted the entire subject of intellectual property. Although important in pre-Internet property matters, intellectual property considerations became dominant in protecting one's rights to one's creations and the value of a site, its creations, and processes—whether by copyrights, trademarks, or patents.

Copyright Law

Your computer is a worldwide copying machine, and the Internet made it extraordinarily easy for nearly anything to be instantly copied, e-mailed, and printed out anywhere, regardless of the true copyright holder's rights. In response, the United States took the lead to enact legislation that complemented the basic law of copyrights and met this tension between competing interests.

The first major step taken was its enactment of the U.S. Digital Millennium Copyright Act of 1998 (DMCA). The online service provider section of the DMCA establishes the procedures for copyright owners to contact service providers with their complaints over a subscriber's improper online use of copyrighted material. This act mandates providers to remove materials used improperly once they reasonably determine there are, in fact, copyright infringements as alleged. If the subscriber files a counterprotest, however, then the provider must repost the material unless the complainant files a lawsuit against the infringer for copyright infringement over the offending use.

In effect, this legislation grants copyright owners an administrative tool to remove infringing material without having to litigate the problem, as well as a "safe harbor" against liability for U.S. online service providers. The definition of "service providers" is broad and includes not only Internet service providers (ISPs), Web hosting companies, wire and fiber transmission entities, and router services, but also corporations, universities, municipalities, governmental agencies, and other entities that "provide" online services. To receive the protection of this federal statute, an organization must register under the act with the U.S. Copyright Office and follow the DMCA's removal provisions. Check out http://www.loc.gov/copyright for the details on the DMCA.

The United States was the first country to enact DMCA legislation, and this statute took it into compliance with an international copyright treaty (the WIPO Copyright Treaty, 1996). As other countries imitate this general approach, the ability to cause infringing material to be removed without using expensive litigation will begin to become globally codified. Another

significant U.S. legislative enactment was the No Electronic Theft Act of 1997 (NET). Under the NET, criminal penalties can be imposed on people who exchange or barter unauthorized copies of software, videos, clips, or music, whether or not they receive money for it. The only requirement is that the value of the pirated material exceed $2,500 (for felonies) in a given 6-month period. Although enforcement of the NET Act has been limited to high-profile cases thus far, all users should be aware of its provisions.

Among other important copyright areas, cases have held that publishers must pay additional fees for pre-Net work completed by freelancers, including a U.S. Court of Appeals ruling that the National Geographic Society made an unauthorized use of pictures taken by a freelance photographer back in 1961 when it issued a CD-ROM years later of its back issues (*Greenberg v. National Geographic Society*, 2001). It was ordered to pay license fees for that use. The U.S. Supreme Court decided the issue when it later ruled that media companies must obtain the consent of their freelance writers and creators (as employees create "works for hire," their employers typically gain those copyrights) before any pre-Net text, picture, or creation could be posted or sold online, thus forcing royalties to be paid for that use (*New York Times v. Tasini*, 2001).

In the late 1990s, music lovers using a Website and software program called Napster began file-sharing music by swapping digital copies of recordings with one another. After lawsuits by recording industry groups effectively shut down Napster (*A&M Records v. Napster*, 2001), Internet users began sharing music files by using programs that allow them to search the computer libraries of other users. Rather than providing a centralized server where swappers could trade copyrighted material directly à la Napster, this technology allowed users to download software from sites such as Grokster and trade copyrighted music among themselves in an environment that didn't involve a central server. In 2004, the U.S. Court of Appeals for the Ninth Circuit in *MGM Studios v. Grokster* (2004) held that Grokster's use of such a decentralized environment was not a violation of applicable copyright laws as was Napster. On appeal, the U.S. Supreme Court heard oral arguments in 2005 on this case with its decision expected later in the year.

In addition to these aspects, other developments occurred as to the online copyright infringement issue, whether concerning books or music. The U.S. Supreme Court held in *Eldredge v. Ashcroft* (2003) that Congress had acted constitutionally in 1998 when it extended copyright protection for most works through the Sonny Bono Copyright Term Extension Act (Supp. 1999), retroactively increasing the copyright protection term from 50 years after an author's life by another 20 years to 70 in total. Various

cases upheld the constitutionality of the DMCA, including its safe-harbor provisions for ISPs.

The federal courts also have apparently answered the issue as to whether the DMCA mandates ISPs to turn over customer information to the recording industry of those suspected of illegally trading music files. In *Recording Industry Association of America* (*RIAA*) *v. Verizon Internet Services* (2003), the U.S. Court of Appeals in Washington, D.C., overturned the District Court's decision and ruled that the RIAA could not use just subpoenas or simple notices under the DMCA to force ISPs to supply it with user names that it could only identify by their computer's online addresses. The RIAA would have to file a formal lawsuit, then after that filing of its "John Doe" complaint, request a subpoena to secure the identity from the ISP. Immediately after the decision, the RIAA filed four new lawsuits naming 532 "John Does" to show that this added cost to its litigation policy would not deter it. The Supreme Court refused to grant certiorari and rejected the appeal without comment.

Whether the situation concerns Napster imitators, video downloading, or copying overseas, the legal wrangling between copyright holders and the public over "fair use" considerations will continue unabated. As other countries enact their own cyber copyright and intellectual property laws, the likelihood of global jurisdictional disputes increases.

Domain Names and Trademark Law

Trademark Law and Domain Names. For decades before the emergence of the Internet, trademark law was relatively straightforward. Trademarks and service marks abound, simply arising from a company's use of marks identifying certain products or services as being theirs (e.g., Apple with its rainbow apple and eBay's stylized logo). The concept of trade and service marks came about to keep businesses from "passing off" their products as being those of their competitors or of rightful owners, and the ownership of marks is another important intangible property right.

Then along came the Internet, domain names, and new Web sites that had registered the addresses of bona fide trademark and service-mark holders (i.e., Burger King vs. the "burgerking.com" registered by an individual). They knew that the domain name used to access any site was an important asset of identification, just as an entity's mark was important in the decision to purchase a product (or domain name selection). Because domain names must be registered to have any validity and registrars don't conduct background checks over an applicant's representations as to who owns the

legitimate trademark rights, registration even today can be a race to the swiftest on a "first come, first serve" basis.

In the early and mid-1990s, "entrepreneurs" recognized this grand opportunity. In a style reminiscent of the old Gold Rush days, they raced to tie up as many of those good corporate names as they could, whether it was "harvard. net" or "burgerking.com." Later, they would send a demand letter to those entities and offer to sell their domain names back—at a tidy profit. Or the new owners would sit on their names and wait for that interest, conjuring up the concepts of "cybersquatting" and "cyberpirating." When one adds to this equation the various classifications (i.e., from ".com" and ".org" to the later introduced ".biz" and ".info") with the different country designations that are possible, it is easy to see the large opportunities created to tie up good corporate names at a good profit.

A brisk market in the buying and selling of domain names started—just hit the key word "domain name" in your search engines and see what arises. The people who registered general names, such as "business.com" or "loans.com," made excellent business decisions. One Houston businessman paid $150,000 in 1997 for the rights to "business.com," then sold that to a California company for a cool $7.5 million 2 years later. In 2000, mortgage.com was sold for $1.8 million and loans.com for $3 million.

Without any statutory guidance, the courts handed down mixed decisions as to when a mark holder would prevail, if at all, over a cybersquatter and a given domain name. The reason: The law was clear at the time that domain-name registrations and trademarks and service marks, whether registered or not, were two different concepts. Because there was no right by itself to use a mark as a domain name, owning one didn't necessarily convey any ownership rights to the other.

Anticybersquatting Consumer Protection Act (ACPA; 1999). Before the passage of the ACPA, the Federal Trademark Dilution Act (FTDA, 1995) was the statutory alternative that trademark holders used to fight cybersquatters. The FTDA did not require proving a likelihood of confusion on the part of consumers on the use of a disputed mark, but that there was a "dilution" of that mark. This act provided a mark owner with injunctive relief against another's commercial use of one that diluted the distinctive quality of that distinctive mark. Dilution occurred when an unauthorized use lessened the ability of others to distinguish goods or services from the other, including if those actions cheapened that mark (i.e., one Billy Nike establishes a bar called "Nike's Sleazy Palace" to which the sporting goods manufacturer, Nike, takes exception). The FTDA's effect was to protect

famous marks—such as McDonald's or Goodyear—from the use of others that would "dilute" their value. *Panavision v. Toeppen* (1998) was one of the first cases to expand the FTDA's dilution protection of trademarks to domain names. In *Panavision*, the appellate court held that the defendant's actions diluted the value of Panavision's trademark because his registration of "panavision.com" (and attempts to sell that back to the company) weakened the ability of its potential customers to find Panavision on the Internet. So long as the defendant held the Internet registrations, he curtailed, or diluted, Panavision's value of its trademarks on the Internet, and the court upheld the injunction against that use. The problem was that entities had to prove that their trademark value had been diluted under the FTDA, as well as that this action could be ineffective and costly, when all that they wanted was to get their domain name back. Some states' laws, in fact, were stronger than the FTDA. (Later, in *Moseley v. Secret Catalogue* (2003), the U.S. Supreme Court affirmed that actual harm must be proven before even FTDA injunctive relief can be obtained.)

In response, the United States passed its Anticybersquatting Consumer Protection Act, or ACPA, in late 1999. This act allows civil lawsuits to be brought for trademark and service mark violations against anyone, who with a "bad faith" intent to profit from a mark, registers, uses, or attempts to sell a domain name that's identical or confusingly similar to that protected mark. Factors indicating bad faith are whether the name owner actually diverted the trademark owner's customers, offered the registered name for sale without having used it, or registered multiple names. Under the Anticybersquatting Act, the courts can cancel a "pirated" domain name, assess attorney fees and costs, and levy penalties up to $100,000 against an infringer (depending on the level of bad faith and the actual damages). This act gave broad legal weapons for any mark holder to protect its trade or service mark, as well as more remedies and damages for any unauthorized use.

This legislation also made it illegal to register the name of any living person without that person's consent, while intending to profit by that action. Actors Brad Pitt and Kenny Rogers immediately filed suit on this provision alone, Kenny Rogers objecting to the "kennyrogers.com" registered to theWeb site of a California wedding service. Both celebrities, among others, retrieved their "names."

ICANN's Dispute Resolution Process ICANN instituted a procedure for resolving domain-name disputes. Under an agreement called the Uniform Domain-Name Dispute-Resolution Policy (UDRP), those with a dispute

over a registered domain name involving their trademark or service mark have the alternative to file a complaint with an ICANN-approved dispute-resolution service. Pursuant to these procedures, the service provides an arbitration panel that then rules which party has the legitimate right to that name, and if either party disagrees with the handed-down ruling, then that party can litigate the disputed matter further in court. The judge in the court case can review all of the facts and isn't necessarily bound by the review board's determination. Once a final decision is reached, the registrar then transfers the domain name as the court or administrative panel decided; for further details on this policy, see ICANN's site at http://www.icann.org.

Whether marks are registered or not, legitimate holders can take their case to different alternative dispute resolution centers under this process, and the United Nation's World Intellectual Property Organization (WIPO) hears most of these cases. (For more details, see its site at http://www.wipo.int/.) Basically, the claimant must prove (a) that the domain name very closely resembles a trademark registered or owned by that entity, (b) that the party that registered the domain name has no rights or legitimate interest in that name, and (c) that the domain name was registered and used for illicit purposes or in bad faith. This is an inexpensive process (a one-person panel for a case involving up to five domain names at the time of this publication costs the complainant $1,500, and a three-person panel costs $4,000); fast (the arbitrators' decision is normally rendered within 60 days); convenient (there is no hearing to attend; the arbitrator or panel reviews only the complaint, response, and supporting documents); and the decisions typically favor the trademark holder (some four-fifths of the determinations favor the mark owner).

The initial decisions on domain names reached conclusions in favor of companies with recognizable names, such as the World Wrestling Federation, Stella D'Oro Biscuits (a Nabisco affiliate), and Telstra (the Australian telecom company), ordering their domain names transferred back to them. WIPO arbitration panels handed back the Web addresses bearing the names of the Corinthians (Brazilian soccer team), Dan Marino, Julia Roberts, Kevin Spacey, Yahoo!, ESPN, and Wal-Mart. However, Sting, Bruce Springsteen, the Reverend Dr. Jerry Falwell, and Ted Turner failed to prove that their personal names had been used in a trademark sense as a label of particular goods or services and did not prevail in their UDRP proceedings. ICANN's dispute-resolution policy, however, does not apply to all registrars—it applies to the TLDs (top-level domains of ".com," ".net," ".biz," etc.) and not directly to the "ccTLDs" (individual country domains, such as ".cn" for China), unless that country agrees or has established its own dispute resolution board. A number of the ccTLDs have done so.

The Legal Weapon Trade-offs. Entities with U.S.-based domain name/trademark conflicts must decide between using the Anticybersquatting Act, an ICANN proceeding, or both. ICANN gives a fast resolution, whereas ACPA litigation can take up to 2 years or more for a decision. Although the federal statutory-authorized lawsuit allows for a preliminary injunction, the opportunity to be awarded good damages, and transfer back of the domain name (which is all that an ICANN-UDRP procedure can do), this alternative is highly expensive with much more downtime, complexity, and legal dollars required. The ACPA is a final determination, whereas the extent to which an ICANN decision can be litigated further is currently being determined.

The rest of the world is not as restrictive as the United States or other developed countries, and the game is still being played in some fashion. Countries in Asia, the former Soviet Union, Eastern Europe, and elsewhere have not yet tightened their laws, although over time, they likely will. It may still be possible in small nations such as Moldavia (until they change) for cybersquatters to purchase domain names that aren't already reserved, and the question of conflicting laws always seems to rear up when lawsuits are brought to challenge ICANN administrative rulings.

For international protection, entities need to register their mark with the U.S. Patent and Trademark Office (PTO), and U.S. concerns need to file that registration with the appropriate agency of the foreign countries in which they operate. Although the granting of a registration by the PTO is not conclusive on the issue of who owns a mark, it is prima facie evidence of that ownership (see the PTO at http://www.uspto.gov for the details). Given the estimated numbers of domain names (escalating from present numbers to more than 100 million in 2 years by various estimates), the number of permutations, and various country designations, the volumes of conflicts, arguments, and opportunities for these disputes can only increase over time.

Patent

Through patents, the United States by its Patent and Trademark Office grants an inventor the exclusive right to make, use, or sell an invention for 14 years (design patents) or 20 years (inventions). To obtain a patent, the inventor must meet certain requirements, such as novelty, usefulness, and nonobviousness. Computer hardware (i.e., the design of electronic components, handwriting recognition systems, and so on) is patentable, but software typically isn't brought into the process because of the time it takes for a patent to be granted and contrary regulations in a few cases.

The number of patent applications for Internet applications increased in recent years owing to court decisions (beginning with *State Street Bank v. Signature Financial Group*, 1998) upholding patents issued for Web site business processes and operating methods. Amazon.com (its "one-click" online purchasing system), Onsale (operating auctions), Cybersettle (its "double-blind bid" dispute resolution procedure), Priceline.com (conducting an online "reverse" auction), Microsoft (online shopping and merchandising), Sun Microsystems (Internet bill processing), Tumbleweed Communications (online greeting card delivery), E-Data Corporation (online selling to any point-of-sale location), and other e-commerce entities have received patents on their specific business or operational models. As expected, the court challenges from competitors over these patents have also increased, as competing entities battle over controlling important operational methods.

DEFAMATION

Cyberspace creates an inordinate ability to post defamatory comments quickly that injure another person's reputation and can be seen around the world. Those who post libelous comments, however, do not enjoy the anonymity in cyberspace that one might first expect. A cyber-defamation lawsuit is typically filed in the city where the chatroom provider or ISP is located and lists various "John Does" or "Jane Does." This is legal jargon for naming unknown parties to the lawsuit, whose actual names will be added later after discovering their true identities. The lawyer then files a subpoena (demanding that the desired information be released) against the provider to gain the identity of the particular John or Jane Doe who posted the inflammatory remarks.

Lawyers serve subpoenas daily on CompuServe, AOL, Yahoo!, Microsoft, and others to retrieve some poster's identity. If the ISP doesn't turn over the demanded information, the attorney then goes to court to ask the judge to force the ISP to divulge the required data. The judge balances the right to protect someone's anonymity versus the injured party's right to be protected from harm. The plaintiff, or injured party, usually must prove that there's no other way to obtain relief without securing this specific information. If multiple servers are involved, the attorneys will follow the e-mail address back through that chain with multiple subpoenas.

A doctor at the Emory University School of Medicine in Atlanta, Georgia, came across a posting on a Yahoo! message board. It falsely suggested that he had taken kickbacks from a urology company to give his department's pathology business to the company and had been forced to resign over this conflict of interest. The message was from "fbiinformant,"

who later was discovered to be a former employee at the urology company who disliked the doctor. In what was believed to be the first Internet defamation case to reach trial, a U.S. district court judge awarded $675,000 to that doctor, all because of this one "anonymous" Internet message (see *Graham v. Oppenheimer*, 2000). Litigating defamatory e-mails, postings, and communications continued on unabated from there.

As to the online service providers, the court decisions have consistently upheld that there is no liability on their part for defamatory postings made by third parties. The Communications Decency Act of 1996 (CDA) bars tort-based claims or lawsuits against ISPs for defamatory, obscene, or other objectionable postings, provided there is no complicity by the ISP with that third party over those postings or other unreasonable behavior (the provider also must "actively" remove the objectionable material). Although portions of the CDA were later held to be unconstitutional (see *Reno v. American Civil Liberties Union*, 1997), these provisions continued in their legal validity and effect.

PRIVACY CONCERNS

At this time, there is no general, sweeping U.S. law regulating or requiring entities to disclose how they use sensitive financial and other personal information gained from their customers or users, nor how they gather that data. Notwithstanding recent U.S. Federal Trade Commission (FTC) high-profile proceedings against companies over their information practices, the FTC has had, in effect, a "self-policing" policy, promoting industry self-regulation in the fields of data collection and customer profiling. Congress did enact legislation as to the online privacy protection of children, however, when it enacted the Children's Online Privacy Protection Act (COPPA) in 1998. This statute requires thatWeb sites "earmarked" for children, or who knowingly collect data on users under age 13, need to (a) obtain verifiable parental consent for any collection or use of their children's information (i.e., "no consent, no collection") and (b) on request, provide the parent with the ability to review any personal information that has been so collected. The FTC has issued administrative rules on COPPA to guide these "kiddie" Web sites on their compliance with this legislation (see http://www.ftc.gov for more on this subject). Additionally, the FTC has charged entities with violating COPPA and reached settlement with several of those Web sites.

Congress also passed the Gramm–Leach–Bliley Act (GLBA), known also as the Financial Services Modernization Act of 1999 and which applies to Internet transmissions and electronic data collection. This legislation basically requires that financial institutions (a) inform consumers of their

privacy policies and (b) notify consumers before acquiring, transferring, or selling their private data to third parties, giving them the opportunity to "opt out" of such data-transfer practices.

Additionally, various states have passed privacy legislation both in the financial area and in preserving the confidentiality of sensitive medical records, including diagnosis, treatment, and prognosis. As with most state laws, these acts are not uniform—for example, depending on the subject area, some states require opt-in conditions before data can be collected or used, whereas others establish opt-out standards. Rules have also been enacted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in this area (see the U.S. Dept. of Health and Human Services at http://www.os.dhhs.gov for more), and the court challenges on its implementation are under way.

The differences between the United States and other countries, such as Canada and the European Union (EU), couldn't be more pronounced than in the rights of privacy area. Canada's Personal Information Protection and Electronic Documents Act (S.C., 2000) implements a wide array of data protection, including a phase-in of "opt-in" provisions for its citizens. The EU's Data Protection Act came into effect in 1998, also using a completely different approach from that of the United States. Citizens there gained enhanced rights to prohibit their private data from being released, including requiring entities to secure "opt-in" permission in various situations before personal data can be acquired, sold, or shared. For further information, including on the "safe harbor" guidelines for U.S. companies with subsidiaries operating under the more stringent EU privacy laws, see the U.S. Department of Commerce Web site at http://www.commerce.gov.

CENSORSHIP

The First Amendment places strong limitations on the government's ability to censor, or unduly regulate, the rights to basic freedoms such as those of speech and expression, and the Internet is no exception. For example, Congress passed the Communications Decency Act of 1996 (CDA) which, among various provisions, essentially made it a crime for anyone to knowingly distribute obscene material for sale in cyberspace. Later in 1997, the U.S. Supreme Court in *Reno v. American Civil Liberties Union* declared that most of the important provisions of the CDA dealing with obscenity were unconstitutional, holding that these provisions were so vague as to be void on their face. The fact that statutes applied to cyberspace didn't mean the constitutional tests applied were any less strict, and later legal battles over

subsequent pornographic statutes have applied the same strict construction tests of the offline world.

For example, Congress in 1998 passed the Child Online Protection Act (COPA) as a successor to the struck-down CDA provisions in another attempt to stop children from gaining access to sexually explicit materials on the Internet. In 2002, the U.S. Supreme Court reviewed COPA and partially upheld it, adding further legal uncertainty. In *Ashcroft v. ACLU* (2002), the court ruled that the act's reliance on community standards to identify "material that is harmful to minors" did not by itself render the statute unconstitutional. The divided court kept alive the fight over whether the measure was unconstitutional, however, by affirming the appellate court's ban against COPA's enforcement, then returning the issue for further review on free-speech questions that the court felt had been left unresolved. Subsequently affirming the preliminary injunction on COPA's use, the U.S. Court of Appeals for the Third Circuit in its decision, *Ashcroft v. ACLU* (2003), then rejected the U.S. Supreme Court's reasoning, finding that the law was not the least restrictive way to achieve the government's interest in protecting children. This panel of circuit judges said that the law was "vague, overbroad, and puritanical" and violated the First Amendment. The Justice Department again appealed. The U.S. Supreme Court then agreed with the appellate court in *Ashcroft v. ACLU* (2004) that enforcement of COPA should be enjoined because the statute likely violates the First Amendment, and that employing filters a less restrictive way than COPA's mandated use of credit cards or other measures employed to restrict access. Yet, the Supreme Court remanded the case again to the lower court for consideration whether there are less restrictive ways to achieve the government's objectives. Whether in cyberspace or not, the complexities of First Amendment case law continue.

The U.S. Supreme Court in *United States et al. v. American Library Association* (2003) held by a 6–3 majority that Congress could require public libraries to install mandatory filters on Internet computers as a condition of receiving federal technology grants and "e-rate" discounts, upholding the constitutionality of the Children's Internet Protection Act (CIPA, 2000). The Supreme Court later declined to review the "Nuremberg Files" case, in which an 11-judge U.S. Court of Appeals panel voted 6–5 in *Planned Parenthood v. American Coalition of Life Activists* (2002) to uphold a 1999 trial verdict against an antiabortion Web site that disclosed the names, addresses, and family information of physicians who performed abortions. The trial jury awarded punitive damages of $107 million against the coalition of activists, but the appellate panel remanded the damage amount back to the trial court to determine whether the award was excessive or not.

In a case in which the judge described a dispute between the protection of trade secrets versus freedom of speech, a federal judge ruled a Web site operator could continue posting confidential Ford Motor Company documents on new car designs and other internal data (see *Ford Motor Co. v. Lane*, 1999). Lawsuits over employer Internet-use policies, however, provided the policies are reasonable with notice given to the employees, have generally been upheld in the employer's favor. An employer's use of Web filtering software (where worker e-mails are subject to scrutiny) also is under challenge, but most legal scholars believe that these challenges generally won't be sustained. Moreover, the courts so far have not been receptive to employee claims that work done on an employer's computer system is personal and entitled to constitutional protection. Please see the chapter on E-Mail and Internet Use Policies for more on this subject.

Courts have generally upheld the right of "suck.com" Web sites to criticize the operations of major businesses (e.g. http://www.ballysucks.net; see *Bally v. Faber*, 1998), although the complaining companies have had more luck in challenging these sites under ICANN domain name proceedings. For example, the Salvation Army filed an ICANN-UDRP proceeding over the name "salvationarmysucks.com," and the arbitrators ruled in favor of it, when evidence of offers to sell the name back to the Salvation Army came to light. Generally, provided the posted allegations are basically true or represent protectable opinion rather than false facts, the cases hold these expressions to be protected by the First Amendment. If you use a search engine with the descriptive word "suck.com" or type your favorite company name with a "suck.com" after it, watch the complaint Web sites surface that already are in existence.

Another growing First Amendment consideration involves its application in disputes where software sites collide with commercial trade interests. For example, the DVD Copy Control Association (DVDCCA) attempted to shut down Web sites, including that of California resident Andrew Bunner, which provided a link to DeCSS software code that unscrambled encrypted DVDs and allowed them to be played on unlicensed computers. A California Court of Appeals (*DVDCCA v. Bunner*, 2001) overturned the trial judge's temporary injunction against Bunner's site as an unconstitutional prior restraint protected by the First Amendment. In reversing the appellate court, however, the California Supreme Court (*DVDCCA v. Bunner*, 2003) decided that computer source code is a form of speech that can be constitutionally protected, but that this injunction was appropriate because it was not based on the content of Bunner's speech—it was only protecting the DVDCCA's trade secrets. The court sent the issue back to the appellate court for a ruling on whether the injunction was warranted under

the state's trade secret laws. The California Court of Appeal (*DVDCCA v. Bunner*, 2004) held that the facts did not support the injunction because the DeCSS software was so widely distributed before the injunction was requested.

CYBERFRAUD

Cyberfraud is a major problem on the Internet, owing to its anonymity, commercial reach, and speed in exchanging credit card data. Hackers abound, trying to exploit any weakness in a site's systems and database. The ease of entry onto the Internet makes it even easier for "fly by night" firms to race in, skim off money, and quickly disappear without leaving a trace. No matter where you live, the Web has indeed become global in when and how the unwary are fleeced. In the United States, the FTC is the federal agency charged with prohibiting unfair or deceptive commercial acts, including misleading advertising (fraudulent investments are handled by the Securities and Exchange Commission, or SEC). The FTC's rules and regulations against unfair or deceptive business practices specifically cover Internet transactions, and its Web site (http://www.ftc.gov) has pages with information about Internet fraud, complaints, and its fight against this problem.

The FTC has brought countless numbers of fraud and misleading advertising complaints to stop such unfair practices, both online and offline. In 2001, the FTC opened a Web site with statistics and information on primarily U.S. Internet fraud and identity theft. The site is called "Consumer Sentinel" (see http://www.consumer.gov/sentinel), and it started with a database of more than 300,000 complaints lodged with the FTC over the last several years. The site provides data on fraudulent transaction trends, as well as the ability to submit online complaints (as does the FTC with its Web site). From year to year, identity fraud is the overall top consumer fraud complaint from all sources received by the FTC and by a wide margin, followed by Internet auctions and Internet services/computer complaints. If you find online fraud problems involving different countries, then head to "econsumer" at http://www.econsumer.gov/, which has in place direct links to consumer fraud agencies in various countries and represents a coordinated world effort to work together on this global problem. This site also allows for the filing of international fraud complaints.

The Internet is an excellent tool both for investors with easy access to research sources, as well as for the shysters, hipsters, and con artists to get to the investors' and other people's money. Because anyone with a

computer and modem can reach tens of thousands of potential investors simply by creating an attractive Web site and spamming, the U.S. SEC has had to become active on the Internet. It established a national cyberforce of attorneys, accountants, and analysts specifically trained to watch out for fraudulent online security transactions (see http://www.sec.gov for more information, including its reported Internet fraud cases).

For example, one case involved a company that used spam e-mail to announce an initial public offering (nearly all of us have received junk e-mail of this type), stating that it had been approved by the SEC and would realize at least $1 billion in eyewear sales. In fact, it had never been approved by the SEC and didn't even own an office or inventory. The owner of the company used the "invested" money for restaurants (eating meals), casinos (gambling), and adult entertainment clubs. The investors lost everything that they had invested—the usual and unfortunate result with fraudulent investments, regardless of whether the FTC or SEC intervenes later.

Regardless of the state or country, the law is clear with regard to cyber-fraud: (a) any Web advertisement of illegal transactions under a particular country's or state's laws (e.g., gambling or usury) will be illegal there; (b) fraudulent, false, or materially misleading statements are illegal and unenforceable, no matter where you live; and (c) the regulatory agencies in different states and countries vary widely in their ability to crack down on misleading advertising, even when the customers or investors have lost all of their money. Remember: If the advertised "return" is too good to be true, then it usually is; and investors must be quite careful when reviewing potential investments of any kind, whether online or offline.

E-COMMERCE LAW

"Click" Contracts

Given the ease with which online contracts can be made, the tearing down of geographic barriers, and e-mail "proof" that lasts forever, basic contract law is even more important on the Net. From what is needed for a legitimate contract (i.e., mutual assent, consideration, capacity, and no legal defenses) to how duties are delegated and determining damages, all of the fundamental contract laws apply in cyberspace. (For an excellent discussion on this area, see *Cyberlaw, Text and Cases, Second Edition* by Ferrera, Lichtenstein, Reder, Bird, & Schiano, 2003.) As expected, e-contracts do have important aspects that stand out from offline contracts.

You can't discuss and then sign an e-contract with your handwritten name, as you can when you're in a face-to-face meeting with the other

party. In place of this "personal touch," the law basically allows that you can agree to the terms and conditions of an electronic agreement when you click the "I agree," "I'll buy," or "Subscribe" button. The mouse click on that agreement button sets the approval to the conditions of your e-contract.

The courts generally have upheld these "click" contracts as being as valid as if you signed a written agreement on the dotted line. (See, for example, *Crispi v. The Microsoft Network,* 1999, and *Geoff v. AOL, Inc.*, 1998.) Any on-screen click, no matter where it's located (but provided it's reasonably identified as the "click" agreement button), will do. The legal premise is that the medium in which a signature or contract is created shouldn't affect its validity, and the transaction is enforceable, whether that medium is paper or electronic. There are limitations on when click contracts will be enforced, however, and this is discussed later in this section.

E-Signatures, Taxation, and Spam

The U.S. government and nearly all of the states have enacted a version of an electronic signature statute. The federal act (Electronic Signature in Global and National Commerce Act, 2000) ensures that electronic records, signatures, and contracts have the same legal effect as their ink-and-paper counterparts (including that electronic records satisfy statutes mandating that records be kept in writing), validating online commerce and allowing for the eventual recordation of documents such as deeds, mortgages, and bills of sale by accepting digital notarization. Along with its state counterparts, this legislation mandates that an e-signature is enforceable if both parties agree to its technological format (whether signature verification is based on encryption software, smart cards, mouse-pad technology, or whatever), and it provides that a signature may not be denied legal effect simply because it is in electronic form. It is an enabling statute that sets down standards that can be followed and allows states to enact their own but generally consistent legislation within this umbrella, prohibiting laws that limit permissible electronic signatures to one single technology. The states differ widely in their authorizations because numbers are applicable to all electronic transactions, whereas others can be more limited in their scope and effect. Internationally, many countries (from Brazil and Taiwan to the individual members of the EU) have enacted e-signature and e-commerce laws, simply because it is in their best interests to do so.

In 1998, the United States' Internet Tax Freedom Act capped taxes on online sales with a 3-year moratorium on any *new* state, local, or

federal Internet taxes (as defined) to October 20, 2001; after an interim delay, the moratorium was extended for an additional 2-year period that then expired on November 1, 2003. It is a misnomer, however, that this statute generally ended Internet taxation. Among other allowed taxes (including "grandfathered" Internet taxes and taxes on Internet access) when the "moratorium" expired, 45 states charged sales tax on tangible products bought online, given that the seller had some form of a physical presence or "nexus" (i.e., a warehouse, retail store, office, or sales representatives) in that state—all as permitted under already existing tax law (see *National Bellas Hess v. State of Illinois*, 1976).

What was held in abeyance was the legal ability to tax an online purchase from a resident in a state where no such nexus or connection to the selling site's state was present. In late 2004, Congress finally approved the extension of these federal restrictions against taxing online sales transactions to November 1, 2007, and President Bush signed this legislation into law. Notwithstanding this, it is expected that the states and non-Internet merchants will continue to make the pleas to Congress to tax online sales as never before—and the lobbying will continue well past any further legislation that's enacted, whether the ban is made permanent or another short-term "moratorium" ensues.

As e-commerce expanded, huge increases in unwanted electronic solicitations (otherwise known as spam and junk e-mail) have also taken place. Given the Net's anonymity, enforcement difficulties, jurisdictional issues, and that more serious crimes are usually in line for prosecution, controlling spam legally will not be possible until the U.S. and the international community in general pass federal laws with strong enforcement mechanisms. Although the U.S. federal government passed an antispam bill, the CAN-SPAM Act of 2003, critics believe that this law doesn't go far enough. For example, there is no requirement of an "opt-in" provision, because the act allows e-marketers to continue spamming until the recipient responds with a required "opt-out" message (which also confirms that e-mail address). Further, this legislation legitimizes unsolicited e-mail as a marketing tool and is ineffective on those spammers who increasingly operate outside U.S. jurisdictional limits; this act also supersedes conflicting state antispamming laws that are stricter in cases. (Even given that nearly all U.S. states have enacted laws regulating spam, including fines and jail time as penalties, these laws are rarely enforced or difficult to enforce. In numbers of states, no one has yet been prosecuted under those statutes.) In contrast to the U.S.'s position, countries from Australia to the European Union have passed strict antispam laws with "opt-in" provisions and varying effective dates. For the latest on antispam legislation and developments, see http://www.spamlaws.com.

Although beyond the scope of this chapter, the global e-commerce legal aspects are considerable and ever changing; please see the treatment of these international areas throughout this treatise.

"Terms of Use" Provisions

Many Web sites separate out the necessary purchasing information from their legal Terms of Use and Privacy policies. Although the general areas treated are similar, each site's provisions are different, depending on whether a particular location sells products, provides services, gives information, or some combination. Nonetheless, the general concepts covered are basically the same.

Given that the basic contract business terms (e.g., quantity, price, time for delivery, delivery mode, and so on) are present, what was once "just legal boilerplate" has now become more important: disclaimers of liability, limitations of warranty, indemnity, handling of disputes, applicable law, and dispute resolution, among other areas—and this is especially true when distant localities become involved.

The disclaimer-of-liability provisions typically limit a seller's liability for injury or loss incurred by the buyer to exchanging the product or a refund of the purchase price, all at the seller's option. This refund policy is usually coupled with a disclaimer of liability, such as the following: "Seller disclaims all liabilities and warranties, express or implied, including the warranties of merchantability and fitness for a particular purpose, and this Web company shall not be liable for any damages, whether consequential or incidental."

The intent of these provisions is for the seller to "duck away" from liability, leaving the manufacturer on the hook. Although not unanimous in their decisions, the courts generally uphold limitations on consequential damages (for example, a site's loss of data that results in a further loss to its users or customers) in business transactions, and it is well-settled law that two contractual parties in commercial situations can negotiate at arm's length the extent to which either party's damages will be limited, given equal bargaining power (see *Robotic Vision Systems v. Cybo Systems, Inc.*, 1998). These provisions usually are not upheld if a personal injury is involved with an individual, however, such as when a customer is injured using a defective product that caused those injuries.

As a basic legal concept, no one can contract against the effects of strict product liability or one's own negligence, unless separately negotiated between two contracting businesses. If that were the case, then there could never be any product liability, because every manufacturer and retailer in the world would be contractually providing, "Sorry, if there's a problem with

our product, even if it's entirely our fault, we don't accept that liability—you do." Depending on the circumstances, Web sites can be held completely responsible for a customer's damages, notwithstanding these one-sided contract provisions. For example, if a pharmacy Web site erroneously fills a prescription for high blood pressure medication that severely worsens the problem, that Net retailer typically will have to compensate that injured person for his or her damages from those bad pills, regardless of any Terms of Use limitations to the contrary.

Standard Terms of Use agreements also provide for "tight" indemnity provisions (i.e., that the user is responsible for any damages), as well as favorable provisions on applicable law (typically the site's state law, if favorable), dispute location (the Web site's hometown and state), copyright use (i.e., one must gain their written consent to any copying), privacy policies, and the like. Although courts tend to uphold these one-sided provisions, sites cannot be totally unfair in them, nor limit what the law already allows. For example, the United States provides for a "fair use" exception for copyrights, and the courts will generally not allow any such one-sided, restrictive statements to erode this long-standing doctrine. Just because aWeb site operator says it's true doesn't necessarily make it legally so. However, any user must be aware that all Terms of Use provisions, including privacy policies, are agreements of legal significance and that it will take a successful court challenge to overturn their application. If possible with larger companies, it's better to negotiate out ahead of time the legal provisions, or boilerplate, that aren't in your favor.

Validity

Most courts uphold "take it or leave it," click e-agreements, provided (a) the terms are written in understandable English with readable print and not hidden from the user's view; (b) the user has the opportunity to read and understand these terms, all before having to make any purchase or use decision; (c) the provisions are reasonable; and (d) the user has to take some affirmative action to agree (such as clicking an "I agree" button). Because courts tend to enforce software shrink-wrap agreements (where the act of opening the software package is deemed to be acceptance of the included terms), they're doing the same with Web site Terms of Use "click" provisions, provided these elements are present.

If, however, the language used is hidden or not conspicuous, in small print, or wholly unreasonable in effect (e.g., "This Web site is not responsible for any of your damages, regardless of how much we are at fault"), then courts will generally not uphold them. There must be some knowledge (the

terms are easily located and understood), prior decision making (the user can decide before having to order), and facts showing at least mutual assent or an implied agreement (e.g., clicking on an icon to show your assent).

A leading Second U.S. Circuit Court of Appeals case, *Specht v. Netscape Communications Corp.* (2002), reviewed the standard terms and provisions applied when a user downloaded software. The standard terms provided that all provisions came into legal effect when any user simply downloaded or installed the software. However, users could directly download this software before coming or scrolling down to the "I agree" icon and any inspection of the terms of use that bound their decision. Applying standard contract law on mutuality of assent, the court upheld a lower court's decision and refused to enforce an arbitration clause in the Web site's forum state, holding that the required mutuality for contract assent was not present.

When the requisite criteria are present, courts will uphold these terms on a general, conceptual basis, provided additionally there is no blatant unreasonableness in those provisions. Based upon the Uniform Commercial Code's Section 2-302 (basic to most states' laws) that codifies the traditional common law doctrine of unconscionability, courts still have the ability to set aside those standard terms. The intentional misuse of a Web site by a user, however, can negate provisions that don't meet these standards. For example, in *Register.Com, Inc. v. Verio* (2000), a court held that when Internet users intentionally misuse a site's content, there is an implicit agreement to any terms of the Web site's legal notice that would prohibit that action.

A recent Northern California Federal District Court case, *Cairo v. Crossmedia Services* (2005), consistently applied both *Specht* and *Register* to a Web site's terms-of-use provisions that involved a forum-selection clause. Contrary to Crossmedia Services' (CMS) forum clause that required lawsuits to be filed in Illinois, plaintiff Cairo filed a declaratory relief action in California. The federal court found that Cairo's use of CMS's Web pages in allegedly copying promotional materials was such an "actual or imputed knowledge" of those terms as to effectively bind Cairo to the forum selection clause mandating Illinois as the proper venue. CMS's motion to dismiss was granted.

INFORMATION SECURITY LEGAL LIABILITIES

Whether owing to electrical brownouts, software errors, or hacker interference, systems crash every minute with loss of data, inoperable equipment, and frozen software. Along with the reported cases, there are general rules of

law that apply in deciding how and where liability for damages will reside. Basically, liability sits with the computer software and hardware manufacturers for their products' "inability to perform as promised," along with a growing Web operator liability when users lose data or incur damages—but along distinct legal lines.

Computer Software and Hardware Manufacturer Liabilities

The great majority of cases involving computer software or hardware defects are brought usually on contract, breach of warranty, fraud, and recession grounds, not on general tort grounds such as negligence or strict liability theories. As basic law, courts apply contract law to contract situations such as the purchase of computer software, errors, and breach of warranty problems, with tort law applied to noncontract situations (see, for example, *Grynberg v. Agri Tech, Inc.*, 2000).

Owing to an apparent general acquiescence of system malfunctions, vendor responses in solving their users' problems, insurance coverage, continuing technological improvements, responsive security safeguards (i.e., stronger firewalls, backing-up data, internal security procedures, etc.), and limitation of damage clauses, only a tiny fraction of security-related problems come to court, and then most settle before trial. Two issues are common in these contractual disputes (and see the earlier discussion on "Terms of Use" and "Validity"): (a) Whether shrink-wrap (physically opening the plastic wrapping of a software box) or clickwrap (digital clicking on an Internet "I Agree" icon) acts are present, was there a valid contract entered into that included the standard Terms of Use provisions? (b) If so, was there a legally enforceable disclaimer of liabilities and/or damages?

Various courts have concluded that shrink-wrap and clickwrap licenses are a valid form of contracting, that a vendor may propose a contract of sale be formed, not in the store or over the phone, but after the customer has had a chance to inspect both the item and the terms in the box (or after "clicking" an "I Agree" button) as to standard, unchangeable terms. For example, see *ProCD, Inc. v. Zeidenberg* (1996); *Brower v. Gateway 2000, Inc*. (1998); *Mortenson Co. Inc. v. Timberline Software Corp*. (2000); *i.LAN Systems v. NetScout Service Level Corp*. (2002). Basically, if a shrink-wrap license agreement is enforceable with implicit contractual assent, then it is also correct to enforce a clickwrap agreement on the Internet.

Typically, these agreements contain limitation on liabilities, such as limiting any damages to a refund of the software price (or replacement of the hardware within a certain period) with no compensation for any out-of-pocket losses or ensuing damages. As mentioned in the previous section

on e-commerce Terms of Use provisions, exclusionary clauses in purely commercial transactions—especially where the parties are of equal bargaining power and specifically negotiate their contractual terms—are generally upheld.

For example, in *Mortenson v. Timberline,* plaintiff Mortenson purchased a bid-analysis software package from defendant Timberline. After Mortenson used the software to prepare a bid that erroneously turned out to be nearly $2 million less than it should have been, Mortenson sued on breach of warranty grounds. The Washington Supreme Court affirmed the lower courts' holding that the limitation of damages contained in the vendor's shrink-wrap package was valid. Mortenson was limited to a refund of the cost of the software with no provision for the much larger damages it had incurred due to that software error.

Other courts, however, have gone in different directions on this issue. In *Amsan LLC v. Prophet 21 Inc.* (2001), for example, a federal judge in Pennsylvania ruled that the software licensee could avoid the limitation-of-liability clause in its license agreement and pursue its remedies under the UCC, holding that because the warranty had failed in its essential purpose, the limitation clause had to also fail.

Except for the outstanding issue of these limiting provisions, however, it is clear there can be contractual liability if a software manufacturer warrants to anyone that its product will specifically perform in some way (i.e., "calculate mortgage payments to the penny") and doesn't. When a system crashes owing to no fault of the software provider (i.e., a hacker cracks through the site) at this time, the great majority of users generally seem to accept their fate. However, when an employee is responsible for that loss of data or security problem, the liability issues are clear.

Security-Related Liabilities (Employee)

Liability against others for security-related breaches and damages is dependent mainly on whether an employee or outside third party is responsible for creating the security breach. Employee-created liabilities, even if the intentional act or tort of that employee, creates liability for his or her employer based on common-law liability standards—regardless of whether the Internet, information security, or online operations are involved. Under the doctrine of respondeat superior, an employer is held accountable for the damages created by its employee, provided that employee was operating at the time within the scope of the employment relationship.

When an intentional tort is involved, as opposed to just being negligent or at fault, liability is still found on various grounds, including that the

particular employee's acts would have normally been furthering the employer's business or was within their job responsibilities—even given that the intentional act would not have been condoned by the employer (see also Bick, 2003). Employees can create this vicarious liability for their employers, whether it's hacking into confidential databanks, disabling protective software programs, or sending sexually harassing e-mail messages. In fact, as Continental Airlines found in *Blakey v. Continental Airlines* (2000), businesses have liability for the individual online harassing acts of their employees; in this case, other pilots posted sufficient harassing gender-based messages on the pilots' bulletin board (and only accessible by them) that the court found the employer liable for a hostile work environment.

When hackers and viruses unexpectedly show up, however, whether it's cracking passwords, exploiting software design flaws, or coordinating attacks on target computers and Web sites, the issue becomes expectedly more complicated.

Hackers, Crackers, and Viruses

Several large Web sites, such as Yahoo!, Amazon.com, eBay, CNN, and Dell, in February 2000 were severely disrupted by distributed denial-of-service (DDoS) attacks. Later estimates of the lost business, data, and operational downtime ranged from $1.2 to $1.7 billion dollars. A 15-year-old teenager (known online as "Mafiaboy") living with his parents in Montreal, Canada, was responsible for the attacks. Despite the large-scale damages, Mafiaboy (Canadian law protects the anonymity of juveniles) received a sentence of 8 months in juvenile detention and a $250 fine to charity. If a teenager could do this, think what a dedicated hacker might be able to do. Or an experienced cracker on subscriber passwords.

Just 3 months later, the "I Love You" virus infected 45 million computers around the world. This hacker virus embedded itself in a computer's system files, causing system crashes and freezing, then ordered the "host" computer to forward an infected electronic mail attachment to all addressees in the user's e-mail address book. Depending on the estimate—and including nearly 30 copycat viruses that came into being in the next weeks, the "I Love You" virus cost between $6 and $10 billion in lost productivity. There were no reported major U.S. cases decided regarding these security-related breaches, although claims and litigation with insurers over their coverage occurred.

Newspapers still report all too frequently the disruption caused by worldwide Internet attacks by hackers on computers and, given its market domination, on Microsoft operating systems in the main, such as the 2003

"LovSan" virus. Given massive losses of data, or stolen identities, the question becomes just who is legally responsible for these problems—the software manufacturer(s), their Web site operator-customers, or the individual site users—and to what extent.

Clearly, hackers are subject to a variety of criminal and civil law sanctions (see generally Jacobson & Greene, 2002). Yet as seen so clearly in the Mafiaboy case, hackers—if they can be located at all—don't have the money to pay for damages. The problem escalates when the virus or attack is terrorist inspired, and it will be years before any final court decisions are handed down on the myriad legal questions inherent in the September 11, 2001, tragedy (i.e., the extent to which the victim, such as the airlines, can be held liable for the intentional and criminal acts by others).

Regardless of cause, Web site operators work hard to recreate lost data and mitigate damage to their users—or risk losing their customers. When users can't access a particular site or lose data, compensation is rarely given, however, and it isn't cost-effective in the great majority of cases to litigate over limiting damage provisions. In high damage cases, users look toward the software manufacturer or Web operator (or both) with insurance coverage on both sides playing a dominant role (see also the next section, "Insurance Law"). The tendency by all players is to "downplay" any system malfunctions, reporting little, if anything, to the authorities or their users, preferring to negotiate with their vendors over any business losses or with their insurance carriers.

However, lack of information-security practices, record-retention policies, or backup procedures can create numerous headaches with state and federal regulatory agencies (see generally Bick, 2001). For example, the SEC penalizes organizations that it deems not to be in compliance with its record-keeping directives. In 2003, the SEC announced in a settlement agreement that it had fined five large, reputable businesses with broker-dealer operations—Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray—a total of $8.25 million ($1.65 million each) for failing to have in place adequate procedures to retain e-mails and keep them accessible, all in violation of record-keeping procedures (*Deutsche Bank,* 2002). Not having generally reasonable procedures for storing data, backup systems, or online and offline storage facilities can create problems when in litigation; courts are not accepting of excuses when discovery requests are thwarted by lack of data, and this violation can lose you a lawsuit (Buford, 2003). Further, state professional ethics bodies can and will intervene if, for example, a law firm or physicians group doesn't adequately protect its electronic records with backup files.

To What Extent Is the Victim Liable?

The question then becomes to what extent is the victim liable to its own customers? Generally speaking, an organization or individual is not liable to its customers for the unanticipated, independent tort of a third party. Presently, Web sites and their users seem to generally accept their losses from hackers and viruses, whether the software manufacturer could have anticipated the rogue programming or not—even when a protecting software patch against the computer virus was available and the site operator didn't quite get around to employing it.

Legal experts maintain (for example, see Pinkney, 2002, and de Villiers, 2003) that common-law negligence and strict-liability grounds should be available, whether a patch was actually in existence or not. The theory of negligence involves proving four separate elements: a duty to a third party, the breach of that duty, proximate cause (or some "connection" or foreseeability between the breach and any ensuing damages), and damages that occur. Strict product liability is where liability is basically imposed regardless of fault on any merchant who introduces into commerce a good or product that is "unreasonably dangerous" when in a "defective condition." To the extent that the software manufacturer and Web operator are not completely at fault, an offset to any user damages could be available. In both cases, end users can be compensated to the extent that any resulting losses are not their fault. By applying a standard of reasonableness or not being "unreasonably dangerous" with strict product liability, this line of reasoning implies that there is a duty or standard on the part of Web operators and the software and hardware manufacturers to create "information-secure" sites.

Victims of a computer virus infection, consequently, under current negligence theory and these arguments can sue the providers, distributors, and operators of infected software for their damages. Proof of specific negligence can be straightforward when the circumstances involve a familiar virus strain that could have been cost-effectively prevented. In cases involving complex and novel strains, however, these evidentiary standards may not be available and such direct proof not exist. Even in these cases, circumstantial evidence based on the doctrine of *res ipsa loquitur* (and see further, de Villiers, 2003) can be used to prove one's case. (The theory of res ipsa loquitur, or "the thing speaks for itself," allows an inference of negligence based on the mere occurrence of an accident and its surrounding circumstances, not requiring the proof of specific negligence.) Another de Villiers' article (de Villiers, 2004) analyzes the use of a negligence cause of action in the inadvertent transmission of a computer virus and discusses these liability parameters within a virus infection context.

The same line of reasoning can be applied in hacker attacks that involve multiple computers. When DDoS attacks take place, the hacker typically has accessed a "master" computer that enslaves multiple numbers of other "zombie" computers in marshalling their systems to act in concert and flood the target system with massive amounts of e-mails, requests, and traffic in an attempt to cause that system to crash or deny service to legitimate users. If a patch is available to protect these computers from being so enslaved, then using a negligence or strict liability standard can conceivably bring even these outside systems into the sphere of liability (Radin, 2001, 2002).

To do this, the courts will need to carve an exception to the general rule that disappointed expectations and economic damages (i.e., lost business profits, customers, and personnel downtime) under a "sour" contract are not recoverable, as well as the application of limiting Terms of Use liability and damage provisions, because negligence or strict product liability concepts in the great number of cases are not applied to these factual situations that don't involve tortuous physical harm to persons or property (see *Springfield Hydroelectric Company v. Copp*, 2001; *Gus' Catering, Inc. v. Menusoft Systems*, 2000).

When basic contract law and the UCC are applied instead of torts or strict liability, as we have seen, there is a much higher likelihood that limitation-of-liability and damage clauses will be upheld. In tort actions, courts go the other way and generally disregard these limitations (i.e., those providing that any damages are limited to just a refund of the product's purchase price), holding that as a general policy individuals and organizations should not be allowed to contract against their own negligence.

Contractually, larger companies and entities with greater bargaining power negotiate with their software providers to insert protective language into their licenses in place of these limiting damage provisions. For example, their contracts may directly provide that the software companies are liable for any costs of security breaches and hacker attacks that exploit software weaknesses (i.e., the costs of data replacement, cleanup, and lost business). If the software provider wants the business, then it may very well accept this different language.

Smaller users are typically protected if a hacker or thief steals a credit card number and uses this to charge for goods, whether online or offline: The customer is protected under current law for losses exceeding $50, provided he or she doesn't unreasonably delay in their notification of the credit card company after learning of the loss. In response, MasterCard, Visa, and American Express, among others, are understandably working with their banks and merchants to increase online information security with time lines to institute safeguards or else the participating institutions bear the cost of any charge-backs for purchases made from stolen credit cards and identities.

As leading court decisions are awaited, state agencies and legislatures are beginning to make the first inroads. In 2003, the New York attorney general's office cited Ziff Davis ("ZD"), the New York–based print and online publisher of computer magazines such as *PCWeek,* for failing to provide reasonable computer security standards. In an offering of free limited subscriptions to a computer gaming magazine, ZD and its Web host failed to take precautions to protect consumer data, including leaving unencrypted subscriber data in the open on a publicly accessible server with no authentication controls. Hackers immediately gained access to the subscriber list, soon gaining the credit card information of 50 holders and posting the names and e-mail addresses of some 12,000 of its readers. Ziff Davis agreed to pay a $100,000 fine to the states of New York, California, and Vermont, along with $500 to each of the 50 subscribers whose credit card information was so accessed. Additionally, the settlement agreement provided that ZD would store data on protected servers, encrypt data in protected files, and use automated security tools (i.e., firewalls and intrusion detection systems), in addition to undertaking other safeguards. Organizations that fail to implement reasonable security systems and procedures are at risk for similar governmental action should a hacker break in.

Additionally, companies risk needing to call in the Federal Bureau of Investigation (FBI) or Justice Department under the Homeland Security Act (2002) if a hacker intrudes into sensitive information. For example, Data Processors International (DPI) is a U.S. firm that processes credit card information for Visa, MasterCard, American Express, and Discover. To its chagrin, DPI discovered that a hacker in February 2003 had accessed some 8 million credit card numbers. DPI called in the FBI to conduct a criminal investigation.

On July 1, 2003, California became the first state to pass a database privacy and antihacker act. This legislation requires that state agencies and companies with databases must notify their California customers when user personal information is illegally accessed from that computer network (California Legislative Service, 2002). If they don't so notify their users or customers quickly and without unreasonable delay, then the company assumes the damages incurred by its users. Californians can bring civil actions for damages and injunctive relief. The law is intended to help consumers protect against identity theft by requiring businesses, wherever located, to disclose quickly any breach in their security system of personal information that is not encrypted. At this time, there is no comparable federal law. Unlike the California law, however, the federal U.S. Homeland Security Act makes the disclosure of these breaches voluntary.

The present lack of statutory and court direction will change, however, when a massive hacker attack involves a nuclear power plant, worldwide identity thefts, airline controller traffic, or some terrible act of injury. The resulting damage and noninsured liabilities will create an unfortunate climate mandating the standards as to who will pay for those liabilities and under what circumstances. Courts then will hand down decisions on negligence, strict liability, and the comparative negligence parameters. Legislatures will be forced to get down to business.

INSURANCE LAW

With the technological sophistication of rogue programmers, the risks of operating on the Internet can be substantial. Whether hackers or employees destroy data systems, intercept stored or transmitted personal information (identity loss), commit computer fraud, or order DDoS attacks, there are multiple risks of data loss and damages. Where a loss is uninsured, the risks increase that affected sites will need to compensate, one way or another, a large user's losses or accept that loss of business or even a lawsuit. A critical issue is whether Internet insurance risk coverage is present, and several basic considerations need to be analyzed first.

Unless a special rider or policy is purchased, the typical homeowner's policy does *not* cover an individual's losses for loss of data or other Internet damages, although it will generally cover the destruction of that computer. If you're running a business, then your personal insurance policies (whether fire, homeowner's, or car) in nearly all cases will not insure against loss when you're conducting your business operations—whether your activities are online or offline. You will need business or commercial insurance generally for such commercial protection.

Two basic insurance areas for any business are first-party property coverage (i.e., insuring your buildings and personal property against loss) and third-party liability coverage (i.e., lawsuits brought by third parties against you due to your operations). A separate commercial general liability (CGL) insurance policy typically covers third-party customer or user claims. CGL, excess liability, and other liability policies protect the policyholder against liability, including outside claims of "property damage" or "physical damage to the tangible property of others" from your acts.

Pre-cyberspace, the notion of "direct physical loss" was easy to recognize because this involved specific identified risks such as fire, slip-and-fall incident, or an automobile accident. The legal question was whether a given policy covered the submitted asset loss or third-party liability claim. The problem then came about when these decades-defined incidents under

standard policy provisions now involved the loss of electronic data as the Internet Age created new forms of loss. The question was just how "physical" were these intangible, millions of bits of information.

Insurance companies understandably took the position that their standard commercial CGL, E & O (errors and omissions), BPP (business owner's package policy), and other policies did not cover most Internet risks, arguing generally that loss of access, data, and the use of information systems was not the equivalent of a direct physical loss. Although the majority of cases held that these pre-Net policies did *not* cover electronic data losses from hacker attacks or crashed sites (see *Lucker Manufacturing v. Home Insurance Co.*, 1994), a few courts have taken a broad policy look at the issue and held for the insured (see *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, 2000). In *Ingram Micro*, an Arizona federal district court made a basic policy decision that coverage "must exist" for these types of losses in light of the realities of the modern Internet world.

In very specific areas other than loss of data, standard umbrella and CGL insurance policies can provide some small Internet insurance coverage—but discuss these provisions with your insurance agent or manager in detail. For example, claims stemming from a policyholder's online advertising activities that, in turn, involve defamation, libel, slander, violation of privacy rights, or copyright infringement can generally be covered (provided the insurer didn't change that language later). CGL policies also generally provide coverage for the "oral or written publication of material that slanders or libels a person or organization (including product disparagement)," including the "publication of material that violates a person's privacy." Although some professionals recommend that businesses review their CGL policy for such coverage or negotiate with their insurer, legal experts believe that the better approach is to purchase specific Internet policies (i.e., media Internet operations)—and to be sure there is stated, definite coverage for your particular Net operations and risks.

Insurance companies then developed specific Internet data loss and third-party liability policies specifically covering the risks of loss from hackers, computer viruses, employee hacking, and much of the Internet privacy and intellectual property claims that clearly were not covered under traditional CGL, E & O, excess liability, and other pre-Internet policies. Supplemental e-commerce first-party property policies now can cover loss of electronic data, while digital error and omission policies can protect an insured from liability in defined areas, such as the above-mentioned advertising/personal liability, electronic data transmission, security lapses, and even copyright infringement (see, for example, Savetz, 2002). Web operators anticipating losses from Internet security problems can consider insurance coverage from

their inland marine policies, fidelity policies, computer crime policies, and any other ones that have specific insurance coverage for these anticipated claims (see generally Gold, 2002). That's the good news.

The bad news is that insurance companies already are eliminating the provisions in their CGL policies that could infer coverage (such as in the advertising and privacy areas) that withstood court scrutiny and are tightening up sections to exclude Internet operations specifically. With the advent of worldwide virus attacks, such as the "Code Red" worm (an estimated $2 billion in damages in 2001) and "Slammer" worm (some $1 billion in lost global productivity in 2003), various insurance companies have raised premiums for Internet coverage or simply excluded certain Net coverage, such as that caused by computer viruses. Where reasonable coverage is possible, insurance companies are requiring that companies take strong preventive loss measures (i.e., strong firewalls, frequent backing-up of data, use of encryption, smart cards, electronic keys, and data restoration equipment plus procedures to secure their online systems), along with requiring stand-alone hacker policies—or go unprotected. The horrors of September 11 further compounded the question with the specter of terrorists unleashing viruses and the need for vulnerable industries to implement security procedures plus acquire adequate insurance to cover these risks (if affordable).

The bottom line is that it's a much better idea to discuss what Internet and security coverage is possible and at what cost with your insurance agent or risk manager before you incur an online loss. Read the policy provisions closely and, if possible, obtain a letter from your insurer that specifically outlines your coverage. Litigating against your insurance company and agent over a denied claim—especially when that includes your customer's or user's complaints against you—is not a good alternative. You may be better off paying the higher premiums of specific Internet loss coverage or knowing, alternatively, that you are "self-insured": the euphemism that in return for not paying premiums, you know you're absorbing all of your and your users' losses.

THE CLASH OF LAWS

Given the numbers of cyberlaw conflicts, a key issue is whether a court in the plaintiff's geographical area can hear and decide the case. Simply put, if the problem is big enough, you want your understandable laws to apply, to eat and sleep in your own home, to work in your office when not in court, and to not have to hire an expensive attorney in a different state or foreign country. People involved in a court case don't want jetlag, bad food, unfamiliar surroundings, a strange language, and being away from

their family for weeks on end, which is why jurisdiction and conflicts of law are such a large cyberlaw issue.

Jurisdiction over a nonresident Web site or Internet transaction in the United States is normally based on a local state's long-arm statute. These laws provide that a state can assert jurisdiction over a nonresident defendant who commits a tort, transacts business, or has some connection with that state. When a state court asserts jurisdiction over a particular controversy to render a binding decision, for the most part it will also be constitutionally permitted to apply its laws, given sufficient connections with that dispute. (Federal courts apply the appropriate state substantive law when relevant to their decisions.)

The U.S. Supreme Court's landmark *International Shoe Company v. Washington State* (1945) decision established the law in this area. For a court to have proper jurisdiction, defendants must have purposely availed themselves of the privilege of doing business in that particular state (i.e., traveling through, selling there, advertising in, or other contacts in that state), and these "minimum contacts" must meet sufficient levels of due process so as not to offend our "traditional concepts of fair play and substantial justice."

For example, if a Wyoming rancher died and willed his ranch to his Wyoming son, it would offend our sense of "fair play" if a second son, who happened to live in Alabama, could sue and haul that Wyoming brother into an Alabama court. There are no connections with Alabama to this case, so the only court with jurisdiction should be Wyoming—and that court would apply Wyoming law (the property is there, the decedent and his heir lived in the state, the will was probated there, and so on).

When it comes to jurisdiction on the Net, U.S. courts generally look at a Web site's level of Internet activity, drawing distinctions between passive and active locations—and this distinction will be drawn more in foreign courts, although it is not a trend overseas. Called the "Zippo sliding scale," this test was set down in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.* (1997).

At one end of the spectrum, Web sites that enter into contracts with out-of-state residents involving repeated contacts, e-mails or other correspondence, and selling appreciable amounts of products or services into that state are held to be "active" Web sites. These active sites can be sued in the state of their customers, or in those of out-of-state residents, as various U.S. cases have held. Given the existence of these sufficient contacts, a local court could (depending on the facts) disregard a contrary Terms of Use condition of the Web site that provided it could only be sued in its home state.

On the other side of the equation, sites that only advertise or post information about their business on the Internet—not taking any orders or

conducting business through that Net site—are held to be "passive" Web sites. These Internet "informational" sites generally cannot be sued out of state and dragged from their home base into foreign courts, simply because they maintain a virtual presence. To hold differently would be to subject Net operators to being sued anywhere in the world that allowed an Internet connection to be made.

In between are Net sites that provide more connections between their state and out-of-state customers—and it usually takes more than having an e-mail capability and a toll-free number to confer that jurisdiction. With these same facts, e-mailing questions about a potential purchase (without more) doesn't suffice either, although some courts view this as borderline and "getting very close." If a defendant Web site displays a downloadable mail-in order form, toll-free telephone number, and e-mail address but no orders are ever made there, then these facts are not normally good enough. Given a finding that a passive site was involved, the upset user then must travel to the Web site's home state to sue. As indicated, a factual decision needs to be made in each case as to whether these minimum connections for due process reasons are present.

Some courts have developed an "effects"-based approach exception to the Zippo sliding scale. When using this approach, the court focuses its analysis on the actual effect that a Net site had in its state or the defendant's intent, not on how interactive the Internet location was. This test derives from the U.S. Supreme Court's *Calder v. Jones* (1984) decision, in which jurisdiction was found over a nonresident defendant newspaper, based on its intentional conduct outside the forum state that was deemed to cause defamatory injury to the plaintiff resident in that state—even though strong factual connections weren't otherwise present. Although courts tend to apply the "effects" test in cases involving intentional torts, such as defamation or trademark infringement cases, they do differ on what conduct constitutes the kind of "express" aiming or effect that's required to satisfy the test. Applying the "effects" test can find jurisdiction when there aren't sufficient contacts of the type called for under the Zippo sliding scale.

In a closely followed case, the California Supreme Court in *Pavlovich v. Superior Court* (2002) overruled a court of appeals decision involving the application of the effects test. Pavlovich had posted his programming adaptation of DeCSS software, a technology allowing the scrambling system in DVDs to be rendered ineffective and their contents copied. The appellate court held that California had jurisdiction over Pavlovich, a Texas resident but who was an engineering student at Purdue University in Indiana at the time. Although the defendant's actions didn't come close to meeting the Zippo test, the appeals court held that because there was an "effect" in

California from Pavlovich's "intentional tortuous" actions, California had jurisdiction, could apply its long-arm statute, and force the defendant to come there and defend himself. The California Supreme Court, however, reversed this decision on a 4–3 vote. It held that under the Zippo test, the Web site was merely an informational one and there was no evidence that the defendant had expressly hurled his activities at California. It ruled that a defendant's knowledge or foreseeability alone of harmful effects ensuing in a specific state (California) is not sufficient by itself to establish any "purposeful availment" of that state's law under the effects test. There must be more than that.

As can be seen, these can be complicated cases, whether the issue involves e-commerce differences, sales tax assessments, or defamation cases. Further, not only can a business (or wrongdoer) be a resident of one state, or even offshore from the United States, his server may be located physically in a different state, the connecting routers in others, and the end user or complaining party in another completely different one.

Keep in mind that the U.S. Supreme Court hasn't yet ruled on this area of virtual personal jurisdiction, nor what happens when a Web site's Terms of Use provisions are different from the reviewing court's laws—and courts, domestic and foreign alike, can and do give "wild" judgments that don't seem to meet any tests or analysis. For example, Australia's highest court ruled in *Dow Jones v. Gutnick* (2002) that a publisher could be sued for defamation in whatever country an individual's reputation has allegedly been harmed. This case arose when an Australian businessman, Joseph Gutnick, sued U.S.-based Dow Jones & Co. for comments made about him in an article posted on the Internet in *Barron's Online*. This court found that because damage to the plaintiff's reputation had occurred in Victoria where the article was downloaded and read, it was appropriate for Gutnick to seek damages in that Australian forum. If other countries follow the Gutnick decision, let's say Canada, then it is entirely likely that if a defamatory digital publication is read in Canada, there can be a sufficient nexus to maintain a defamation action in Canada, regardless that the publisher and server of that entity is located entirely in the United States—not an appealing legal proposition for that publisher.

Because laws vary greatly from country to country, what's prohibited by one nation can be entirely permissible in another. Unless an international treaty governs (e.g., the United Nations' Contracts for the International Sale of Goods [CISG]), countries are free to apply their own, quite different laws. The court that feels it has the greatest "connections," or the greatest interest in protecting its citizens, can and will take charge. It is quite possible that the courts in two countries could reach two entirely different

results—and this has happened numbers of times. The basic question then is the extent to which the laws of one country may be enforced against Web sites and hosts located in others.

As one example, a French judge ordered U.S.-based portal Yahoo! to block Web surfers in France from an auction where Nazi memorabilia were sold, including a fine of 100,000 francs (U.S. $13,700) for every day of noncompliance. Although Yahoo!'s offering sales of Nazi items was legally protected in the United States under the U.S. Constitution, it voluntarily banned the sale of these items in response. Arguing that the French court had no jurisdiction over it, however, Yahoo! quickly countersued in a California Federal District Court to overturn that decision's effect in the United States.

In late 2001, the U.S. court ruled that Yahoo! didn't have to comply with the French court's order (*Yahoo! v. La Ligue Contre le Racisme et L'Antisemitisme*, 2001). It held that a U.S. court cannot enforce a foreign order that violates the U.S. Constitution by "chilling protected speech that occurs simultaneously within our borders." Thus, the U.S. court held that Yahoo! didn't have to comply with all the laws in other countries that conflicted with those of the United States. French civil rights groups appealed this decision to the Ninth Circuit Court of Appeals. (In 2003, a French court acquitted Yahoo! of criminal charges that it had violated French criminal law by previously allowing the online sale of Nazi memorabilia from its U.S. Web servers.)

The appellate court in the United States, however, reversed the District Court's order (*Yahoo! v. La Ligue Contre le Racisme et L'Antisemitisme*, 2004), concluding that there was no basis for general jurisdiction in this case because the French groups did not have the continuous and systematic contacts with the forum state to support a finding of general personal jurisdiction. A key issue was that the French groups had never tried to collect on their judgment. Instead, Yahoo! had filed a preemptive lawsuit against the groups, and in a split 2–1 decision the majority didn't reach the First Amendment issue, holding that Yahoo! would have to wait on that question until the French litigants came to the United States to enforce their judgment. The Ninth Circuit Court of Appeals then decided to rehear the case "en banc" (the full court), but whatever its final decision, an appeal to the U.S. Supreme Court is expected.

The problem is not simple: Given other countries entering this fray, which court is right, when, and under or with what final authority? Because no international Supreme Court exists to adjudicate private disputes, there is no real way to settle this problem unless the parties later agree to those procedures. If the parties had negotiated the applicable law and forum before that dispute arose, then that agreement would control.

Fundamental differences among the various countries abound that affect basic principles, whether it's the United States and its First Amendment or EU countries with their basic consumer privacy protections. France mandates the use of the French language for numbers of documents in that country, whereas the EU and Japan have enacted strong antispam laws. Germany provides for a 2-week right of recession on online purchases, the U.S. to the contrary in this situation as well.

One way to solve these questions is for countries to pass an international jurisdiction treaty that binds the signatory states. The Hague Conference on Private International Law with over 60 member countries presently has established the "Hague Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Cases." (For more on the Hague Convention and its jurisdictional efforts, see its Web site at http://www.hcch.net.) The Hague's jurisdictional treaty legislation is in the works but will take years to finalize—and this state of affairs is the reason why alternative dispute resolution is growing in e-importance.

CYBERLAW DISPUTE RESOLUTION

One cyberlaw fact of life stands out: Resolving disputes arising from the Internet's global reach through litigation is complex, expensive, and loaded with unclear results. In response, the Net community is actively pursuing alternative dispute resolution techniques (ADRs) such as mediation and arbitration—both offline and online. Given their low cost, confidentiality, limited negativity, and speed in resolving cyberdisputes, the use of ADRs is accelerating among users.

Web sites and online operators actively promote ADRs in their agreements and Terms of Use provisions. ADRs have been used to settle all types of Internet disputes, whether between Web partners, competing sites, domain name holders, ISPs and their subscribers, copyright holders and copiers, and many other Net matters. Credit card companies use an ADR form when they use "charge-backs" to end a customer's complaint with an online seller. As discussed before, ICANN has established a worldwide arbitration procedure to resolve domain name "cybersquatting" disputes. The U.S. Digital Copyright Act basically provides for an administrative procedure in resolving copyright disputes.

One of the striking ADR advances has been the rise of online cybermediators who work primarily online. For example, one party contacts the cybermediator about the problem and the parties' inability to solve it; the mediator then contacts the second party. If both parties agree to use a

mediated approach and accept the ground rules, the online mediation begins. Typically, each party e-mails the mediator with his or her position or an acceptable settlement amount. The mediator then intercedes, shuttling back and forth electronically to reach a settlement. Although the experience has been that not having an actual presence between the mediator and parties (i.e., not experiencing body language and "real-time" emotions with words having a stronger unanticipated impact when made by e-mail) can be a drawback of online mediation, the 24/7 availability at any time, low cost, and no need to travel have proven to be advantageous.

Online resolution has particular advantages with lower monetary claims. In financial disputes, each party e-mails the amount at which they would settle their claim. In these "mediations," the agreed rules can provide for three rounds or more of settlement offers. Each party has also agreed to lower its demands by an agreed percentage—let's say 10%. By the third round, if the sides are close (let's say within 20%, or by some other formula), then that difference is halved and a deal struck. This is a brilliantly simple, mathematically oriented solution with special advantages for low-figure disputes.

The leading player in providing this "double-blind bid" procedure is Cybersettle.com, which was awarded a U.S. patent (among other countries) for that process. Other ADR service providers in cyberspace are ClickNsettle.com, SquareTrade.com, InternetNeutral, American Arbitration Association (adr.org), and SettleOnline, to name a few, and there are over fifty online dispute resolution Web sites at this time. Rather than being caught up in establishing expensive legal precedents over simply the issue of which law applies, where, and when—and then the main legal case must be fought—more and more parties are settling their disputes on or off the Net by using ADRs.

THE LAW OF LINKING

The World Wide Web depends on linking for its very existence, because this makes the Internet what it is. With the Net's maturity, however, the previous unconditional freedom to link has evolved into a framework of commonsense legal and netiquette rules that dictate limits on this freedom.

The general rule is that one doesn't need permission to link directly to another site, provided there is no commercial gain or some competitive informational advantage brought about by that linkage (even for a nonprofit institution). It is clear, moreover, that users should receive permission when they are "deep linking" or "framing," if only as a courtesy—and whether one should ask permission before any linking is a question of cyberethics,

quite distinct from the law and any of its requirements. Clearly, any stated or implied representation by linking that another's work is yours would be trade or service-mark infringement (e.g., using its logo in conjunction with a trade or service), unfair competition and libel (e.g., saying something is yours when it's not), or a violation of the covenant of "good faith" that's implied in netiquette. Linking to illegal content by itself can also be illegal; in *Universal City Studios v. Reimerdes* (2000), the court enjoined the defendants from creating links from their court-prohibited site to numbers of other "mirror" sites.

When links bypass home pages, connecting instead to a page deep within that site, additional considerations become present. Lawsuits have been filed and settled in the plaintiff's favor in which the plaintiffs complained over "deep links" bypassing the advertising on their home page, decreasing the "hit count" (users surf past the "count" page), diminishing their site's value, and allowing the defendant to "pass off" that information as its own.

The U.S. legal community, for example, watched closely when the owners of a newspaper, the *Shetland Times* in Scotland, brought a lawsuit against the *Shetland News*, a startup news service located in the same town. The *Shetland Times* published a daily online version of its newspaper, and the *News* was the first local daily to publish solely on the Web. It linked directly into the *Times* for news, and the *Shetland Times* went to court. The court granted the *Times* a temporary restraining order against the *News* and its linking practice (*Shetland Times v. Shetland News,* 1996), and the case soon settled out of court.

One well-publicized framing case was the lawsuit brought by various media companies (CNN, Time Warner, *USA Today,* the *Washington Post,* etc.) against Total News for its framing strategy. The media argued that the use of those frames, whereby Total News showed news stories taken from the plaintiffs with only its advertising displayed, violated their copyright and trademark rights. Total News reached a settlement before trial, agreeing not to frame any content and paid to link to their sites in a separate window (*Washington Post Co., et al. v. Total News*, 1997).

An accelerating Net phenomenon has been the rise of linking agreements in which a linked site pays for the exposure. These situations occur in two ways: (a) the linkage is in reality an advertising contract or customer referral agreement (see Amazon.com's "Associate" program); (b) the linked site commercially profits or otherwise benefits from a deep link. In both cases, a written linking agreement is essential.

Commercially profiting by deep linking or sophisticated software without the other site's permission is another growing legal area. Known as "robots," "bots," "spiders," or "crawlers," these automated software systems steam

past home pages deep into data banks, gathering information and transporting copies of whatever is desired back to the host site. If done frequently enough, these "hits" can create a near simultaneous look at whatever data are out there.

The largest Internet auction service, eBay, filed a lawsuit in late 1999 against Bidder's Edge, one of several Net auction search services. It had been accessing eBay's site up to 125,000 times daily (as much as 1.53% of the total daily requests to eBay) in searching out what was going on specifically at eBay's auctions, and eBay promptly sued after not being able to work out a license agreement with Bidder's Edge to pay for this continuing access.

The judge granted an injunction, agreeing with eBay's contention that Bidder's Edge and its robots were trespassing on eBay's site by using and diminishing the resources of eBay's computer systems without permission (*eBay v. Bidder's Edge,* 2000). Bidder's Edge quickly appealed, but just before the appellate court issued its decision, the two companies agreed to settle their lawsuit. Later, eBay reported that the settlement prohibited Bidder's Edge from sifting through its site for information and that Bidder's Edge agreed to pay an undisclosed amount of money.

Internationally, a Danish court in *Danish Newspaper Publishers Association v. Newsbooster.com* (2002) ordered an online news site, Newsbooster.com, to remove links from its site to articles on the Web sites of various newspapers, on the grounds that the links violated the EU Database Directory and bypassed the newspapers' home pages—following past precedent, both U.S. and a growing international law.

The directions of the law of linking are clear: (a) The general rule is that users do not need permission to link directly to the home page of another site, provided they don't disparage, misrepresent, or misappropriate; (b) given that these facts aren't present, framing and deep linking as opposed to linking will more likely constitute a violation; and (c) deep linking in commercial situations, as opposed to noncommercial ones, are likely to be violations in which (1) direct competitors are involved, (2) there is an advantage being taken by that linkage, and (3) there is an element of "unfairness" or bad faith on the part of the linking party. Furthermore, if data are being misappropriated, misused, or passed off by another as its own, even nonprofit or noncommercial sites may have valid causes of action.

CYBERCRIME

Cybercrime flourishes on the Internet, whether it is fraud, phony investments, hackers and poppers, pornography, rigged auctions, computer stalking, or prohibited gambling (and see http://www.cybercrime.gov for more).

The advantages of the Net for all users can quickly turn into disadvantages for law enforcement. The ease of entry and ability to disconnect from the Web allow criminals to appear and disappear within seconds with their illgotten gains. Arresting criminals is further complicated by the myriad jurisdictions that cybercriminals can cross so quickly, the protection of rogue nations, and differing state or national laws that can make extradition difficult. In turn, the authorities have had to add technology patrols to their arsenal of weapons, and Net users must be ever on the alert.

Although nations add protective laws over time (e.g., the United States with its Access Device Fraud Act, 18 U.S.C. 1029 [1984]; Computer Fraud and Abuse Act, 18 U.S.C. 1030 [1986]; Trademark Counterfeit Act, 18 U.S.C. 2320 [1984]; and the various others mentioned previously), the question of jurisdiction and enforcement is always raised in this context. With criminal statutes, states and countries look at jurisdiction from the point of view of their laws and interest in protecting their citizens. For example, if gambling is illegal in State A but not State B, then a Web site in State B could be prosecuted by State A for its allowing the residents of State A to use that site. The reasoning is that every Web operator has the ability to be in compliance with State A's laws by simply refusing to allow A's residents to break their state's laws (i.e., by filtering out State A users).

Enforcement is always another question. Located in the Bahamas or other locations where activities such as gambling are legalized, just how do you enforce State A's judgment penalizing another in a foreign state or country, not to mention the inherent personal jurisdiction and conflicts of laws question (i.e., the Yahoo! Nazi memorabilia decisions)? Unless there's increased cooperation among the differing authorities and criminal justice treaties agreed to, the First Amendment legal considerations by themselves will be voluminous. When property rather than an individual's freedom is concerned, courts seem to have fewer problems in determining rights, especially as to property that has already been seized (see, for example, *U.S. v. $734,578.82 in U.S. Currency*, 2002).

The horrors of September 11 brought other considerations of Internet crime to the forefront, given the ability of terrorists to communicate, raise money, and transfer assets over the Net. Among various legislative proposals, the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, or the "USA PATRIOT Act," illustrates these new thrusts. Among other provisions, the USA PATRIOT Act requires key financial sectors to implement programs that prevent their services from being used to launder money or finance terrorism. Entire new industries, such as operators of credit card systems, money transfer companies, check cashiers,

security firms, insurance companies, and even casinos—whether online or not—now are encompassed by strict regulations that once included only banks. This act also amended various provisions of the U.S. Code to allow broad interceptions of electronic communications and seizure of customer records (and also is controversial). Other nations have or are enacting similar legislation. Their courts, including those of the United States, are currently being asked to rule on just how legal these restraints are on individual privacy and constitutional rights. See the chapter on cybercrime and fraud, among other chapters on cyberterrorism and the criminal justice system in the U.S.

CONCLUSION

Hold onto your hats, the Internet hurricane of change is still howling—but inside your office or study. Legally, as well as technologically, there are more vibrant areas of change coming. For example, professional associations these days face Web sites that give information out to potential patients, clients, and customers on a global basis. From medicine and accounting to lawyering and filling drug prescriptions, state licensing boards are taking issue with this "practice without a required state license." This area continues to be well litigated.

Another area involves the ability of the Internet to "cut out the middleman." Because this medium allows consumers to contact suppliers directly, the old ways of conducting business are being seriously challenged in the courts. Travel agents sue airlines, wine distributors litigate with wineries that sell direct (in effect, suing their own customers or suppliers), and offline textbook distributors sue online retailers, not to mention the ever-increasing numbers of other industries that are litigating these types of developments. Although the consumer has benefited, it's clear that the legal industry also has.

A U.S. Supreme Court decision (*Granhold v. Heald,* 2005) ruled that laws dating back to post-Prohibition days were unconstitutional that allowed in-state wineries to ship directly to adult consumers within their borders, but then prohibited out-of-state wineries from shipping to the same accounts. The Court ruled that restricting the ability of out-of-state wineries to ship directly to consumers in today's Internet Age violated the Commerce Clause, despite the Twenty-first Amendment (which repealed Prohibition) which basically established that wine entering a state typically must be sold through a three-tier system of "producer to wholesaler to retailer" before reaching the consumer. If a state chooses to allow direct shipments of wine, then it must now do so on "evenhanded terms"—and the traditional wholesaler lost economic power again.

International price competition, courtesy of the Internet, is another litigious trend. For example, the Food and Drug Administration, citing safety concerns and regulatory violations, has sued U.S. companies that solicit drug prescriptions in the United States, then fax them to Canadian or other overseas suppliers, which then fill the orders and mail them back to their U.S. customers—at prices much lower than those available in the United States, owing to price regulations in effect overseas. These overseas Internet competitive developments will only increase over time, including the accompanying legal issues, battles, and legislative developments.

There's no question that the megasites and huge portals (such as AOL and Yahoo!) dominate the Internet, and that the question of antitrust will rear its head even higher in the future. From AOL's acquisition of gigantic Time Warner to the Covisint cyberventure between the world's six largest car manufacturers and their suppliers, the Web trend continues toward greater concentrations of power.

With the increase in cyberlaw actions over time, the rise and accepted use of cybercourts will also become a reality, along with more jurisdictions and courts converting to public-accessible electronic record keeping and filing. The federal government has instituted a PACER (Public Access to Court Electronic Records) system, which is an electronic public access service that allows users to obtain case and docket information from federal appellate, district and bankruptcy courts, including a U.S. Party/Case Index. Links to almost all of these courts are available by registering with PACER, the judiciary's centralized registration, and a relatively inexpensive fee is assessed for usage (see http://pacer.psc.uscourts.gov/ for more on this). States have also instituted their own digital-access court information systems and procedures, some more advanced than others; check out yours with a search engine.

In this direction, Michigan became the first state to create a specific cybercourt (Mich. Pub. Acts, 2001). When funded and operational, the new cybercourt under this legislation could become a model for other states. This court would have concurrent jurisdiction over commercial litigation in disputes where the amount in controversy exceeds $25,000. All filings are to be made electronically, whereas all actions, depositions, and court appearances are by "electronic communications," such as streaming video, audio, and Internet conferencing; the intent is that there will be no paper transmitted or physical interface between judge, litigants, or witnesses. Appeals are to be made either to a new cybercourt of appeals or through a normal appellate court. See http://www.michigancybercourt.net for the details and background of this approach.

Internationally, countries from England and Australia to Singapore already are experimenting with cybercourt systems and procedures. The Singapore Supreme Court, for example, has established a successful Technology Court allowing video conferencing for pretrial conferences, ex-parte applications, and other "noncontentious" applications, thus allowing lawyers to have their applications heard and decided by the court without the need to appear personally. Further, a digital filing service, service of process, notification system, and other electronic systems are in place, making this a model for the future (and see http://www.supcourt.gov.sg/ for more).

Regardless of the new Internet legal controversies that will rise up further in this new millennium, three realities exist: (a) the legal concepts already in place have proven to be quite adaptable to these challenges; (b) the concepts of fair play, common sense, and netiquette are filling in the gaps through court decisions and statutes; and (c) the use of ADR on the Net will continue to grow over time because of the inappropriateness of litigation to solve the cyberdisputes among the citizens of the world.

The Internet has enhanced our lives and challenged our laws. The legal system is continuing to meet the challenge, including the impact of information security issues, but our world is never again going to be the same.

GLOSSARY

Anticybersquatting Consumer Protection Act (ACPA) A U.S. statute (15 U.S.C. 1125, 1999) that protects trademark or service mark holders (including the names of famous people) from those who register a mark's domain name or its equivalent with a bad faith intent to profit from that act (e.g., cyberpirates). It allows the trademark or service mark holder to sue for actual or statutory damages (when actual damages are difficult to prove) and force the domain name to be transferred back.

"Click" or "Clickwrap" Contracts An agreement whereby a party agrees to the terms and conditions of an online agreement by clicking on a space reading "I agree," or some wording to that effect, to indicate the requisite mutual assent to those conditions and understanding.

Communications Decency Act Section 230 of this act (47 U.S.C. 223, 1996) provides that an online service provider is not to be treated as a publisher for purposes of liability for defamatory postings by third parties, nor liable for defamation in such cases.

Cyberlaw The emerging body of law that governs cyberspace transactions and disputes, otherwise known as the "Law of the Internet."

Cyberpirates Persons or entities who register a domain name that is the valid trademark or service mark of another, intending to sell that registered domain name back to the legitimate mark holder at a profit. This term is similar to

"cybersquatters" who register domain names ahead of such interest but wait (or "squat") on those names until offers to buy back those names are received from others.

Defamation A false statement made by some person or entity about another, either orally or in writing, that is published to a third party and wrongfully harms the injured party's reputation.

Digital Millennium Copyright Act (DMCA) The 1998 act that amended U.S. copyright law and included (a) a section prohibiting circumvention of encryption or security protections on copyrighted software to violate its copyright (17 U.S.C. 1201–1204) and (b) a section on online service provider liability (17 U.S.C. 512). The online provider provisions set down an administrative proceeding that is used to resolve copyright disputes over third-party postings with online servers and establishes a "safe harbor" liability protection for those providers.

Distributed Denial of Service (DDoS) Attack A simple denial of service ("DoS") attack typically involves one computer making repeated connection requests in trying to overpower the target system. In a DDoS attack the connection requests originate from a large number of computers, making it difficult to distinguish attacking traffic from legitimate ones. To launch a DDoS attack, a hacker accesses a computer system without authorization and inserts a software program that renders the system a "master," able to control other computer systems. The hacker places software code given on numbers of other computer systems, causing them to operate as "agents" or "zombies" of the master system. The master system instructs its zombies to produce a flood of simultaneous requests to connect to the target system, overwhelm its capabilities, and attempt to thwart legitimate connection requests.

Fair Use The U.S. Copyright Act provides that the "fair use" of copyrighted works involving purposes such as criticism, comment, news reporting, teaching, scholarship, or research is not copyright infringement. Thus, some copying or copyright use is legally permissible in the United States that ordinarily would not be allowable in other countries.

Intellectual Property Property that the mind creates from intellectual, creative processes, whether music, books, inventions, poetry, software, trademarks, domain names, or even trade secrets. Depending on the form of intellectual creation, such property is protectable by copyrights (i.e., music, software, or a Web site's "look and feel"), trademarks (i.e., distinctive marks, whether identifying products or service), patents (i.e., inventions and Internet business procedures), and trade secrets (i.e., customer lists, Coca-Cola's formula, and so on).

Internet Corporation for Assigned Names and Numbers (ICANN) The nonprofit organization that oversees a wide range of Internet functions (once the responsibility of the U.S. government) and is now managed by an international board of directors. Among other functions, ICANN promulgates policy on the registration of domain names, accreditation of new registrars, and implementation of domain-name dispute resolution policies.

Jurisdiction The power of a court or governmental agency to hear a case and decide the rights of the people or entities that appear before it. This jurisdiction can be *in personam* (determining the rights of people or entities, wherever they reside) or *in rem* (determining the ownership rights to property that is located within the court's territorial limits, regardless of where the disputing parties reside).

Long-Arm Statute U.S. state statutes that authorize a local court to assert personal jurisdiction over a nonresident defendant located outside that state, given certain factual circumstances being present, such as causing injury within that state by an act that takes place within it (i.e., a car accident).

Netiquette An informal, essentially noncodified doctrine of "Web manners," courtesy, and cyberethics aimed at creating a system establishing what is or isn't acceptable conduct on the Net, regardless of what the law provides.

No Electronic Theft Act (NET) A U.S. act (17 U.S.C. 506(a), 1997) that provides there is an illegal infringement when pirated copyrighted material has a value of $1,000 (a misdemeanor) or $2,500 (a felony), even though there is no monetary gain or economic incentive on the part of the infringer.

"Opt In" and "Opt Out" The two distinct privacy policies used by Internet firms and Web sites, which may or may not be codified. With "opt-out" provisions, the user must take the affirmative step to say "no" or refuse permission to a Web site's collection and transmission of financial and other sensitive consumer information. With "opt-in" policies, the Web site must take the steps to gain the positive approval of a user before it can collect, transmit, or sell such private information. Marketing firms prefer "opt-out" policies or laws, because these are less marketing restrictive and put the burden on the user, not the site.

Prima Facie Evidence Evidence presented that indicates a strong presumption the given fact or evidentiary assertion is factually true.

Service Mark A word, name, logo, mark, device, or some combination used by any person or entity to identify and distinguish services performed by it from those of another (e.g., Priceline.com's name and logo).

"Shrink-wrap" Agreement An agreement whereby a party agrees to the terms and conditions of the contract, the provisions contained inside the box in which the goods are packaged, by opening the wrapper, or plastic shrink-wrap, that encloses the entire package. The act of opening the plastic, or box, indicates the requisite mutual assent to those conditions and understanding.

Terms of Use The legal provisions that govern anyone's use of a particular Web site, including purchasing its product or service, and typically include disclaimers of liability, indemnity, handling of disputes, applicable law, dispute resolution, copyright and trademark notices, linking conditions, among other areas. Terms of Use provisions generally are located at the bottom of the home page with an icon of the heading "Legal Provisions," or some similar identification. They can also include privacy provisions, although these provisions are typically set out separately.

Tort The breach of a legal duty to exercise reasonable care that proximately causes injury or damage to another. This is a civil wrong that does not arise from a breach of contract.

Trademark A word, name, logo, mark, device, or some combination used by any person or entity to identify and distinguish its goods from those of another (e.g., McDonald's golden arches or Nike's winged shoe).

U.S. Copyright Office The U.S. agency that oversees the registration and regulation of copyrights (see http://www.loc.gov/copyright).

U.S. Patent and Trademark Office (PTO) The U.S. agency that oversees the registration and regulation of patents and trademarks/service marks (see http://www.uspto.gov for further information).

World Intellectual Property Organization (WIPO) The specialized United Nations agency and intergovernmental organization that is responsible for promulgating and administering major international intellectual property conventions.

REFERENCES

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (2001).

American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., 2000 U.S. Dist. Lexis 7299, D. Ariz. (2000).

Amsan LLC v. Prophet 21 Inc., No. 01-1950, 01-1954, (E.D. Pa.), U.S. Dist. LEXIS 16698 (2001).

Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125(d) (1999).

Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002).

Ashcroft v. American Civil Liberties Union, 322 F. 3d 240 (2003).

Ashcroft v. American Civil Liberties Union, 124 Sup. Ct. 2783 (2004).

Bally v. Faber, 29 F. Supp.2d 1161 (1998).

Bick, J. (2001). Securities law. Avoiding the violations risked by companies that use the Web to disseminate information. *The Internet Newsletter. 6* (7), 1.

Bick, J. (2003). Are you breaking the law? *The Internet Newsletter, 1* (6), 1.

Blakey v. Continental Airlines, 164 N.J. 38, 751 A.2d 538 (2000).

Brower v. Gateway 2000, Inc., 246 A.D.2d 246 (1998).

Buford, D. (2003). Cyberspace is being discovered, and employers may be footing the bill. *New York Employment Law Letter, 10* (7).

Cairo v. Crossmedia Services, 2005 WL 756610, 2005 U.S. Dist. LEXIS 8450 (N.D. Cal., April 1, 2005).

Calder v. Jones, 465 U.S. 783 (1984).

California Legislative Service, Ch. 915, S.B. 1386 (2002).

Children's Internet Protection Act, 20 U.S.C. 9101 (2000).

Children's Online Privacy Protection Act, 47 U.S.C. 231 (1998).

Crispi v. The Microsoft Network, L.L.C., 323 N.J. Super. 118 (N.J. App. Div., 1999).

Danish Newspaper Publishers Association v. Newsbooster.com, Bailiff's Court of Copenhagen, Denmark (July 5, 2002).
Deutsche Bank, In the Matter of, SEC No. 3-10957 (2002).
de Villiers, M. (2003). Virus Ex Machina: Res Ipsa Loquitur. *Stanford Technology Law Review*, (1).
de Villiers, M. (2004). Computer Viruses and Civil Liability: A Conceptual Framework. *Tort & Insurance Law Journal*, *40* (123).
Dow Jones v. Gutnick, 2002 HCA 56 (2002).
DVD Copy Control Association, Inc. v. Bunner, 93 Ca. App. 4th 648 (6th Dist., 2001).
DVD Copy Control Association, Inc. v. Bunner, 75 P. 3d 1 (2003).
DVD Copy Control Association, Inc. v. Bunner, 116 Cal. App. 4th 241 (2004).
eBay v. Bidder's Edge, 100 F. Supp.2d 1058 (2000).
Eldredge v. Ashcroft, U.S. Sup. Ct. No. 01-618 (2003).
Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001 (2000).
Federal Trademark Dilution Act, 15 U.S.C. 1125(c) (1995).
Ferrera, G., Lichtenstein, S., Reder, M., Bird, R., & Schiano, W. (2003). *Cyberlaw: Text and Cases* (2nd ed.). Cincinnati, OH: South-Western.
Financial Services Modernization Act, 15 U.S.C. 6801 (1999).
Ford Motor Co. v. Lane, E.D., Michigan, No. 99–74205 (1999).
Geoff v. AOL, Inc., No. PC 97–0331, R.I. Super. Ct. (1998).
Gold, J. (2002). Insurance coverage for Internet and computer related claims. *The Computer & Internet Lawyer*, *19* (4), 8.
Graham v. Oppenheimer, No. 3:00cv57, E.D. Va. (2000).
Granhold v. Heald, U.S. Sup. Ct. (Docket No. 03-1116, decided May 16, 2005).
Greenberg v. National Geographic Society, 244 F. 3d 1267 (2001).
Grynberg v. Agri Tech, Inc., 10 P.3d 1267 (2000).
Gus' Catering, Inc. v. Menusoft Systems, 762 A.2d 804 (2000).
Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 (1996).
Homeland Security Act of 2002, U.S. Pub. L. Nos. 107-296, 116 Stat. 2135 (2002).
i.LAN Systems v. NetScout Service Level Corp., 183 F. Supp.2d 328 (2002).
International Shoe Company v.Washington State, 66 U.S. Sup. Ct. 154 (1945).
Jacobson, H., & Green, R. (2002). *Computer crimes. American Criminal Law Review*, *39* (273).
Lucker Manufacturing v. Home Insurance Co., 23 F.3d 808 (1994).
MGMStudios, Inc. v. Grokster, Ltd., 380 F. 3d 1154 (2004).
Mich. Pub. Acts 262 (2001).
Mortenson Co. Inc. v. Timberline Software Corp., 140 Wa.2d 568, 998 P.2d 305 (2000).
Moseley v. Secret Catalogue, Inc., 537 U.S. 418 (2003).
National Bellas Hess v. State of Illinois, 386 U.S. 753 (1976).
New York Times v. Tasini, 533 U.S. 483 (2001).
Panavision International, L.P. v. Toeppen, 141 F.3d 1316 (1998).

Pavlovich v. Superior Court (DVD Copy Control Association, real party in interest), 29 Ca. 4th 262 (2002).
Pinkney, K. R. (2002). Putting blame where blame is due: Software manufacturer and customer liability for security-related software failure. *Albany Law Journal of Science & Technology*, *13* (43).
Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058 (2002).
ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (1996).
Radin, M. J. (2001). Distributed denial of service attacks: Who pays? (part I). *Cyberspace Lawyer*, *6* (no.9), 2.
Radin, M. J. (2002). Distributed denial of service attacks: Who pays? (part II). *Cyberspace Lawyer*, *6* (no.10), 2.
Recording Industry Association of America v. Verizon Internet Services, 240 F. Supp. 2d 24 (2003).
Recording Industry Association of America v. Verizon Internet Services, 351 F. 3d 1229 (2003).
Register.Com, Inc. v. Verio, 126 F. Supp.2nd 238 (2000).
Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
Robotic Vision Systems v. Cybo Systems, Inc., 17 F. Supp.2d 151 (1998).
Savetz, K. (2002, May 1). Lawsuits, downtime, data that has been stolen or destroyed—data insurance helps tech companies recoup unexpected losses. *New Architect*, p. 32.
Shetland Times v. Shetland News, Scottish Outer House, 1997 S.C. 604 (1996).
Sonny Bono Copyright Term Extension Act, 17 U.S.C. 101, 302–305 (Supp. 1999).
Specht v. Netscape Communications Corp., 306 F.3d 17 (2002).
Springfield Hydroelectric Company v. Copp, et al, 779 A.2d 67 (2001).
State Street Bank v. Signature Financial Group 149 F.3d 1368 (1998).
Universal City Studios v. Reimerdes, 82 F. Supp.2nd 211 (2000).
U.S. v. $734,578.82 in U.S. Currency, 286 F.3d 641 (2002).
United States, et al v. American Library Association, 123 S. Ct. 2297 (2003).
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
Washington Post Co., et al. v. Total News, 97 Civ. 1190, S.D.N.Y. (1997).
WIPO Copyright Treaty, 36 I.L.M. WIPO Treaty, WIPO Doc. CRNR/DC/94 (1996).
Yahoo! v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp.2nd 1181 (2001).
Yahoo! v. La Ligue Contre le Racisme et L'Antisemitisme, 379 F. 3d 1120 (2004).
Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1122 (1997).

FURTHER READING

Ambrose, S. F., Jr., & Gelb, J.W. (2003). Consumer privacy regulation, enforcement, and litigation in the United States. *The Business Lawyer*, *58*, 1181.

American Civil Liberties Union et al. v. Ashcroft, 322 F. 3rd 240 (2003).
Ashcroft v. American Civil Liberties Union, 124 S. Ct. 399 (2003-1).
Bensusan Restaurant v. King, 937 F. Supp. 295 (1996).
Child Online Protection Act, Pub. L. No. 105-277, Title XIV (1998).
Consumer Sentinel, for the latest on primarily U.S. fraud protection and online complaint procedures: http://www.consumer.gov/sentinel
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), Senate No. 877 (passed November 25, 2003; signed into law, December 16, 2003).
Department of Commerce, for latest developments including EU "safe harbor" privacy guidelines: http://www.commerce.gov
Econsumer.gov, for data on international fraud protection and online complaint procedures: http://www.econsumer.gov/
For EU rights developments, including its copyright directive: http://eurorights.org
FTC site, for data on COPA, consumer protection, and latest developments in other areas: http://www.ftc.gov
ICANN, for information on its domain name dispute resolution process, registration, and accepted registrars: http://www.icann.org
International Money Laundering Abatement and Financial Anti-Terrorism Act, U.S. Pub. Laws No. 107–56, Title III (2001).
Kelly v. Arriba Soft Corp., 280 F.3d 934 (2002).
PACER, for information on Federal Appellate, District and Bankruptcy courts, including a U.S. Party/Case Index: http://pacer.psc.uscourts.gov/
Powers, D. M. (2002). *The internet legal guide: Everything you need to know when doing business online.* New York: Wiley.
Securities and Exchange Commission, for information on securities and investment fraud: http://www.sec.gov
Spamlaws.com, for the latest developments on antispam laws, both in the United States and globally: http://spamlaws.com
U.S. Copyright Office information, including DCMA and registration data: http://www.loc.gov/copyright/
U.S. Dept. of Justice, for overall and latest information on computer-related crimes: http://www.cybercrime.gov
U.S. Patent and Trademark Office, for information on trademarks, service marks, and patents: http://www.uspto.gov
Vir, Monica (2003). The Blame Game: Can Internet Service Providers Escape Liability for Semantic Attacks? *Rutgers Computer and Technology Law Journal*, *23* (193).