COVERAGE ISSUES RAISED BY E-MAIL AND THE INTERNET

(*Followed by 2005 Supplement!*)

Mark G. Sheridan*
Adam H. Fleischer
BATES & CAREY LLP
191 N. Wacker Drive, #2400
Chicago, IL 60062
(312) 762-3100

***The authors wish to express their sincere appreciation to David M. Alt for his assistance in preparing this article.**

I. [13.1] INTRODUCTION TO CYBERCLAIM RISKS

The Internet is the fastest growing form of communication in human history. Radio required 38 years to reach 50 million listeners. Television reached that many viewers in 13 years. The Internet, however, went from a fledgling form of communication in 1989 (with an estimated 90,000 users) to 40 million users just 7 years later. Since 1996, the number of users has been estimated to have almost doubled each year, such that it is now likely that the number of Internet users exceeds half a billion people. See Howard B. Stravitz, *Personal Jurisdiction in Cyberspace: Something More Is Required on the Electronic Stream of Commerce,* 49 S.C.L.Rev. 925 (1998).

Given this explosive growth, many insurance coverage practitioners anticipate a huge new wave of coverage litigation involving the Internet. Indeed, it is common to hear predictions that the volume of coverage litigation involving cyberspace will approach the volume of coverage litigation involving asbestos or environmental contamination. Although it remains to be seen whether these expectations are overblown, there is little doubt that courts will soon be faced with a myriad of coverage disputes involving underlying cyberspace claims, or "cyberclaims." Indeed, as described in this chapter, the first examples of these coverage actions have already been filed.

Because the number of reported coverage decisions involving Internet claims is still quite small, insurance coverage practitioners should prepare for the anticipated coverage disputes by examining how the risks associated with cyberspace differ from traditional torts. Cyberspace torts, or "cybertorts," differ in two principal ways from their "offline" predecessors:

a. The number of suits involving these intellectual property claims can be expected to be exponentially greater than the number of suits involving these torts prior to the introduction of the Internet.

b. The complexity of the issues involving international law, multi-jurisdictional disputes, and technical computer expertise will increase the expense of defending and indemnifying these types of losses beyond the costs associated with defending and indemnifying the same torts arising from brick-and-mortar businesses.

Both of these differences increase the stakes of insurance coverage litigation involving Internet claims.

Because cyberspace claims arise in both the third-party and first-party contexts, this chapter examines the nature and elements of third-party and first-party cyberclaim risks. This chapter then addresses the corresponding third-party and first-party coverage issues associated with traditional insurance policies.

II. [13.2] THIRD-PARTY CYBERCLAIM RISKS

Insureds seeking coverage for cybertorts are most likely to focus on the "advertising injury" coverage granted in CGL policies. Insureds may argue that Internet activity giving rise to

cybertorts may constitute "advertising" within the definition of a policy's "advertising injury" provision. Therefore, in determining whether coverage exists, cybertorts must be analyzed within the framework of the "advertising injury" provision of the policies.

A. [13.3] Defamation

The Internet can be characterized as a large publisher. In this sense, and for ease of discussion, we can refer to the torts associated with the publishing aspect of the Internet as "publishing torts." "Publishing torts" arising in cyberspace include the defamation claims of libel and slander, invasion of privacy, and copyright, trademark, and patent infringement. The chief characteristic that differentiates the cyberspace version of these torts from their predecessors is the increasing ease and perceived anonymity with which the "publication" can take place over the Internet. The ability for every user to act with perceived anonymity has led some people to lose their inhibitions and their common sense, which in turn has generated a flood of Internet publishing torts.

1. [13.4] Introduction to Defamation Law

Slander is spoken defamation, as opposed to libel, which is written defamation. In most jurisdictions, a statement is considered defamatory if it is false, made recklessly, and tends to cause harm to the reputation of another by lowering that person's reputation in the eyes of the community or deterring third persons from associating with the defamed individual.

Typically, there are five types of slander that are considered "actionable per se." *Suhadolnik v. City of Springfield,* 184 Ill.App.3d 155, 540 N.E.2d 895, 913, 133 Ill.Dec. 29 (4th Dist. 1989). The plaintiff need not plead or prove actual damage to his or her reputation with respect to slander "per se," as the damage is presumed if the slander is proved. The five categories of slander "per se" are

a. that which imputes the commission of criminal offenses;

b. that which imputes infection with a loathsome communicable disease;

c. that which imputes the inability of the plaintiff to perform or lack of integrity in the discharge of duties of office or employment;

d. that which prejudices a party or imputes the lack of ability in his or her trade, profession, or business; and

e. that which imputes adultery or fornication. *Id.*

A plaintiff asserting a cause of action for slander bears the burden of proving that the alleged statements were not protected speech under the First Amendment to the United States Constitution. If the alleged statements are considered to be solely statements of opinion, they are likely to receive First Amendment protection. If the statements are considered either purely factual or opinions that imply defamatory facts, then the statements may be actionable as slander. *O'Donnell v. Field Enterprises, Inc.,* 145 Ill.App.3d 1032, 491 N.E.2d 1212, 96 Ill.Dec. 752 (1st Dist. 1986).

In determining whether the statements are purely opinion or whether they contain actionable defamatory facts, courts may consider three factors:

a. whether the language of the statement has a precise and readily understood meaning;

b. whether the general tenor of the context in which the statement appears negates the impression that the statement has factual content; and

c. whether the statement is capable of being objectively verified as true or false.

Defamation law in cyberspace may place a greater burden of proof on private individuals than the current defamation law. According to traditional legal theory, if the plaintiff is a public official or a public figure, then he or she is required to prove that the publication was made with actual malice. If the plaintiff is a private "ordinary" person, however, he or she need prove only that the published remarks were false and were made negligently. *See Kuwik v. Starmark Star Marketing & Administration, Inc.*, 156 Ill.2d 16, 619 N.E.2d 129, 188 Ill.Dec. 765 (1993). The rationale for this distinction is that public figures can more easily combat defamation through superior access to media and, therefore, have an advantage that is not as readily available to a private person. However, it can be argued that, via the Internet, even the ordinary private individual has access to a fantastic weapon with which to battle allegedly defamatory remarks, so all Internet users are "public persons" for purposes of defamation analysis.

If adopted, this theory would require that all defamation plaintiffs publicly debate their accusers and obtain legal recourse only if they can prove actual malice. Placing such an affirmative duty on defamed individuals to defend themselves on the Internet has numerous shortcomings. First, it encourages the publication of misleading half-truths because the author has the comfort of knowing that no liability can possibly result as long as there is no actual malice present. Second, forcing defamed individuals to engage in a public defense will inevitably lend legitimacy to the defamatory comments. These reasons may lead courts to reject the argument that individuals defamed over the Internet should be considered "public persons."

2. [13.5] Defamation Claims in Cyberspace

In the pre-Internet world, defamation claims involved an individual arguing that the insured said or printed an untrue comment that damaged the individual's reputation. These claims are difficult to prove, and the damages are difficult to calculate. However, the defamation claims stemming from the Internet are often brought by corporate plaintiffs rather than individuals. These claims arise when the insured provides access to or hosts an online chatroom or bulletin board. Users may post messages in these chatrooms claiming a company is the focus of a federal investigation or containing other false and disparaging information. This type of defamation has severely impacted the stock of many companies, and the companies have aggressively fought back through filing defamation claims against the defaming individual (if identifiable) as well as the host of the chatroom or bulletin board. For example, on February 15, 2001, Go Online Networks Corp. announced it was filing suit against an individual who posted false information on the Internet regarding the company's diversification efforts. See *Go Online Networks Pursues Legal Action After Hoax,* Reuters (Feb. 15, 2001) (available online with subscription at www.nytimes.com/reuters/technology/tech-goon-linenetworks).

In a ruling of the first of its kind, a California court recently ruled that Internet message boards devoted to discussions about a publicly traded company are indeed "in connection with a public issue" and are fully protected from defamation claims. *Global Telemedia International, Inc. v. Doe 1,* 132 F.Supp.2d 1261 (C.D.Cal. 2001). The court held that a publicly traded company is of public interest because its successes or failures not only will affect individual investors but also, in the case of large companies, potentially may impact market sectors or the markets as a whole. In addition, the court noted that the fact that a message board generates tens of thousands of messages further indicates that the company is of public interest.

3. [13.6] Communications Decency Act

The Communications Decency Act of 1996 (CDA), Pub.L. No. 104-104, 110 Stat. 133, serves as a shield from liability for Internet service providers (ISPs) and other online conduits of information. The CDA exempts ISPs, telecommunications carriers, and search engines from defamation liability for information disseminated by another "information content provider." 47 U.S.C. §230. The CDA also exempts persons who are "similarly engaged in the transmission, storage, retrieval, hosting, formatting, or transmission of a communication made by another" as long as the person does not alter the content of the message by deleting it. 47 U.S.C. §231. Section 230 also bars courts and legislatures from treating ISPs as the "publisher or speaker" of content that was provided by "another information content provider," which is defined as anyone "responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." *See Jane Doe One v. Oliver,* 46 Conn.Supp. 406, 755 A.2d 1000 (2000); *Jane Doe v. America Online, Inc.,* 783 So.2d 1010 (Fla. 2001) (America Online found not liable for defamation even though it may have had notice of defamatory third-party posting).

The CDA also grants ISPs "Good Samaritan" protection from civil liability for prohibiting the transmission or posting of offensive material, *i.e.,* protection for attempting to censor content. Section 230 dictates that ISPs are not liable for blocking content considered to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

4. [13.7] John Doe Suits

A number of companies have attempted to determine the identity of the authors of alleged defamatory messages posted on the Internet. These companies have filed "John Doe" defamation suits in which they then attempted to subpoena the identity of the alleged defamers from America Online or other ISPs. However, these suits have resulted in little success. A federal court recently blocked the efforts of a bankrupt Internet company to learn the names of people who anonymously derided it in an investor chatroom. In *Doe v. 2TheMart.Com, Inc.,* 140 F.Supp.2d 1088 (W.D.Wash. 2001), the court found the company had not provided sufficient evidence to set aside First Amendment rights of people who spoke in the chatroom under nicknames such as "NoGuano" and "The Truthseeker." The ruling was the first by a federal judge to address the issue of whether the identities of people not named in a lawsuit could be disclosed because of statements made on the Internet. See Steve Miletich, *Court Ruling Big Win for Net Privacy,* Seattle Times, Apr. 20, 2001 (available online at http://seattletimes.nwsource.com/html/businesstechnology/134286864_privacy20.html).

B. [13.8] Invasion of Privacy

Individuals make e-mail transmissions from home, pay bills and perform banking functions online, have medical histories and health care information stored in computer databases, and even have items like movie rental habits stored on the neighborhood video store's hard drive. Because of these modern methods of information storage and transmission, new issues related to privacy are constantly surfacing. When a letter is mailed and received or a telephone call is dialed and terminated, there is no easily discoverable evidence of the communication once the communication has ended. In cyberspace, however, it is easy to report that a transmission was made, as well as record or preserve the content of the message and any response. Public and private parties have grave concerns about the ease with which all types of messages are sent, deleted, filed, and answered — as well as how they are intercepted by those other than the communicating parties.

1. [13.9] Invasion of Privacy in Cyberspace

One legal issue that presents a mixture of security and invasion of privacy concerns is the fact that consumers' private information is thought to be extremely vulnerable to hackers and to misuse in relation to the growing e-commerce industry. As customers visit e-commerce sites, they leave electronic footprints that potentially can reveal everything from their interests to their income. Companies can use this information for their own marketing purposes or for sale to others.

Many Internet privacy complaints are caused by the "cookie monster." A "cookie" refers to a small text file implanted on a computer by the Web site that the user is visiting. The file contains an identification number that allows an Internet company to recognize a user when that user accesses a Web site. The Web site then collects information such as e-mail addresses, mailing addresses, and phone numbers and stores it in that person's cookie file. Thus, Web sites can recognize a repeat visitor and tailor Web content (including advertisements) to the user's interests. Some advertisers now use cookies to monitor what advertisements a user has most recently seen on other sites or what sites the user has most frequently visited. Cookie technology can be at work without a user ever knowing it.

In the past, cookies have been labeled with random numbers rather than user names; *i.e.,* the Web sites that your computer visits can collect data about your computer's buying habits, but those sites cannot identify the name and address of the person who owns or uses your computer — yet. However, some companies are taking steps to match downloading information obtained by "cookies" with the identity of the downloader. For example, drug companies were recently found to be paying a third-party firm, Pharmatrak, to monitor the information consumers reviewed on the drug makers' Web sites. See Robert O'Harrow, Jr., *Firm Tracking Consumers on Web for Drug Companies,* Washington Post, Aug. 15, 2000, at EO1 (available online at www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A25494-2000Aug14). Pharmatrak's services included, among other things, reporting to the drug companies which computers downloaded information about HIV or a particular prescription drug. While not directly identifying users requesting this information, the company eventually plans to match the information to user identities ("In the future, we may develop products and services which collect data that, when used in conjunction with the tracking database, could enable a direct identification of certain individual visitors." *Id.*).

2. [13.10] Invasion of Privacy Examples Related to Internet Marketing

Invasion of privacy on the Internet can take the form of the disclosure of private information, such as credit card numbers. A breach of security at Columbia House, an online retailer, lead to the disclosure of thousands of customer names, addresses, and credit card numbers. Stefanie Olsen, *Columbia House Breach Exposes Customer Info,* CNETNews.com, www.cnet.com/news/0-1005-200-4891643.html (Feb. 21, 2001). Likewise, a security glitch with the OfficeMax Web site caused customer data to be forwarded to other shoppers. When customers sent the OfficeMax Web page links to friends and business associates, the customers were unknowingly forwarding their credit card data and other personal information as well. Carol King, *Security Glitch at OfficeMax; Retailer Says It's Resolved,* InternetNews.com, www.internetnews.com/ec-news/article/0,,4_596241,00.html (Feb. 22, 2001).

An example of an invasion of privacy suit involves RealNetworks and its RealJukebox product. The RealJukebox product is available for free on the Internet. RealJukebox helps users organize their CD libraries, but it does so by uploading the users' CD information onto the RealJukebox server — without telling the users that this is happening. Individuals who had personal information uploaded by the product filed a class action lawsuit. The suit seeks $500 in damages for each of RealNetworks' 30 million users. *See In re RealNetworks, Inc., Privacy Litigation,* No. 00 C1 1366, 2000 WL 631341 (N.D.Ill. May 8, 2000).

C. Copyrights

1. [13.11] Introduction to Copyright Law

Copyright infringement occurs when copyrighted material is reproduced, utilized, or repeated without the consent of the copyright holder. Copyrighted material, including words, photos, artwork, or images, is the exclusive property of the copyright holder, who is said to "own" the material. The Copyright Act of 1976, Pub.L. No 94-553, 90 Stat. 2584, protects eight kinds of material: literary works; music; drama; choreography; pictorial, graphic, and sculptural works; motion pictures and audiovisual works; sound recordings; and architectural works. 17 U.S.C. §102(a). Computer software falls within the "literary works" category of the Copyright Act. Every time an item of software is loaded into a computer's memory, a "copy" of that software is created. A transmission over the Internet of any of these types of protected material, with valid copyrights in place, may result in copyright infringement.

The Copyright Act provides that only the owner of a copyrighted work enjoys the right to reproduce the work, prepare derivative works based on the copyrighted work, distribute copies of the work to the public, and (with regard to certain types of copyrighted material) perform and display the work publicly. The Act also provides that one who violates the copyright holder's exclusive rights is strictly liable as an "infringer of the copyright." 17 U.S.C. §501(a). To present a prima facie case for copyright infringement, the holder must establish "ownership" of the copyrighted material and "copying" by the defendant but need not prove intent or knowledge by the infringer. *Bourne Co. v. Hunter Country Club, Inc.,* 990 F.2d 934 (7th Cir. 1993).

Copying can be difficult to prove over the Internet. The plaintiff must show that the defendant had access to the copyrighted material and that there is a substantial similarity between the two works. If a plaintiff cannot prove access, a showing that the two works are "so strikingly similar as to preclude the possibility of independent creation" is sufficient. *See, e.g., Playboy Enterprises, Inc. v. Webbworld, Inc.*, 968 F.Supp. 1171, 1174 (N.D.Tex. 1997), citing *Ferguson v. National Broadcasting Co.*, 584 F.2d 111, 113 (5th Cir. 1978). Federal law will preempt claims under Illinois law for copyright infringement unless an additional element qualitatively different from those necessary under federal law is present *Marobie-Fl., Inc. v. National Association of Fire Equipment Distributors*, 983 F.Supp. 1167, 1180 (N.D.Ill. 1997).

There are three types of copyright liability that could affect insureds with respect to Internet claims: direct, vicarious, and contributory. *See Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143 (7th Cir. 1992).

A plaintiff makes a case for *direct copyright infringement* when he or she establishes the prima facie elements, as provided above. There is no need to prove the defendant's intent or knowledge to establish liability.

A defendant can be held liable for *vicarious copyright infringement* if he or she has a financial interest in the activity causing the infringement as well as supervisory right and opportunity over the action causing the infringement, *e.g.*, the right and ability to control what is posted on a defendant's Web site. Financial interest in the infringing activity needs to be significant and direct. Again, a plaintiff need not show intent or knowledge to make a claim for vicarious copyright infringement. The defendant's supervisory authority and financial interest are issues of law to be decided by the court.

A defendant is liable for *contributory copyright infringement* when infringing activity occurs and the defendant has knowledge of and contributes to the infringing activity.

The most common exception to copyright infringement is the "fair use doctrine," which is a complete defense if the use is for nonprofit or educational purposes or if the material used is insignificant relative to the whole. See 17 U.S.C. §107. *See also Sega Enterprises Ltd. v. MAPHIA*, 948 F.Supp. 923 (N.D.Cal. 1996).

2. [13.12] Examples of Copyright Claims in Cyberspace

One of the most notable cases involving a copyright claim in cyberspace was brought by record companies and music publishers against Napster. The record industry sought injunctive relief prohibiting Napster from facilitating the transmission and retention of digital audio files by its users. The record industry alleged that Napster was directly, contributorily, and vicariously infringing on its copyrights. The district court preliminarily enjoined Napster from "engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings without express permission of the rights owner." *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d 896 (N.D.Cal. 2000), *aff'd in part, rev'd in part, remanded*, 239 F.3d 1004 (9th Cir. 2001).

In affirming the district court's decision, the Ninth Circuit held that there was sufficient evidence in the record to support the conclusion that Napster directly, contributorily, and vicariously infringed on the plaintiffs' copyrights. In finding a likelihood of direct infringement, the court noted that most of the files available on Napster were plaintiffs' copyrighted material. Moreover, the court dismissed Napster's claim that the "fair use" doctrine operated as a valid affirmative defense. The court emphasized that copying an entire work militates against a finding of fair use. 239 F.3d at 1016.

In addition to direct infringement, the court also held that there was sufficient evidence to hold Napster liable as a "vicarious infringer." 239 F.3d at 1022. The court noted that Napster's future revenue is directly dependent on increases in user base. The court also affirmed the district court's reasoning with respect to contributory infringement to the extent that Napster received notice from the record industry of specific files infringing copyrighted material. 239 F.3d at 1027.

Despite the recording industry's legal victory, enforcing the injunction has proved to be difficult. See David Kravets, *Judge Powerless To Stop Copyright Infringement on Napster,* The Detroit News, Apr. 28, 2001 (available online at www.detnews.com/2001/technews/0104/29/technology-218023.htm). Nonetheless, as one of the first federal appellate court decisions applying copyright principles to Internet claims, the *Napster* decision is likely to have significant impact on the development of the law in this area.

3. [13.13] The Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA), Pub.L. No. 105-304, 112 Stat. 2860 (1998), limits the liability of ISPs and any other company that qualifies as a "service provider" from vicarious or contributory copyright infringement. The DMCA defines "service provider" as any entity that offers the transmission of "digital online communications, between or among points specified by a user" or that provides "online services or network access." 17 U.S.C. §512(k).

Liability may be limited by satisfying three threshold requirements as stated in 17 U.S.C. §512(i). The ISP must first adopt a policy that is "reasonably implemented" under which it will terminate in "appropriate circumstances" the accounts of "repeat infringers." Second, the ISP must inform its account holders of this policy. Third, the ISP must facilitate and not impede "standard technical measures," *i.e.,* measures used by copyright owners to protect their works. Issues such as what constitutes a "repeat infringer," "reasonable implementation," and "appropriate circumstances" are obviously open to interpretation. The DMCA also requires ISPs to remove or disable access to stored material when the ISP receives a written notice from a user who presents evidence of the copyright infringement.

The DMCA creates five specific "safe harbors" in which ISPs are protected from liability for copyright infringement. ISPs can obtain a degree of immunity for certain types of claims that fall within a safe harbor. The first safe harbor, *transitory digital network communications,* protects an ISP from liability for copyright infringement when copyrighted material passes through the ISP's network. 17 U.S.C. §512(a). The second safe harbor, *system caching,* protects an ISP from liability for temporarily storing copyrighted material on its network before passing it on to service subscribers. 17 U.S.C. §512(b). The third safe harbor protects an ISP with respect to copyrighted

materials that are stored on the ISP's network at the direction of third-party users. 17 U.S.C. §512(c). A fourth safe harbor protects an ISP from liability for any good-faith act to disable access to material believed to be infringing on a copyright. 17 U.S.C. §512(g). The fifth safe harbor protects an ISP accused of negligently linking or referring users to another site with infringing material. 17 U.S.C. §512(d).

To qualify for protection against these types of claims, the ISP (a) must have no actual knowledge that the material is infringing, (b) must be unaware of "facts or circumstances" that would make infringing activity apparent, (c) must act quickly to take down the infringing material once it has actual or apparent awareness, (d) must not benefit financially from the material if the ISP has the right to control the activity, and (e) must act expeditiously to remove the infringing material regardless of actual knowledge or apparent awareness and upon receiving proper notice under the DMCA.

D. Trademark Law

1. [13.14] Introduction to Trademark Law

A trademark is intended to distinguish the provider of goods or services from the provider's competitors. A trademark essentially designates the source of the goods or services as an individual entity. When a provider advertises a trademarked good or service, that provider is building the value of the trademark investment. *Platinum Home Mortgage Corp. v. Platinum Financial Group, Inc.,* 149 F.3d 722 (7th Cir 1998). Trademarks appear in the form of a word or words and either stand alone or appear along with a design, called a "composite mark." Trademarks can also appear in the form of slogans or symbols. Trademark law provides protection for the mark's owner when usage by a third party would cause confusion.

The Trademark Act of 1946 (Lanham Act), 15 U.S.C. §1051, *et seq.,* governs trademark claims. It requires claimants to show consumer confusion between the two disputed trademarks. However, a second manner of proving trademark infringement was introduced by the Federal Trademark Dilution Act of 1995, Pub.L. No. 104-98, 109 Stat. 985, which added 15 U.S.C. §1125(c), which requires proof only of a lessening of the capacity of a famous mark to identify and distinguish goods and services. The Dilution Act is available only to trademarks that are "famous" in the eyes of the court.

Trademarks differ from other types of intellectual property, such as patents and copyrights, in that trademark law is not derived from art. I, §8, of the United States Constitution. Federal law, therefore, is not preemptive in trademark law, and state and federally registered trademarks coexist equally with the common law trademark standards.

Federal registration of a trademark is prima facie evidence that the trademark is valid, the registering party owns the mark, and the registered owner has exclusive rights to use the mark. However, there is a major limitation on these rights: The Lanham Act states that filing an application to register a trademark confers a national right of priority against any party *except* for a party who has already used the mark prior to the filing. 15 U.S.C. §1057(c). "Using" a mark is, according to 15 U.S.C. §1127, usage in commerce or the ordinary course of trade and not merely a reservation of the mark. The mark must be used or displayed in the sale or advertising of goods or services.

The primary category of trademark cases arising through Internet usage is domain name disputes, as discussed in §13.15 below. *See, e.g., Minnesota Mining & Manufacturing Co. v. Taylor,* 21 F.Supp.2d 1003 (D.Minn. 1998) (defendant committed trademark infringement and violated federal anti-dilution statute by registering domain names substantially similar to plaintiff's registered trademark and then attempting to sell those domain names). However, other unique areas of trademark infringement that have sprouted from the Internet include metatag claims as well as framing and linking disputes. See discussion in §§13.19 and 13.20 below.

2. [13.15] Domain Name Disputes

Domain name disputes are perhaps the most senior of the Internet torts. Legally, these disputes are a form of trademark infringement. However, because of the burgeoning number of these cases and the fact that they affect every company operating a Web site, domain name disputes sometimes merit attention as their own unique cause of action.

Domain name disputes revolve around a class of entrepreneurs sometimes called "cybersquatters." This term was coined in *Intermatic, Inc. v. Toeppen,* 947 F.Supp. 1227 (N.D.Ill. 1996). Cybersquatters register domain names that contain the name of a famous commercial entity, such as abc.com, mcdonalds.com, or coke.com, and then attempt to sell the domain names to the target companies or, in some cases, to the target companies' competitors. Even the organizations charged with policing the Internet have fallen victim to cybersquatters, as the World Intellectual Property Organization and International Telecommunication Union have been stung by an individual who registered the sites "WIPO.com" and "ITU.com" and then posted them for sale on the Internet. See Makoto Ushida, *CYBERSLICE: What's in a Name? A Whole New Domain,* World Reporter — Asia Intelligence Wire (June 21, 1999) (available on Westlaw at 1999 WL 17699402).

Both a full trademark search and a full domain search must be conducted when adopting a domain name. Once a domain name is cleared, the company pays a registration fee to the accredited registrar. If the domain name has a conflict, the company can decide whether to litigate, negotiate, or choose another domain name. The company should also register with the U.S. Patent and Trademark Office and foreign patent and trademark authorities.

Despite the work of these institutions, disputes arising over domain names have become so rampant that legislation has been passed, as discussed in §13.18 below. Domain name disputes should be particularly significant to insurers because they may strike any company that operates a Web site. As with many cybertorts, domain name disputes are significantly more prevalent than traditional trademark disputes because companies that were once from disparate industries in opposite parts of a country are now placed side by side on the Internet when users search for a company by name. These suits are not limited by industry, nor are they limited by geography. To identify the potential for these types of risks, many insurers now require that a copy of a U.S. Trademark and Patent Office search for applicable domain names be attached to the insurance application.

One example of a domain name suit is *Avery Dennison Corp. v. Sumpton,* 189 F.3d 868 (9th Cir. 1999). In that case, the defendant operated an Internet e-mail service that sold "vanity" e-mail addresses to users from the thousands of addresses it had registered. Two such addresses in

the defendant's "last name" database were "avery.net" and "dennison.net." The office products company Avery Dennison sued, claiming that it had registered both of the terms "Avery" and "Dennison" and even sold products at "avery.com." The Ninth Circuit ruled that Avery Dennison did not adequately establish the "famousness factors" under the Federal Trademark Dilution Act, that the defendants were not utilizing the trademarks as a "commercial use," and that there was a genuine issue of fact as to whether a likelihood of confusion existed.

3. [13.16] Domain Name Dispute Resolution Methods

In the last year, companies pursuing domain name disputes have used two new weapons. The first is the mandatory administrative proceeding that has been implemented by the Internet Corporation for Assigned Names and Numbers (ICANN). See ICANN's Uniform Domain-Name Dispute-Resolution Policy page, www.icann.org/udrp (visited Mar. 4, 2002), which contains both the UDRP Policy and the Rules for Uniform Domain-Name Dispute-Resolution Policy (UDRP Rules). The second is the Anticybersquatting Consumer Protection Act (ACPA), Pub.L. No. 106-113, Div. B, §1000(a)(9), 113 Stat. 1536 (1999), codified at 15 U.S.C. §1114, *et seq.* These two tools allow trademark holders to pursue litigation without relying exclusively on historic trademark law.

a. [13.17] ICANN Dispute Resolution

An ICANN proceeding starts when a complainant sends a complaint to a registrant and to a specific "provider," which is a dispute resolution service approved by ICANN. The complaint must allege that the registrant's domain name is identical or confusingly similar to the trademark holder's mark and that the registrant registered and used the domain name in bad faith. This is easily proved in situations in which the domain name has been offered for sale at a profit.

A registrant can establish a defense if he or she used the name with a "bona fide offering of goods or services" before receiving notice of the dispute. UDRP Policy ¶4(c). A second defense is established if the registrant was commonly known by the domain name even without having registered the name as a trademark. *Id.* The last defense available is that the registrant may establish "a legitimate noncommercial or fair use" with no intent of commercial gain. *Id.*

The entire procedure is intended to cost approximately $1,000, to take place online, and to be completed within 45 days. While the federal government has made all registrants of top-level domains (*i.e.*, .com, .net, .org, etc.) subject to the ICANN rules, the party that institutes or submits to the proceeding does not necessarily lose its right to go to court and seek relief. *See Weber-Stephen Products Co. v. Armitage Hardware & Building Supply, Inc.*, 54 U.S.P.Q.2d 1766 (N.D.Ill. 2000) (court held that it was not bound by ICANN administrative proceeding). As the ICANN proceeding is new, coverage disputes may arise over whether attorneys' fees incurred in ICANN proceedings constitute defense costs under a comprehensive general liability (CGL) policy.

b. [13.18] Anticybersquatting Consumer Protection Act

If a trademark has acquired a famous or distinctive "secondary meaning," then the Anticybersquatting Consumer Protection Act creates a cause of action against any domain names

that are identical, confusingly similar, or dilutive of the famous mark. 15 U.S.C. §1129. However, the plaintiff must prove the defendant's "bad faith intent to profit" from the mark. ACPA states that there can be no bad faith if the registrant reasonably believed that using the domain name was a fair use or otherwise lawful. In February 2001, Bruce Springsteen lost his bid to evict a fan club from an Internet Web site sporting his name based on the fact that Springsteen failed to demonstrate that the fan club was using the name in bad faith. *Rock Star Springsteen Loses Cybersquatting Case,* The Industry Standard, Feb. 7, 2001 (available online at www.idg.net/go.cgi?id=420735).

Because locating the people who register certain domain names can be very difficult, if not impossible, ACPA also allows plaintiffs to bring an action in rem against the domain names themselves. In such in rem actions, the trademark holder must prove that it was unable to locate the registrant after using due diligence. Remedies for this type of action are limited to cancellation or transfer of the infringing domain name.

ACPA also creates a cause of action against those who register an individual's personal name as a domain name. While perhaps intended to protect celebrities, this statute does not require the plaintiff to be famous or to have used the name as a trademark.

The Second Circuit is the only federal circuit to issue a ruling relying on ACPA. *See Sporty's Farm L.L.C. v. Sportsman's Market, Inc.,* 202 F.3d 489 (2d Cir. 2000). In that action, the parties filed trademark dilution claims against each other stemming from each party's rights to the domain name "Sportys.com." Sportsman's contended that it had used "Sporty's" for years in its mail order sales of aviation equipment, tools, and home accessories and claimed that the plaintiff was a competitor who infringed on its trademark by using the domain name Sportys.com in 1996.

The Second Circuit found that, under the Act, the mark "Sporty's" was distinctive and, therefore, the domain name "sportys.com" was confusingly similar and a violation of the Act. The court further found that the use of the domain name was a bad-faith action by Sporty's Farm to profit from the use of that mark. Despite this bad-faith finding, the court did not order damages under ACPA because ACPA's statutory remedies were not in effect at the time the domain name was registered.

Further domain name disputes decided pursuant to ACPA include *Caesars World, Inc. v. Caesars-Palace.com,* 112 F.Supp.2d 505 (E.D.Va. 2000), and *Virtual Works, Inc. v. Network Solutions, Inc.,* 106 F.Supp.2d 845 (E.D.Va. 2000).

4. [13.19] Metatag Disputes

A metatag dispute is a classic illustration of a new kind of "cyberlitigation" for which trial judges and the advocates appearing before them have little experience. Metatag claims can strike any company that maintains a Web site. Metatags are key words embedded in the background code for each Web page by its creator. They are the hooks "behind the scenes" that reel a user to certain Web sites. When an Internet user uses a search engine (*e.g.,* Yahoo!) to find all Web pages involving "basketball," all Web pages with "basketball" in their "hidden" metatags will come up, regardless of whether the word "basketball" actually appears on the page. The trademark dispute ensues when a Web page incorporates another company's trademark in the "hidden" background code for its own Web page.

For example, in *Playboy Enterprises, Inc. v. AsiaFocus International, Inc.*, No. Civ. A. 97-734-A, 1998 WL 724000 (E.D.Va. Apr. 10, 1998), AsiaFocus used Playboy's federally registered trademarks "Playboy" and "Playmate" in the background code for its Web page. The court found that AsiaFocus had infringed on Playboy's trademark by intentionally misleading viewers into believing the site was connected with Playboy. *See also Playboy Enterprises, Inc. v. Calvin Designer Label*, 985 F.Supp. 1220 (N.D.Cal. 1997).

In a similar action, Playboy sued the search engine Excite for allowing a pornographic sex site to use the metatag "playboy." *Playboy Enterprises, Inc. v. Netscape Communications Corp.*, 55 F.Supp.2d 1070 (C.D.Cal.), *aff'd*, 202 F.3d 278 (9th Cir. 1999). The court ruled against Playboy, explaining that Playboy failed to establish that either Netscape or Excite used the trademarks in interstate commerce, obviating any confusion with the common usage name "playboy." The court also found that Netscape's and Excite's use of the word "playboy" was protected by the First Amendment and the fair use doctrine.

For further cases addressing metatag infringement, *see Bally Total Fitness Holding Corp. v. Faber*, 29 F.Supp.2d 1161 (C.D.Cal. 1998); *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*, 174 F.3d 1036 (9th Cir. 1999); *Nettis Environmental, Ltd. v. IWI, Inc.*, 46 F.Supp.2d 722 (N.D. Ohio 1999); and *Niton Corp. v. Radiation Monitoring Devices, Inc.*, 27 F.Supp.2d 102 (D.Mass. 1998).

5. [13.20] Linking/Framing

Another novel area of Internet trademark law is the "linking" and "framing" of Web sites. Linking allows a Web surfer to click on an icon and jump instantly to another site. Framing occurs when one site is linked to another site, but then the content on the second site is "framed" so that it appears that the second site is part of the original site, or that the two sites are "unified." There are also varying degrees of linking. One Web site can be linked to the "home page" of another, or "deep links" can be established that take Web surfers deep within a second site, bypassing advertising or pertinent information contained on the front pages of that site.

Linking and framing disputes can impact copyright as well as trademark laws. In *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F.Supp.2d 1290 (D. Utah 1999), the court held that a Web site operator was liable for contributory copyright infringement for having hyperlinks to Web sites containing copyrighted material and, therefore, encouraging others to view and copy the material.

E. Patent Disputes

1. [13.21] Introduction to Patent Disputes

There are three types of patents available in the United States. First, utility patents cover a new and useful process, machine, article of manufacture, or composition of matter. Second, design patents cover only ornamental features of an object and specifically exclude any functional aspects or features. Third, plant patents cover asexually reproduced plants.

Patent infringement claims may be seen in a new light after the decision in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.,* 149 F.3d 1368 (Fed.Cir. 1998), *cert. denied,* 119 S.Ct. 851 (1999). In this case, a bank sought to invalidate Signature's patent on a computerized accounting system used to manage mutual fund investment structures on the grounds that it was an unpatentable mathematical algorithm or business method. However, the court disagreed and reinforced the idea that computer methods of doing business can be statutorily protectable and patentable interests. This decision led to a new flow of computer businesses filing patents, which inevitably led to new patent infringement claims. For example, the U.S. Patent and Trademark Office granted 1,390 patents related to the Internet in the first half of 1999, compared with only 648 in all of 1997. Saul Hansell, *Web Sites Face Patent Disputes/Companies Are Claiming Rights to Broad Concepts of Online Business,* The Austin American-Statesman, Dec. 11, 1999, at A24.

The right to a patent is a "negative right"; *i.e.,* it excludes unauthorized copying or manufacture, use, sale, or offer for the subject patented. The patent term is 20 years from the date of the filing of the patent application. (In the past, patents were valid 17 years from the date of patent issuance.) There is a presumption of validity once a patent is issued, although it is a presumption rebuttable by clear and convincing evidence. A validity challenge can be based on three fronts. First, validity can be rebutted by showing that the patent is not novel. 35 U.S.C. §102. Second, a showing that the patented item is not useful can invalidate a patent. 35 U.S.C. §101. Third, the patent can be rebutted as invalid by showing that the patented item is "obvious" to someone skilled in the art when viewed in the light of the relevant prior art. 35 U.S.C. §103.

A patent holder can prove that his or her patent was infringed by showing that each and every element of the claimed invention or its equivalent is present in the infringing item. *See Medtronic, Inc. v. Cardiac Pacemakers, Inc.,* 721 F.2d 1563 (Fed.Cir. 1983); *Wilson Sporting Goods Co. v. David Geoffrey & Associates,* 904 F.2d 677 (Fed.Cir. 1990). Winning one patent lawsuit does not immunize a product or company from future lawsuits, as patents can be challenged repeatedly.

2. [13.22] Examples of Patent Cases in Cyberspace

Recently, in *Amazon.com, Inc. v. Barnsandnoble.com, Inc.,* 239 F.3d 1343 (Fed.Cir. 2001), Amazon.com brought a patent infringement suit against Barnesandnoble.com for allegedly infringing Amazon's patent on its "Express Lane" method of procuring payment from customers over the Internet. Amazon's method allows customers to avoid the traditional "shopping cart" step in ordering products via the Internet. With the "Express Lane" software, customers use a "single action" system that saves time when ordering goods. Barnesandnoble.com initiated a system that allowed customers to complete a purchase order in a single transaction. As a result, Amazon initially obtained injunctive relief prohibiting Barnesandnoble.com from utilizing the system. On appeal, the court reversed, holding that the possible invalidity of Amazon's patent based on obviousness created a less than likely chance of success on the merits for Amazon.

This case illustrates the potential for countless disputes involving methods of doing business on the Internet. As the volume of commerce on the Internet increases, the number of coverage disputes involving insureds' infringement of patented methods of doing business on the Internet will only increase as well.

III. [13.23] FIRST-PARTY CYBERCLAIM RISKS

First-party insurance policies typically provide coverage for business interruption losses resulting from "direct physical loss of or damage to covered property." In the cyberworld, an insured's business can be interrupted without the cause being one of the "traditional" agents of physical damage such as fire, flood, or lightning. Instead, the causes of business interruption in cyberspace are agents like computer viruses/worms, cracking or hacking of an insured's database, and simple computer systems failure.

Statistics show that the examples listed below are becoming more common and are threatening an increasingly large variety of insureds. A recent survey of 643 companies conducted by the Computer Security Institute concluded:

a. Seventy-four percent of the respondents suffered losses stemming from a breach of computer security.

b. Of those companies, only 273 were able to quantify their losses. These losses exceeded $265 million.

c. Sixty-six respondents were able to quantify their loss suffered because of computer-related theft of intellectual property. These losses totaled over $66 million.

A. [13.24] Denial of Service Attacks

A denial of service attack occurs when a Web site's servers are bombarded with e-mails requesting information. When the server responds, the attacker's system sends another barrage of requests. These responses generate new waves of increased requests until the insured's computer system is slowed significantly or ultimately crashes. These types of attacks have come to be known as "denial of service" attacks or "ping storms."

Although systems targeted by ping storms usually recover within a day, the loss of even a few hours' revenue can have serious consequences for many businesses. For example, an apparently coordinated series of ping storms in February 2000 affecting eBay, Amazon.com, Buy.com, Yahoo!, CNN.com, E*Trade, and other Web sites resulted in over $1 billion in capitalized losses, and the lost revenue and advertising dollars totaled over $100 million, according to the consultant firm the Yankee Group. The cost to the affected companies for upgrades of their systems was estimated at $100 million – $200 million.

B. [13.25] Computer Hacking

The Internet is a comparatively safe haven for thieves and other criminals, which makes it a breeding ground for first-party losses. According to George S. Sutcliffe, E-COMMERCE INSURANCE AND RISK MANAGEMENT (Standard Publishing Corp. 2000), there are at least 440 hacker bulletin boards and 1,900 Web sites giving hacking instruction. A hacking survey conducted by Assurex E-Risk (available online at www.assurex.com/otbtemp/newspecial.asp) showed:

1. Twenty-one percent of large network systems have been attacked by hackers.

2. Fifteen percent of large network systems experienced business interruptions as a result of computer hacking.

3. Forty percent of large network systems have faced an increase in attacks by hackers.

One emerging hacking scheme is an online price-switching scam. Hackers find vulnerable sites that utilize online shopping carts and program the code that drastically reduces the price they are paying for the goods. As many as one third of all shopping cart applications at Internet retailing sites are vulnerable to the price switching scam. See Laura Lorek, *E-Commerce Insecurity,* Interactive Week, Apr. 20, 2001 (available online at http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2709873,00.html).

Computer hacking has even become a sword for political organizations. Amid the U.S.-Chinese tensions in April 2001, teams of computer hackers defaced Chinese Web sites. In response, Chinese hackers attacked several American political and corporate Web sites in May 2001. Michelle Delio, *Crackers Expand Private War,* Wired News, Apr. 18, 2001 (available online at www.wired.com/news/business/0,1367,43134,00.html).

C. [13.26] Computer Viruses/Worms

Viruses and worms will likely lead to a staggering number of first-party claims. Viruses are strings of codes that attach to standard programs. They replicate themselves and consume all available memory. Viruses can erase files stored on the hard drive or on the server. They are passed through e-mail or other linked systems such as networks. Worms are similar to viruses but unlike viruses worms do not need a host to spread.

On May 4, 2000, the "I LOVE YOU" virus affected computer systems globally from Britain's House of Commons to the Asian Wall Street Journal. When a recipient attempted to open the "I LOVE YOU" e-mail, it promptly sent itself to the first 300 e-mail addresses in the user's contact list and also proceeded to delete a wide range of files including pictures, music files, and programs written in languages such as Java and Visual Basic. Experts have estimated business losses as high as $5 billion dollars as a result of the virus.

D. [13.27] Power Disruptions

Power disruptions include power fluctuations and the better-known power outages. There are two basic types of power fluctuation: (1) power surge/spike; and (2) power sag. A typical American home or business is wired for 110 – 130 volts. A power surge/spike is a sudden expulsion of electricity that can reach up to 6,000 volts. Sources of surges/spikes include lightning, cycling of heating systems, air conditioners, and refrigerators, and use of power tools. A power sag is an under-voltage of an electric line of 15 percent or more. Long-term under-voltage is termed a "brownout." Even a ten-millisecond sag can cause a personal computer to malfunction. When power returns, there is often a surge/spike. The fluctuations in power can break down insulation and components in appliances, and they may eventually collapse.

A power outage in San Francisco in 1998 halted trading on the San Francisco floor of the Pacific Exchange for almost an entire day while lighting and computers were unavailable. Some trading occurred through the Los Angeles location, but the outage at San Francisco was estimated to cost millions of dollars in lost business.

Increasingly, first-party technology claims are arising from power failures and fluctuations. Three types of damages can be attributed to power fluctuations and failures: (1) physical damage to hardware; (2) damage to data; and (3) corruption of data in transition at the time of the power difficulty.

E. [13.28] Hardware, Software, or Systems Failures

Often unexplained and almost always spontaneous, system failures can be detrimental to a dot-com or Web site-enriched brick-and-mortar business. The causes of the failure cannot always be specified, but the result is far too recognizable: significant loss of profits as business comes to a halt and technicians are frantically called to repair the damage.

Amazon.com's site went down in July 2000 for 40 minutes due to what was described as a "hiccup" in the system just before its second-quarter financial results were posted. The site again went down on the busiest shopping day of the year, November 24, 2000, the day after Thanksgiving Day. Just a few weeks later, another glitch in Amazon's system caused the Web site to crash for 43 minutes. The outages were thought to have been caused by trying to run two incompatible programs at the same time.

NASDAQ halted trading on three separate occasions to repair a glitch in its price quote engine. The stock exchange was silenced for 11 minutes while technicians restored service. Businesses trading on NASDAQ lost unreported profits due to the exchange closing.

On January 3, 2001, the seasoned e-commerce giant eBay suffered an 11-hour site outage due to a series of failures from both its primary and backup systems. The company extended all affected auctions by 24 hours and credited associated fees to its customers.

IV. [13.29] THIRD-PARTY COVERAGE ISSUES

In the past, insureds have sought coverage under CGL policies for defamation, invasion of privacy, and copyright infringement under the "advertising injury" provision, which specifically enumerated these offenses. Insureds seeking coverage for similar offenses that were not specifically enumerated (such as patent or trademark infringement) also looked to the "advertising injury" provision by arguing that patent and trademark infringement were intended to be covered under the provision's additional coverage for "infringement of slogan" or "piracy" or "misappropriation of style of doing business."

A. [13.30] Cybercoverage Under CGL Advertising Injury

For many insureds operating a brick-and-mortar business, the "advertising injury" coverage in a CGL policy provided coverage that was often less significant than the coverage provided for

liability resulting from "bodily injury" or "property damage." A company selling shoes or hardware was not likely to find itself embroiled in litigation relating to advertising injuries. In the new millennium, however, this may well change. Even aside from pure Internet businesses, most old-line companies now have a Web page, engage in e-commerce, or otherwise have a presence on the World Wide Web. Because of the inherently public nature of these activities, many companies could well face increasing exposure to the torts associated with "advertising injury."

1. [13.31] Is Internet Use an Advertising Activity?

Traditionally, standard CGL policy forms require that the enumerated offenses be "committed in the course of the named insured's advertising activities" (see 1973 Insurance Services Office (ISO) CGL Form) or "committed in the course of advertising the named insured's goods, products or services" (1985 ISO form). In 1988, ISO amended its policy form so that coverage is provided for advertising injury if the enumerated offenses were committed in the named insured's "advertisement." The 1998 ISO form defines "advertisement" as

> [a] **notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purpose of attracting customers or supporters.**

With respect to enumerated offenses that do not involve the Internet, most courts agree that "wide-spread distribution of the [offending] material to the public at large" satisfied the requirement that the enumerated offense take place "in the course of the named insured's advertising activities," "in the course of advertising the named insured's goods, products or services," or "in the named insured's advertisement." *See Playboy Enterprises, Inc. v. St. Paul Fire & Marine Insurance Co.,* 769 F.2d 425, 429 (7th Cir. 1985). The debate, however, was whether more tailored communication, even one-on-one solicitation, would also satisfy the "advertisement requirement." *See, e.g., Elan Pharmaceutical Research Corp. v. Employers Insurance of Wausau,* 144 F.3d 1372, 1378 (11th Cir. 1998) (rejecting insurer's argument that coverage for advertising injury applies only to broad dissemination of offending material, court found that policy contained "no express requirement that the insured must direct its advertising activity either towards the general public or actual consumers").

In the context of advertising injury claims arising over the Internet, this debate will likely lose much of its relevance, as an enumerated offense taking place on the Web is disseminated to an extraordinarily large audience. Instead, the issue the courts will likely struggle with is whether any enumerated offense taking place on the Web automatically satisfies the requirement that the enumerated offense take place "in the named insured's advertisement." 1998 ISO Form. Is it possible to have a Web page that is *not* an "advertisement"?

Although it may appear that every Web page inherently markets or publishes information about the host's goods, products, or services for the purpose of attracting customers or supporters, at least one court has found to the contrary. In *Winslow, King, Richards & Co. v. Royal Insurance Company of America,* 46 Mass.App.Ct. 1106, 706 N.E.2d 729 (1999) (table), the owner of a copyright to a publication entitled "Job Hunting Guide" alleged that its copyright was being infringed by a Web site that advertised a publication entitled "Career Search Guide." Although the court acknowledged that the Web site's publication was distributed to clients with the hopes

of increasing the Web page's business, the court held that the information contained in the Web page's guide was strictly informational and did not "proclaim the qualities of a product" or engage in "wide dissemination of information [which is] typically the objective of advertising." Accordingly, the court found that the enumerated offense did not occur "in the course of advertising."

In the coming years, courts will be forced to draw the line between Internet advertising and non-advertising.

2. [13.32] Copyright Coverage Questions

A Fifth Circuit ruling demonstrates the significant hurdles insureds may face when attempting to obtain coverage for copyright liability under an advertising injury provision. In *Delta Computer Corp. v. Frank*, 196 F.3d 589 (5th Cir. 1999), Delta Computer Corporation filed suit against Telephone Electronics Corporation (TEC) alleging that TEC infringed on certain copyrighted software that allowed the company to record the identity of long-distance callers and the length of the calls and then generate long-distance resale bills. The program also specifically allowed for the inclusion of advertising on the text of the bills.

TEC's insurer denied coverage and refused to participate in the defense of the matter. After TEC settled the underlying case, it sued its insurer for coverage. The court granted summary judgment in favor of the insurer because there was no causal connection between the copyright claim and TEC's advertising activities. The underlying complaint did not complain of any injuries suffered in the course of TEC's advertising. The court held that TEC's claim was essentially for infringement of the copyrighted software program, which was developed primarily for billing purposes, not for advertising.

There may also be coverage implications stemming from the recent Napster decision. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Although Napster did not tender its defense or seek indemnification from its insurer, it is conceivable that an entity in Napster's position could seek coverage under the advertising injury portion of a policy. An argument could be made that the distribution and transmission of copyrighted material on the Napster site occurred within the course of advertising, especially if Napster was profiting from selling banners on its Web site. In such case, the transmission of the music would be enhancing the value of space on Napster's Web page, just as advertising would.

3. [13.33] Patent Coverage Questions

Most courts that have addressed the application of "advertising injury" to patent infringement claims have found that no coverage exists for the insured. Because advertising injury provisions specifically enumerate certain types of offenses (*e.g.*, libel, slander, copyright), most courts have held that those offenses not specifically enumerated (*e.g.*, patent infringement) are not intended to be covered. One such court denied an insured's $48 million insurance claim relating to a patent dispute involving office "power supply modules" because the patent infringement allegations were not specifically covered offenses in the policy's "advertising injury" definition. *See Herman*

Miller, Inc. v. Travelers Indemnity Co., 162 F.3d 454 (6th Cir. 1998) (court found that patent claim was not covered because while policy included copyright infringement in its definition of "advertising injury," it did not mention patent infringement even though it could easily have been added had parties so intended).

However, some courts have ruled that patent infringement claims may fall within the meaning of "piracy" as specifically enumerated in the pre-1985 ISO definition of "advertising." *See, e.g., Union Insurance Co. v. Land & Sky, Inc.*, 247 Neb. 696, 529 N.W.2d 773 (1995); *National Union Fire Insurance Company of Pittsburgh, Pennsylvania v. Siliconix, Inc.*, 729 F.Supp. 77, 79 – 80 (N.D.Cal. 1989) (court, however, ultimately found no coverage because there was no nexus between patent infringement and loss at issue).

There does not appear to be anything inherently different or novel about claims of patent infringement on the Internet that would alter or reverse the trend that most courts have followed in traditional patent infringement disputes that there is no coverage for such disputes under standard CGL policies.

4. [13.34] Invasion of Privacy Coverage Questions

In addition to coverage for "advertising injury," insureds facing cyberclaim risks may look to the "personal injury" coverage granted by standard CGL policies. In most CGL forms, the advertising injury and personal injury provisions each list enumerated offenses that are covered, and each usually lists "oral or written publication of material that violates a person's right of privacy." The 1998 ISO form combines both types of coverage in a "personal and advertising injury" provision.

In order for coverage to be found under this "privacy coverage" in the 1985 form, the privacy violation typically must arise out of, and be caused by, an advertisement of the insured's goods. However, under the 1998 ISO form, written publication of material that violates a person's right of privacy need not necessarily arise out of, and be caused by, an advertisement. The difference between the 1985 and 1998 forms is a result of the fact that personal injury and advertising injury have been combined. In the 1998 ISO form, the GCL policy provision covers

> **written publication of material that violates a person's right of privacy; use of another's advertising idea in your advertisement; or infringing upon another's copyright, title or slogan in your advertisement.**

Read literally, this provision does not appear to require written publication of material that violates the right of privacy to be made in an "advertisement."

The change in ISO policy language directly implicates invasion of privacy litigation based on Internet activities. For example, the unannounced placing of a cookie file on a user's computer would probably not meet the 1985 ISO form requirement that the oral or written publication arise from an "advertisement." However, under the 1998 ISO form, insureds may argue that such conduct constitutes an invasion of privacy because it is a written publication of material that may violate a person's right of privacy. Likewise, insureds may contend that the sale of individuals' names or Internet surfing habits triggers coverage under the 1998 policy form. To date, however, there are no reported decisions in this area.

B. [13.35] Coverage for Cyberclaims Under "Property Damage" Coverage Grant

In addition to the advertising injury and personal injury coverage grants, CGL policies also provide coverage for liability arising out of "property damage." CGL policies typically define "property damage" in terms of physical damage to a third party's "tangible property." With respect to cyberclaims, the issue is whether the loss of computer data or other types of corruption of digital information constitutes physical damage to tangible property sufficient to trigger coverage under the "property damage" coverage grant of a CGL policy.

Courts in Illinois have not addressed this issue. In the context of first-party coverage disputes, however, courts in other jurisdictions have reached mixed results. *See American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, No. Civ. 99-185 TUC ACM, 2000 WL 726789, (D.Ariz. Apr. 19, 2000) (lost data constituted "tangible property"); *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195, 198 (8th Cir. 1995) (Missouri law) (court implied data is not "tangible property" within meaning of CGL policy).

Because of uncertainty in how courts will address the issue, ISO submitted its GL-2000 revisions for approval to numerous state insurance regulators. In these revisions, ISO proposed adding the following sentence to the definition of "property damage":

> **For the purpose of this insurance, computerized or electronically stored data, programs or software are not tangible property.**

The ISO Background Comments submitted along with the proposed changes state:

> **The CGL policy provides coverage for physical injury to tangible property, such as computer hardware, but not for lost data. We recognize that there may be other opinions on this subject, but we have drafted the property damage definition to reflect our position. Specific wording to set forth this approach is employed and an option for coverage for this exposure is being developed.**

Significantly, the above proposal applies only to general liability forms and, therefore, will not immediately affect the first-party risks. However, should the above wording be accepted by the states, it is likely that eventually first-party property policies will include similar definitions of "property damage." The newest insurance products on the market, aimed specifically at e-business risks, have taken the opposite approach by specifically including coverage for data loss rather than excluding it.

C. [13.36] Worldwide Coverage Territory Provisions

With the sudden ability of even the smallest insured, operating from a small apartment, to reach a worldwide audience on the Internet, coverage disputes increasingly will involve claims arising outside the United States. Companies operating on opposite sides of the world may now confuse consumers if they maintain overlapping intellectual property on the Internet. These worldwide exposures give new importance to the often overlooked "coverage territory" provision.

1. [13.37] Examples of Worldwide Claims

One example of the complexities of international e-commerce arose when the German Justice Ministry became aware that Amazon.com was violating German law by delivering English language versions of the banned anti-Semitic books MEIN KAMPH and THE PROTOCOLS OF THE ELDERS OF ZION into Germany. Amazon.com eventually relented and stopped selling these titles in Germany. In a similar scenario, Saudi Arabia announced in August 2000 that it was blocking access to Yahoo! clubs because many of the chat and message board communities set up by Yahoo! enabled users to bypass Saudi filters that were intended to prevent citizens from accessing pornography or other types of sites deemed offensive. Yahoo! was also sued in France recently for selling prohibited Nazi paraphernalia on its auction pages.

In December 1999, an Australian Web marketing business named Double Click Australia (DCA) announced that it was suing the world's leading online advertising company, America's DoubleClick, Inc. The case was filed in the federal court of Australia. The suit alleges that DCA established its name in 1987, whereas the U.S. corporation began only in 1996. The complaint alleges market confusion and violations of Australia's Trade Practices Act of 1974.

2. [13.38] Coverage Interpretation

In discussing the geographic scope of coverage available, there are two significant points: (a) Where does the alleged offense need to have occurred? (b) Where does the claim need to be brought? Traditionally, general liability policies cover only claims that arise in the "coverage territory," as defined by the policy. Some policies define this territory as the United States, while other policies may define the coverage territory to include not only the United States but also a few selected countries or territories where the insured carries out its business. In the Internet area, however, the coverage territory must be worldwide. After all, if a company in Japan is defamed by an Iowa resident who posted a message on an Internet message board hosted in Germany, serious questions arise as to where this tort "occurred." Similarly, because a claim may be brought in any one of these jurisdictions, it is important to note whether a policy restricts its coverage to claims brought in the United States.

For example, the Chubb Safety'Net Internet Liability Insurance Policy states: "Coverage under this Policy shall extend to Internet Activities occurring anywhere in the world, but only with respect to Claims made against the Insureds in the United States, its territories or possessions, or Canada." A similar definition of "coverage territory" is also used in the e-Sher policy. These provisions may be contrasted with the "Where Coverage Applies" provision in American International Group's netAdvantage Internet Media Liability Policy, which states, "We cover wrongful acts that occur, and claims that are brought, anywhere in the world." The subtle differences in these "cyberpolicies" may be significant as worldwide liability becomes the rule and not the exception.

V. FIRST-PARTY COVERAGE ISSUES

A. [13.39] Physical Loss or Damage

Traditional first-party policies apply only to "direct physical loss of or damage to covered property . . . caused by or resulting from any covered cause of loss." Most courts have interpreted this language to require some proof of physical or tangible damage to the insured's property. When applied to "cyberlosses," however, questions arise when an insured's computers lose the ability to network, or when important data is erased but the computers continue to function. Has the insured suffered a physical loss to its own property? After all, the computers are not damaged in any way; only data has been lost.

In order to recover for technology losses under first-party policies, the first argument many policyholders make is that the policy does not require "physical damage" despite the phrase "direct physical loss of or damage to" property. While it may appear logical that the word "physical" modifies "damage" as well as "loss," insureds who are seeking coverage for data-related losses argue that the policy requires them to prove only either (1) "physical loss" or (2) "damage." Most courts have rejected this argument and have required insureds to prove "physical loss" or "physical damage." *See HRG Development Corp. v. Graphic Arts Mutual Insurance Co.*, 26 Mass.App.Ct. 374, 527 N.E.2d 1179 (1988) ("physical" applied to both "loss" and "damage"); *Great Northern Insurance Co. v. Benjamin Franklin Federal Savings & Loan*, 953 F.2d 1387 (9th Cir. 1992) (table) (court held that phrase "direct physical loss or damage" could have been intended only to exclude indirect, nonphysical losses).

B. [13.40] Is Loss of Use Property Damage?

In an attempt to argue that lost computer functionality constitutes "physical damage" or "physical loss," policyholders often rely on *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, No. Civ. 99-185 TUC ADM, 2000 WL 726789 (D.Ariz. Apr. 19, 2000). This case presented what could become one of the most common first-party coverage questions: When a party loses computer data due to an unforeseen act, does that lost data constitute "physical damage" necessary to trigger coverage under a first-party policy?

In *Ingram Micro,* the computer facility responsible for database maintenance of all daily transactions was hit by a power outage. Power to all computers and telephones stopped for half an hour, causing the loss of all programming data in the three mainframe computers. Even after these computers were back up, the loss of a custom computer data configuration (caused by the power outage) prevented the mainframe computers from connecting with other Ingram Micro locations in the U.S. and Europe. Ingram argued that the loss of functionality in this system constituted "physical damage." The insurer responded that even though the custom data configuration had been lost, the equipment's inherent ability to function remained intact and, therefore, the system was not physically damaged.

The district court ruled that physical damage is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality. In arriving at its conclusion, the district court analogized to state criminal statues that define "damage" for purposes of electronic crimes to include the alteration or deletion of any part of a computer system.

Contrary to the *Ingram Micro* decision, numerous other courts have refused to equate the loss of intangible data with physical damage to property. *See Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195, 198 (8th Cir. 1995) (court implied that information on computer disks is not tangible property under CGL policy); *Magnetic Data, Inc. v. St. Paul Fire & Marine Insurance Co.*, 442 N.W.2d 153, 156 (Minn. 1989) (insured's erasure of third party's computer disks was not covered under insured's liability policy); *Ronnen v. Commissioner*, 90 T.C. 74 100 (1988) (data stored on computer disks was not tangible property); *Retail Systems, Inc. v. CNA Insurance Cos.*, 469 N.W.2d 735 (Minn. 1991) (court held that computer data was tangible property only because it was integrated onto tangible piece of computer tape that was lost or destroyed); *Peoples Telephone Co. v. Hartford Fire Insurance Co.*, 36 F.Supp.2d 1335 (S.D.Fla. 1997) (court held mobile telephone identification numbers that were misappropriated and sold to third parties who then "cloned" phones were not tangible property under employee dishonesty policy); *Seagate Technology, Inc. v. St. Paul Fire & Marine Insurance Co.*, 11 F.Supp.2d 1150 (N.D.Cal. 1998) (court would not entertain allegations of loss of data resulting from insured's defective disk drive because it could not be considered loss of tangible property due to lost data or loss of use of computer unless there was also physical injury to computer itself); *Centennial Insurance Co. v. Applied Health Care Systems, Inc.*, 710 F.2d 1288 (7th Cir. 1983) (although finding coverage, court noted that there was open question as to whether loss of data from defective computer hardware constituted damage to tangible property under CGL policy).

2005 Supplement To:

COVERAGE ISSUES RAISED BY E-MAIL AND THE INTERNET

Daniel I. Graham, Jr.
BATES & CAREY LLP
191 N. Wacker Drive, #2400
Chicago, IL 60062
(312) 762-3100

II. [13S.2] THIRD-PARTY CYBERCLAIM RISKS

The section is revised:

Insureds faced with cybertort claims often have sought defense and indemnification with respect to these claims under their liability policies' "advertising injury" coverage, as defined in the pre-1998 commercial general liability (CGL) coverage forms published by the Insurance Services Office (ISO), or "personal and advertising injury" coverage, as defined in the ISO's post-1998 CGL coverage forms.

The ISO's pre-1998 CGL forms generally define "advertising injury" to mean injury arising out of several enumerated offenses, which must be committed in the course of advertising the named insured's goods, products, or services in order to implicate "advertising injury" coverage. The post-1998 CGL forms combined many of the offenses contained in the earlier CGL forms' definitions of "personal injury" and "advertising injury" to create a series of enumerated offenses, some of which must be committed in an "advertisement" to implicate coverage. The definition of "advertisement" contained in the 2001 CGL form expressly acknowledges that the term "advertisement" can, in certain instances, encompass Internet means of communication.

In evaluating whether a particular cybertort claim implicates a liability policy's "advertising injury" or "personal and advertising injury" coverage, a court will, as a threshold matter, assess whether one of the enumerated offenses potentially encompasses the wrongful conduct complained of. With this in mind, this chapter discusses categories of wrongful conduct on which cybertorts are commonly based.

IV. THIRD-PARTY COVERAGE ISSUES

A. Cybercoverage Under CGL Advertising Injury

1. [13S.31] Is Internet Use an Advertising Activity?

Add after the bold quotation on p. 13-21:

The ISO later refined its definition in the 2001 CGL form, in which "advertisement" is defined to include notices that are published on the Internet.

The last full paragraph on p. 13-21 is replaced:

Several courts believe that the posting of a Web site implicitly constitutes advertising. For example, finding Amazon.com's alleged infringement of patented music preview technology on its Web site to have been committed "in the course of advertising," the court, applying Washington law, explained, "Amazon's website exists for the purpose of promoting products for sale to the public. This is advertising." *Amazon.com International, Inc. v. American Dynasty Surplus Lines Insurance Co.,* 120 Wash.App. 610, 85 P.3d 974, 977 (2004). *See also Central Mutual Insurance Co. v. StunFence, Inc.,* 292 F.Supp.2d 1072 (N.D.Ill. 2003) (applying Illinois

law, court held that insured's alleged use of competitor's trademark on its Web site provided sufficient link between insured's advertising and complainant's injury for purposes of implicating "use of another's advertising idea" offense in "personal and advertising" coverage); *Specific Impulse, Inc. v. Hartford Casualty Insurance Co.,* No. 5:02-cv-02849-JW, 2002 U.S.Dist. LEXIS 25600 (N.D.Cal. Sept. 17, 2002) (applying California law, the court held that insured's Web site constituted "advertisement," which policy defined to mean, "Any other publication that is given widespread public distribution"); *Westfield Cos. v. O.K.L. Can Line,* 155 Ohio App.3d 747, 804 N.E.2d 45, 51, 2003 Ohio 7151 (2003) (although complainant did not use words "advertisement" or "advertising" in allegations against insured, insurer had duty to defend insured against trade dress infringement claims under "advertising injury" coverage because Web pages from insured's Web site depicting for sale allegedly infringing product deemed "advertising under any definition").

Add after the carryover paragraph at the top of p. 13-22:

The distinction between an informational posting on a Web site and a marketing-related posting was also addressed by the court in *Teletronics International, Inc. v. CNA Insurance Co.,* 302 F.Supp.2d 442 (D.Md. 2004) (applying Maryland law), *rev'd,* 120 Fed.Appx. 440 (4th Cir. 2005) (unpublished). The coverage dispute in *Teletronics* arose from a copyright infringement lawsuit in which an insured manufacturer was alleged to have, among other things, infringed a competitor's copyrighted installation manual, which the insured then posted on its Web site. The insured sought a defense under its liability policy's "advertising injury" coverage, which encompassed copyright infringement committed "in the course of advertising" the insured's goods, products, and services. The insured maintained that because it had posted an electronic copy of the allegedly infringing manual on its Web site to provide potential customers with information about its amplifiers, its conduct was advertising sufficient to trigger a defense under the "advertising injury" coverage of its policy.

The district court dismissed the insured's argument that the posting of the installation manual on its Web site constituted advertising. In doing so, the court explained that the mere presence of the manual on the Web site, which appeared to serve an informational purpose, did not convert the posting into advertising. The district court explained that to conclude otherwise, it would have to find that anything posted on a company's Web site would constitute advertising. The Fourth Circuit Court of Appeals disagreed and reversed on appeal, emphasizing that the posting of material on a Web site is not "advertising" unless its purpose is to generate or solicit business. Finding that the insured had posted the allegedly infringing manual on its Web site to promote the insured's sale of amplifiers, the Fourth Circuit held that the insured's activities constituted "advertising" and therefore triggered the insurer's duty to defend.

Add at the end of the section:

While an Internet posting may be considered an "advertisement," it is clear that unless an insured's liability arises out of one of the offenses enumerated in a policy's definition of "advertising injury" or "personal and advertising injury," the insurer will be found to have no defense or indemnity obligations to the insured under the policy. For example, in *Rombe Corp. v. Allied Insurance Co.,* 128 Cal.App.4th 482, 27 Cal.Rptr.3d 99 (2005), an insured sought defense

and indemnification under the "advertising injury" coverage of its policy with respect to a complaint that the insured had misappropriated trade secrets and customer lists. In support of its claims for coverage, the insured relied on a press report posted on the Internet that discussed the breakfast that the insured hosted to solicit new clients. The *Rombe* court, applying California law, acknowledged that a press report disseminated on the Internet might be an advertisement, as contemplated by the policy's "advertising injury" coverage. Nevertheless, the court held that the insurer had no obligation to the insured with respect to this coverage because the record before it did not suggest that the insured's liability in the underlying action arose out of an offense for which the policy provided "advertising injury" coverage.

2. [13S.32] Copyright Coverage Questions

Add at the end of the section:

Although an insured may face hurdles in attempting to obtain coverage for copyright liability under the "advertising injury" coverage, as long as an insured can demonstrate that the copyright infringement was committed, or alleged to have been committed, in the course of advertising, as required by pre-1998 CGL forms, or in an "advertisement," as required by post-1998 CGL forms, its chances to obtain coverage increase significantly. *See, e.g., Teletronics International, Inc. v. CNA Insurance Co.,* 120 Fed.Appx. 440 (4th Cir. 2005) (unpublished) (applying Maryland law, court held that, because insured had posted installation manual that allegedly infringed competitor's copyright on its Web site for promotional purposes, infringement was allegedly committed in the course of advertising such that insurer had duty under "advertising injury" coverage to defend insured in underlying action), *rev'g* 302 F.Supp.2d 442 (D.Md. 2004); *Specific Impulse, Inc. v. Hartford Casualty Insurance Co.,* No. 5:02-cv-02849-JW, 2002 U.S.Dist. LEXIS 25600 (N.D.Cal. Sept. 17, 2002) (although insurer maintained that it had no duty under "personal and advertising injury" coverage to defend insured in underlying copyright infringement lawsuit because alleged infringement was not committed in course of advertising, court, applying California law, held allegations that insured had posted its allegedly infringing works on Web site were sufficient to satisfy requisite advertising nexus).

2$_1$. [13S.32A] Trademark Coverage Questions

New section:

Insureds have long sought coverage for trademark liability disputes under the "advertising injury" and "personal and advertising injury" coverages of their liability policies. Domain name disputes, which often involve claims of trademark infringement, present unique coverage issues. In *State Auto Property & Casualty Insurance Co. v. Travelers Indemnity Company of America,* 343 F.3d 249 (4th Cir. 2003), for example, the Fourth Circuit Court of Appeals, applying North Carolina law, concluded that an insurer had a duty to defend its insured in a trademark infringement suit brought by Nissan Motor Company, Ltd. and Nissan North America, Inc. (collectively "Nissan"). Nissan alleged that the insured, knowing that Nissan already owned the NISSAN trademark, proceeded to register the domain names "www.nissan.com" and "www.nissan.net." Nissan later discovered that the insured was selling to various automobile and

merchandising companies, advertising space on its Web sites, which utilized a logo that allegedly closely resembled Nissan's, in addition to offering Internet access, hosting, and networking capabilities to interested Web site visitors.

The insured tendered the Nissan complaint to its insurer, seeking a defense against Nissan's claims under liability policies that provided coverage for "advertising injury," which the policies defined to include "misappropriation of advertising ideas or style of doing business" committed in the course of advertising the insured's goods, products, or services. The insurer maintained that it had no defense or indemnity obligations under its policies.

The insurer argued that even if Nissan's trademark claims sought damages for the misappropriation of advertising ideas or style of doing business, the insurer had no obligations to the insured under the "advertising injury" coverage because Nissan complained of the insured's use of the NISSAN trademark in its registration of domain names. The insurer reasoned that because domain names are simply Web site addresses, Nissan's injuries could not have been committed in the course of advertising, as required by the policy.

The Fourth Circuit rejected the insurer's argument. The court maintained that the insured's use of a domain name to lead consumers to its competing Web sites, which the insured was alleged to have utilized for advertisement purposes, was clearly an act that was committed in the course of advertising. Furthermore, the court observed that among Nissan's theories of liability, it had challenged the insured's use of an allegedly infringing logo on the Web sites. As a result, the Fourth Circuit explained that any injuries Nissan suffered as a result of the insured's allegedly infringing logo on its Web sites were implicitly committed in the course of advertising. Dismissing the insurer's other coverage defenses, the Fourth Circuit held that the insurer was obligated to defend the insured against Nissan's trademark infringement lawsuit under the policies' "advertising injury" coverage. *See also CAT Internet Services, Inc. v. Providence Washington Insurance Co.,* 333 F.3d 138 (3d Cir. 2003) (applying Pennsylvania law, court held that, because insured Internet domain name owner allegedly used infringing domain name as means of gaining customers, duty to defend insured against trademark infringement claim existed under "misappropriation of advertising ideas" offense of insurer's "advertising injury" coverage).

3. [13S.33] Patent Coverage Questions

The last paragraph is replaced:

Although most courts have found that a liability policy's "advertising injury" coverage does not encompass patent infringement claims, a Washington appellate court found that the nuances of Internet advertising required it to reach a different conclusion. In *Amazon.com International, Inc. v. American Dynasty Surplus Lines Insurance Co.,* 120 Wash.App. 610, 85 P.3d 974 (2004), Amazon.com International sought defense and indemnification under the "advertising injury" coverage of its liability policy with respect to a patent infringement lawsuit alleging that Amazon.com had infringed a software manufacturer's patented interactive technology to preview music products over the Internet. Amazon.com tendered its defense in the patent infringement action to its general liability and excess insurers. Unlike the excess policy, the general liability

policy did not expressly provide coverage for patent infringement. However, the general liability policy's "advertising injury" coverage listed among its enumerated offenses the "misappropriation of advertising ideas" committed in the course of advertising.

Both insurers refused to defend Amazon.com in the patent infringement lawsuit. Thereafter, Amazon.com initiated a declaratory judgment action against its excess insurer. The excess insurer settled the dispute with Amazon.com, and reimbursed Amazon.com for its underlying defense costs. Amazon.com, in turn, assigned its rights against its general liability insurer to the excess insurer. The excess insurer then filed suit against the general liability insurer, seeking a determination that the general liability insurer had a duty to defend Amazon.com in the patent infringement lawsuit.

The *American Dynasty* court, applying Washington law, acknowledged that, as a general rule, patent infringement arising from the manufacture of an infringing product is not an "advertising injury" even if the infringing product is advertised. However, the court observed that because the misappropriation of an advertising idea encompassed the wrongful taking of another's manner of advertising, patent infringement could constitute an "advertising injury" when the infringement at issue pertained to a patented advertising technique. The court concluded that this was essentially what the software manufacturer had asserted against Amazon.com: that Amazon.com had used the manufacturer's patented music preview technology as part of Amazon.com's advertisement. Evaluating the general liability insurer's coverage obligations under its policy, the court found that these allegations conceivably alleged the misappropriation of an idea concerning the solicitation of business so as to fall within the scope of the general liability insurer's "advertising injury" coverage.

The general liability insurer argued that it had no duty to defend because a software program embedded in Amazon.com's Web site could not satisfy the causal nexus that the "advertising injury" coverage required between Amazon.com's advertising and the manufacturer's injury. The *American Dynasty* court disagreed. The court admitted that the lack of the causal nexus is the reason that most patent infringement claims do not constitute an "advertising injury." However, the court explained that the underlying lawsuit was distinguishable, in that the manufacturer's injury derived not merely from Amazon.com's alleged misappropriation of the patented code, but from Amazon.com's alleged use of this technology as a means to market its goods for sale, as well: "In other words, the infringement occurred in the advertising itself." 85 P.3d at 978. Accordingly, the *American Dynasty* court concluded that the general liability insurer had a duty to defend Amazon.com in the underlying patent infringement lawsuit.

4. [13S.34] Invasion of Privacy Coverage Questions

The last sentence of the last paragraph is deleted.

Add at the end of the section:

An example of this exposure is found in *Preferred National Insurance Co. v. Docusearch, Inc.,* 149 N.H. 759, 829 A.2d 1068 (2003) (applying New Hampshire law), in which an insured

Internet-based information broker argued that the "oral or written publication of material that violates a person's right to privacy" offense of its policy's "personal and advertising injury" coverage encompassed the insured's liability arising out of its sale of a woman's social security number and place of employment to an individual who later fatally shot the woman as she left work. *See also Brown v. Erie Insurance Exchange,* No. G031164, 2004 Cal.App.Unpub. LEXIS 1557 (Feb. 20, 2004) (applying California law), in which an insurer was asked to defend the insured software manufacturer in a class action lawsuit wherein it was alleged that the insured had distributed software host programs that bore spyware that automatically loaded onto users' computers and permitted advertisers to monitor computer and Internet activities any time a user was logged on to the Internet.

5. [13S.34A] Defamation Coverage Questions

New section:

In the years ahead, courts will likely see an influx of coverage issues arising from Internet-related defamation claims. In *Baxter v. Doe,* 868 So.2d 958 (La.App. 2004), for example, a former university vice president filed suit against a university professor, alleging that the professor had operated a Web site that he used to publish, author, edit, or disseminate false, malicious, and defamatory statements regarding the vice president's activities at the university. The professor filed a third-party complaint against its homeowners' insurer, seeking a determination from the court that the insurer was obligated to defend the professor against the vice president's claims.

Finding that the insurer had no duty to defend the professor, the *Baxter* court, applying Louisiana law, observed that the homeowners' policy's coverage was limited to damages because of "bodily injury" or "property damage" caused by an "occurrence," which the policy defined to mean an accident. Because the complaint against the professor complained of intentional conduct, the court concluded that the homeowners' insurer had no duty to defend the professor against the vice president's claims.

B. [13S.35] Coverage for Cyberclaims Under "Property Damage" Coverage Grant

Add after the first paragraph:

In *America Online, Inc. v. St. Paul Mercury Insurance Co.,* 207 F.Supp.2d 459 (E.D.Va. 2002), the court, applying Virginia law, concluded that an insurer had no duty to defend America Online against claims that its proprietary software package had caused physical damage to the computers, computer data, and software systems of its customers. America Online's policy provided coverage for "property damage," which the policy defined, in part, to mean "physical damage to tangible property" or "loss of use of tangible property." America Online asserted that computer data, software, and systems are tangible property because they are "capable of being realized." In contrast, the insurer argued that computer data and the like are not tangible property because they constitute property that one cannot touch.

Because the policy did not define the term "tangible," the *America Online* court construed it in accordance with its plain meaning (*i.e.,* something that is capable of being touched or perceived by the senses). The court explained that computer data, software, and systems are not tangible property, as understood by the policy's "property damage" coverage, because they do not have or possess physical form. However, the court acknowledged that a computer, the medium in which data, software, and systems are held and utilized, is tangible property. The court concluded that although there was no "physical" damage to the complainants' computers as that term is commonly understood, the complainants did, indeed, assert claims for a "loss of use" of their computers. The *America Online* court ultimately concluded that the insurer had no duty under the "property damage" coverage to defend America Online in the lawsuit, however, because the "impaired property" exclusion, which precludes "property damage" coverage for "impaired property" (*i.e.,* tangible property, other than America Online's products or completed work, that could be restored to use by nothing more than (1) an adjustment, repair, replacement, or removal of America Online's products, or completed work that forms a part of it, or (2) America Online fulfilling the terms of a contract or agreement), clearly precluded coverage.

Add after the second bold quotation:

In its 2001 CGL form, the ISO's definition of "property damage" specifically provides that for the purposes of "property damage" coverage, electronic data is not tangible property.

B_1. [13S.35A] Internet and Technology-Related Coverage Limitations

New section:

Given the rise of cybertort claims, the ISO has implemented several Internet- and technology-related definitions, conditions, limitations, and exclusions applicable to both Coverages A and B of its 2001 CGL form. Obviously, insurers and insureds alike will want to be mindful of these provisions when evaluating whether there is potential liability coverage with respect to a particular cybertort claim.

V. FIRST-PARTY COVERAGE ISSUES

A. [13S.39] Physical Loss or Damage

Add at the end of the section:

In *Lambrecht & Associates, Inc. v. State Farm Lloyds,* 119 S.W.3d 16 (Tex.App. 2003), an insured employment agency sought coverage under a business insurance policy, the provisions of which obligated the insurer to "pay for accidental direct physical loss to business personal and property" and "loss of income," for the loss of computer data and related business income that it had sustained after a hacker had injected a computer virus into the insured's computer system. The insurer denied the insured's claim under the policy on two bases. First, it took the position that the insured's loss was not accidental because the act that caused the loss was voluntary and intentional. Second, the insurer maintained that the insured's loss of information on its computer system was not a "physical" loss because the data did not exist in a physical or tangible form.

Resolving all inferences in favor of the insured, the *Lambrecht* court, applying Texas law, dismissed the insurer's arguments. As a preliminary matter, the court emphasized that the insurer could not impute the intent of the person who injected the virus into the computer system to the insured in order to avoid coverage. Accordingly, it concluded that the injection of the virus into the computer network, and the resulting damage, were, from the insured's perspective, accidental.

The *Lambrecht* court also rejected the insurer's argument that the insured's loss of information was not a "physical" loss. The court acknowledged that in *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.,* No. CIV 99-185 TUC ACM, 2000 U.S.Dist. LEXIS 7299 (D.Ariz. Apr. 19, 2000), and *America Online, Inc. v. St. Paul Mercury Insurance Co.,* 207 F.Supp.2d 459, 466 – 467 (E.D.Va. 2002), the courts' analyses addressed whether computer data constituted a quantitative physical mass. However, the *Lambrecht* court concluded that such an "erudite thesis" was unnecessary in the case before it because the insured's policy itself defined personal property in such a way so as to encompass the insured's loss of its server, prepackaged software, and the data stored on the server. 119 S.W.3d at 25.