February 2014

To the Millennium: Emerging Issues for the Year 2000 and Cyberspace

Carl W. Chamberlin

Follow this and additional works at: http://scholarship.law.nd.edu/ndjlepp

Recommended Citation
Available at: http://scholarship.law.nd.edu/ndjlepp/vol13/iss1/8
TO THE MILLENNIUM: EMERGING ISSUES FOR THE YEAR 2000 AND CYBERSPACE

CARL W. CHAMBERLIN*

The approach of the millennium brings novel issues of law that arise from the evolution of technology. The most celebrated of these issues—the "Millennium Bug" or Year 2000 problem—arose from technological limitations that computer programmers faced decades ago. Because of limitations in the amount of information computers could store, programmers decided to identify years using two digits ("99") instead of four ("1999"). As a result, computer systems may read the year 2000 as 1900, causing systems to crash or falter at the turn of the century. Computer and software vendors, manufacturers of medical equipment, traffic controls and other products containing embedded chips, state and federal governments, banks and brokerage houses, and corporate officers and directors all face claims for losses caused by the year 2000 ("Y2K") phenomenon. Companies will collectively spend billions to trillions of dollars over the next few years to correct Y2K problems, defend against Y2K litigation, and comply with Y2K-related government regulations.¹

¹ Of Counsel and Chair of the Internet & Computer Litigation Group at the law firm of Orrick, Herrington & Sutcliffe LLP; Adjunct Professor at the University of California, Hastings College of the Law, and the Santa Clara University School of Law. The author gratefully acknowledges the contribution to this article by Samuel P. O'Rourke of Orrick, Herrington & Sutcliffe LLP. The views expressed herein are not necessarily the views of Orrick, Herrington & Sutcliffe LLP or its clients.

Meanwhile, new legal issues proliferate as the world turns to the Internet for communication, entertainment, and commerce. Never before have so many people had such extensive, instantaneous, and inexpensive access to so many other people across the globe. Because the Internet may be accessed anywhere in the world, individuals and companies who post messages or conduct commerce on the World Wide Web may unwittingly subject themselves to foreign laws in distant jurisdictions. Because only one person or entity may use any particular Web site address, trademark law takes on new significance. Enforcement of copyright law is more difficult, yet more important, due to the ease of copying material on the Internet and the high quality of digital copies. Contract law must be adapted to recognize the advent of online "paperless" transactions, for which there are neither writings nor signatures. Traditional privacy protection laws must accommodate the transfer of information through cyberspace.

This article surveys some of the more salient issues to be resolved in the dawn of the twenty-first century. Part I discusses the Millennium Bug, including likely causes of action, litigation to date, and legislation. Part II addresses issues arising out of the Internet, including personal jurisdiction, the assignment of domain names, liability for Web site content, proposed guidelines for electronic contracting under Uniform Commercial Code Article 2B, and privacy issues.

I. The "Millennium Bug"

In the 1950s and 1960s, computer memory had limited capacity. Programmers decided to conserve memory by identifying years with two digits instead of four, such as "99" instead of "1999." As the next century approaches, the significance of this programming shorthand has become apparent. Because many computer systems will misread the "00" in the year 2000, many systems will produce errors or crash.

The Y2K problem is widespread. Hundreds of thousands of companies have "legacy" computer systems comprised of mainframe software applications that contain two-digit date fields. Because these applications were typically written with little documentation originally, and have been patched and modified with new code over the years, the applications tend to be difficult to understand and correct. Personal computers may also pose Y2K

problems, but to a lesser extent. 2 Standalone software packages or off-the-shelf software may also present Y2K problems. If these computer systems produce errors or fail altogether, there will be widespread disruption in the flow and processing of information and commerce.

To solve the majority of Y2K problems in computers, the software code must be altered or replaced so that the dates in the year 2000 and later are properly recognized. The task is ominous. Although some software programs automate the process of locating and correcting Y2K problems, much of the solution will involve the painstaking rewriting of millions of lines of code. 3 Even after the code is corrected, all the data and the procedures which handle it must be tested and refined so that both "old" and "Year 2000 compliant" data are correctly produced, sent, and received. Moreover, businesses must be concerned not only with their own systems, but also with the systems of their suppliers, vendors, customers, and others with whom they interact. 4

Computers will not be the sole source of Y2K problems. Most sophisticated appliances and equipment, including power plants, fire protection systems, medical devices, security systems, elevator controls, time-dependent lighting and HVAC systems, telephone systems, and electronic time locks are "embedded systems," containing microprocessors programmed with code. 5 A


3. There are several approaches to correcting the code. First, the year field could be expanded to four digits, instead of two. This is the most permanent solution, but the most costly to implement. Second, programmers could leave the two-digit year field in tact, but employ "windowing techniques" by which the system interprets and converts the dates. (For example, all two-digit years from 50-99 might be viewed as 1950-99, and all two-digit dates of 00-49 would be interpreted as 2000-2049). Third, unused bits in the two-digit date code could be changed to try to fit the four-digit year into the two-digit year data space. Fourth, data and programs can be "encapsulated," by which the dates in date files are time-shifted (backward and forward 28 years) during processing.

4. Complicating the Y2K solution somewhat is the fact that the Year 2000 is also a leap year, which Y2K fixes must accommodate as well. In addition, some tape library management systems use the "99" date code to activate special instructions, such as destroying the tape library. Problems arising from this programming convention will be seen in 1999.

failure of these systems could cause substantial personal injury as well as economic losses. Because the code in embedded systems is usually not upgradeable or accessible to those who own and operate the systems, a non-compliant embedded system usually must be replaced rather than corrected.

Companies will spend billions to trillions in assessing and remediating their computer systems and litigating Y2K claims. It is estimated that the costs of becoming Y2K compliant will reach $2 billion for the airline industry alone, and $3 billion for the securities industry. Total cost estimates for correcting the Y2K problem range from $300-600 billion or more worldwide. Others estimate that the total cost, including legal fees and litigation judgments, will reach $1.6 trillion.

Throughout the world, businesses and governments are behind the pace necessary to resolve the Y2K problem before the turn of the century. As of 1998, only a third of the companies in the world had started to address the Y2K problem. Nearly half of the companies with a Y2K problem will not become Y2K compliant in time to avoid having all or part of their computer sys-

6. Y2K problems may affect a wide variety of services, causing mild inconveniences or more severe disruptions for which the Red Cross has proposed comprehensive planning. For a good overview from a lay perspective, see the Red Cross Web site at <http://www.redcross.org/disaster/safety/y2k.html>. The extent of predicted disruptions is addressed in Matt Beer, Y2K Bug: Dud or Disaster? SAN FRAN. EXAM'R, Dec. 27, 1998, at C1.


11. See Capers Jones, Global Impacts of the Year 2000 Problem, in Year 2000 Problem: Strategies and Solutions From the Fortune 100, supra note 2, at 12.

tems shut down or falter. Only 17 percent of technology and business executives are confident that the Y2K problem will be fixed in time.

A. Causes of Action

Y2K-related errors will disrupt business, transportation, and the flow of information and communications around the world. Many individuals and businesses will seek relief in lawsuits based on a variety of claims in contract and tort, as well as claims under securities laws and consumer statutes.

1. Breach of Contract or Warranty

Hardware and software vendors typically sell or license products pursuant to written contracts. Written contracts also set forth the terms by which companies provide maintenance of hardware and software systems and consultants provide Y2K solutions. Claims based on these contracts may be asserted if the hardware or software is not Y2K compliant, computer systems do not perform without interruption, or consultants fail to fix the problem or inject further error into the code.

For the most part, claims based on contracts to sell goods such as hardware or software are subject to the Uniform Commercial Code (UCC). Claims based on contracts for the rendition of services are governed by common law. In either case, it may be difficult to identify a particular contract provision by which the defendant undertook to provide a Y2K compliant product. Until the last few years, contracts rarely mentioned Y2K issues.

In the absence of a contract provision addressing Y2K compliance specifically, plaintiffs will argue that Y2K-related problems reflect a breach of an express or implied warranty. For example, in every sales contract there is an implied warranty that the product complies with the description by which it was sold. Plaintiffs will argue that a Y2K failure breaches a warranty that the product will perform in conformity with the product speci-

15. The formation, terms, and enforceability of a contract for the lease or sale of computer software may be governed by proposed U.C.C. Article 2B. U.C.C. Article 2B (Proposed Draft December 1998) (visited Jan. 11, 1999) <http://www.law.upenn.edu/library/ulc/ucc2b/ucc2bALId98.htm>. See also infra notes 181-87, 191-92, and accompanying text.
cations. U.C.C. § 2-314 recognizes an implied warranty that the goods are "merchantable" in the sense of being fit for their ordinary purpose. Among the ordinary purposes of software and hardware is the processing of data irrespective of the date. U.C.C. § 2-315 recognizes an implied warranty that the goods are fit for the particular purpose that the buyer has for the product, as long as the seller knows of it. Purchasers of computer hardware and software may have articulated at the time of purchase a need for the software to continue functioning into the twenty-first century.\(^{17}\)

2. Fraud or Negligent Misrepresentation

Hardware and software vendors may be sued for fraud or negligent misrepresentation if they falsely represented that their products were Y2K compliant. Even if vendors did not make direct representations of Y2K compliance, such representations may be implied from marketing or other statements that the product would continue functioning long into the future.

To establish a fraud claim, a plaintiff must show a representation of material fact, knowledge of falsity, intent to deceive, actual and justifiable reliance, and damage proximately caused by the fraud.\(^{18}\) In the Y2K context, it may be difficult to establish that the vendor had an intent to defraud, particularly if the transaction occurred years ago when Y2K issues were not readily apparent. Plaintiffs may alternatively assert claims for negligent misrepresentation, which does not require a showing of intent, but merely that the defendant made false statements without reasonable grounds to believe they were true.\(^{19}\)

---


3. Product Liability

Manufacturers face strict liability for physical harm caused by defects in the manufacture or design of a product. Manufacturers also face strict liability for failing to warn of a substantial danger that would not be readily recognized by an ordinary consumer. Because physical harm will more likely arise from the malfunction of embedded systems, the manufacturers of embedded systems are more likely to confront strict liability claims. There is no recovery for economic loss under strict products liability theory.

4. Negligence

Y2K defendants may be sued for negligence, on the theory that they knew or should have known that their products could cause damage because they were not Y2K compliant, yet failed to take reasonable steps to protect against that harm.

In determining whether a defendant's actions were reasonable, courts will likely consider the standards and practice in the industry, the extent to which the defendant complied with any applicable government regulations, the practicability of additional efforts toward Y2K compliance, and the information known to the defendant and to the industry generally. Again, transactions conducted long ago are less likely to be the subject of liability. In the 1950s-70s, it was industry practice for software developers to minimize the amount of data, such as date fields, to be stored in memory. Furthermore, software developers at the time did not know that the software would still be used in the twenty-first century.

---

20. See Restatement (Second) of Torts § 402A (1977). Under the Restatement view, the plaintiff must prove that the product was unreasonably dangerous to use. Id. In California, the plaintiff need only prove that the product was defective. See Barker v. Lull Eng’g Corp., 573 P.2d 443, 451 (Cal. 1978) (design defect); Cronin v. I.B.E. Olson Corp., 501 P.2d 1153, 1162 (Cal. 1972) (manufacturing defect).


5. Securities Fraud and Breach of Fiduciary Duty

Y2K problems may harm the business operations of a public company to the point that its stock price declines. Some companies may fail altogether due to Y2K problems. If officers and directors of a company fail to take appropriate steps to protect the company (and its shareholders) from losses stemming from Y2K problems, they may be personally liable for common law breach of fiduciary duty or violation of their statutory obligations to shareholders. Suits may be based on a failure to assess the company’s systems, to consider the readiness of suppliers or customers, or to perform Y2K due diligence in purchasing another company.

Liability may also arise under the federal securities laws for failing to disclose or accurately represent a public company’s Y2K status. The Securities Act of 1933 requires public companies to make certain disclosures in publicly filed reports, including a "Management's Discussion and Analysis of Financial Condition and Results of Operations" ("MD&A"). Companies must disclose in the MD&A any "material events and uncertainties known to management that would cause reported financial information not to be necessarily indicative of future operating results or of future financial condition." Non-compliant systems or uncertainties surrounding the Y2K compatibility of company systems or vendors may be sufficiently material to require disclosure.


23. See, e.g., In re Caremark Int'l, Inc. Derivative Litigation, 698 A.2d 959, 967 (Del. Ch. 1996) ("The directors allowed a situation to develop and continue which exposed the corporation to enormous legal liability and that in so doing, they violated their duty to be active monitors of corporate performance."); CAL. CORP. CODE § 309(a) (West 1998) ("A director shall perform the duties of a director . . . in good faith, in a manner such director believes to be in the best interests of the corporation and its shareholders and with such care, including reasonable inquiry, as an ordinarily prudent person in a like position would use under similar circumstances.").

ment Companies, and Municipal Securities Issuers," a company must disclose information concerning its Y2K status if its assessment of Y2K problems is not complete, or if management determines that its Y2K problems will have a material effect on the company's business, results of operations, or financial conditions, without taking into account the company's efforts to avoid those consequences. According to the Release, a company must assume that it will not be Y2K compliant in the absence of clear evidence of readiness, and it must assume that material third parties will not be Y2K compliant unless the third parties have delivered written assurances that they expect to be Y2K compliant in time. If required to make a disclosure, the company must state (1) the company's degree of Y2K readiness in plain English sufficient to enable investors to fully understand the company's status, (2) material historical and estimated costs of Y2K remediation, (3) the risks confronting the company, including estimated worst-case scenarios and any uncertainty regarding the effect of Y2K problems, and (4) the company's contingency plans to handle worst-case scenarios.

The failure to disclose the effects of Y2K problems could expose a company and its officers and directors to shareholder actions and both civil and criminal liability. Section 11 of the Securities Act of 1933 provides a private cause of action for material misstatements or omissions in registration reports. Section 12 of the 1933 Act provides a cause of action for misstatements or omissions of material facts in a prospectus or oral communication. Section 10(b) of the Securities Exchange Act of 1934 creates an implied cause of action for untrue state-

26. See id. ¶ 80,723. The standard for materiality is whether the disclosure "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).
28. Id. ¶ 80,729. Release Number 33-7558 superseded the SEC's Staff Legal Bulletin No. 5, issued by the Divisions of Corporation Finance and Investment Management. As modified January 12, 1998, the Bulletin stated that a public company determining that its Y2K issues were material may have to disclose the company's plans to address the Y2K issues and the total cost of remediation. Divs. of Corp. Fin. & Inv. Mgmt., SEC Staff Legal Bulletin No. 5 (CF/IM) (Revised Jan. 12, 1998) <http://www.sec.gov/rules/othern/slbcf5.htm>.
30. Id. at § 77l(a) (1994).
ments or omissions of fact in connection with the purchase or sale of a security.\(^{31}\)

6. Deceptive Trade Practices, Unfair Competition, and Other Business Torts

Manufacturers and maintenance organizations may face liability for false advertising if their products or services do not meet the standards set by their advertising. Section 43(a) of the federal Lanham Act\(^ {32}\) provides that any person who uses a false or misleading description or representation in connection with goods or services is liable to anyone damaged thereby.\(^ {33}\) To prevail, a plaintiff must prove that the defendant's statement was (1) false or misleading, (2) in interstate commerce, (3) in connection with goods or services, (4) in commercial advertising or promotion, (5) misrepresentative of the nature, qualities, or geographic origin of the goods, services, or commercial activities, and (6) actually or likely damaging to the plaintiff.\(^ {34}\) In addition, under the Federal Trade Commission Act (“FTCA”),\(^ {35}\) the FTC may enjoin “[u]nfair methods of competition” and “[u]nfair or deceptive acts or practices in commerce.”\(^ {36}\) Deception exists if

\(^{31}\) Claims under § 10(b) require proof of intent to deceive or recklessness. \textit{Id.} at § 78j(b) (1994). Claims under §§ 11 and 12 of the 1933 Act merely require proof of a lack of diligence. \textit{Id.} at §§ 77k, 77ll(a) (1994).


\(^{33}\) \textit{Id.} Remedies for a violation of the Lanham Act include injunctive relief, damages, and, in some cases, attorneys' fees. In order to obtain damages (for a misleading rather than false statement), the plaintiff must establish that the violation caused actual consumer confusion or deception. \textit{See} Tambrands, Inc. v. Warner-Lambert Co., 673 F. Supp. 1190, 1196 (S.D.N.Y. 1987). Attorneys' fees may be awarded only in an "exceptional" case, such as a case of deliberative and willful infringement. \textit{See id.} at 1198.

\(^{34}\) \textit{See J. THOMAS McCARTHY, McCARTHY ON TRADEMARKS AND UNFAIR COMPETITION,} § 27:24, at 27-39 (4th ed. 1998). \textit{See also} Valu Eng’g Inc. v. Nolu Plastics, Inc., 732 F. Supp. 1024, 1026 (N.D. Cal. 1990); U-Haul Int’l, Inc. v. Jartran, Inc., 522 F. Supp. 1238, 1243 (D. Ariz. 1981). If the defendant’s advertisement is found to be literally false, the plaintiff need not prove that the advertising left a false impression on the buying public. \textit{See} Coca Cola Co. v. Tropicana Products, Inc., 690 F.2d 312, 317 (2d Cir. 1982). If the advertisement is literally true, the plaintiff cannot prevail unless it proves that the advertisement was nevertheless deceptive or misleading, by showing it was likely to influence purchasing decisions and it had a tendency to deceive the customer. \textit{See} Sandoz Pharm. Corp. v. Richardson-Vicks, Inc., 735 F. Supp. 597, 600 (D. Del. 1989).


\(^{36}\) 15 U.S.C. § 45(a)(1). Actions under the FTCA may be brought only by the Federal Trade Commission (“FTC”). The FTC may issue a cease and
"there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." State statutes similarly prohibit unfair competition, consumer fraud, and false advertising.

7. Indemnification Claims

Companies and individuals potentially liable to others for Y2K losses may bring suits against third parties for indemnification. For example, manufacturers of embedded systems, sued by those who have been injured by the system's Y2K malfunction, may bring claims for indemnity against the chip manufacturer or software vendor who provided components for the system. Indemnification may be based on a provision in a written contract between the defendant and a third party, or on equitable principles that losses should be divided among joint tortfeasors according to their proportionate fault.

B. Litigation to Date

So far, Y2K litigation has been based on a variety of contract, warranty, and consumer protection claims. The first publicized Y2K lawsuit—Produce Palace International v. TEC-America Corp.—was filed in Michigan by a grocery store whose cash register system could not process credit cards expiring in or after 2000. The plaintiff asserted claims for breach of warranty, violation of the Magnuson-Moss Warranty Act, violation of state consumer protection acts, breach of warranty, breach of duty of good faith,

desist order requiring the advertiser to refrain from making false or misleading representations about its product or to include qualifying disclosures in its advertisements. 15 U.S.C. § 45(b).

37. Southwest Sunsites, Inc. v. FTC, 785 F.2d 1431, 1435 (9th Cir. 1986) (emphasis omitted).

38. See, e.g., UNIFORM CONSUMER SALES PRACTICES ACT, § 3, 7A U.L.A. 236 (1985); UNIFORM DECEPTIVE TRADE PRACTICES ACT, § 2, 7A U.L.A. 277 (1985); CAL. BUS. & PROF. CODE § 17200 (West 1997) (defining unlawful, unfair, or fraudulent business acts or practices); § 17500 (West 1997) (prohibiting false advertising); § 17506 (West 1997) (providing penalties for unfair competition); § 17538 (West 1997) (requiring vendors on the Internet, as well as vendors using traditional telephone, mail, and catalog media, to disclose their return and refund policies and legal name and address); CAL. CIV. CODE §§ 1770(a), 1780(a) (West 1997) (providing cause of action under Consumers Legal Remedies Act for misrepresentations concerning goods).


negligence, misrepresentation, and breach of contract. The case was recently resolved for $250,000.

Thereafter, consumers filed several class actions alleging that software manufacturers should provide free upgrades to satisfy Y2K problems occurring in earlier versions of the software. A class action filed in California in late 1997 alleged that Software Business Technologies, Inc.’s (SBT’s) accounting software was defective in not being Y2K compliant, and that SBT was improperly forcing customers to pay for an upgrade to correct the problem.41 Two other class actions filed in California alleged that Symantec Corp.’s Norton AntiVirus software prior to version 4.0 is similarly defective, and that consumers should not have to pay for the 4.0 upgrade in order to have the problem fixed.42 Plaintiffs in these cases asserted claims for breach of warranty, fraud, and negligent misrepresentation, and violation of the Magnuson-Moss Warranty Act and consumer protection statutes.43 Several other lawsuits assert similar allegations.44

41. Atlaz Int’l Inc. v. Software Bus. Techs., Inc., No. 172539 (Cal. Sup. Ct., Marin Cty., filed Dec. 3, 1997) (class action for breach of warranty, fraud, unfair business practices). This action was recently settled, with the defendant agreeing to provide certain upgrades at no cost.


43. Id.

44. See, e.g., Courtney v. Medical Manager Corp., No. 98-CV-3347 (D.N.J., filed July 15, 1998) (class action for breach of warranty and state trade practices act, alleging that maker of voice-processing system and computer-telephone integration product should have known system was not Y2K compliant, yet is charging for upgrades); Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc., No. 98-1084 (W.D. Pa., filed June 19, 1998) (class action for breach of contract, breach of warranty, fraud and negligence, alleging that manufacturer of software knew or should have known software was not designed to process dates after 2000); Glusker v. Medical Manager Sales & Mktg. Inc., No. CV775812 (Cal. Sup. Ct., Santa Clara Cty., filed Aug. 3, 1998) (class action for breach of contract, fraud, unfair business practices, alleging software manufacturer knew or should have known software was not Y2K compliant, yet is charging for upgrades); Issokson v. Intuit Inc., CV773646 (Cal. Sup. Ct., Santa Clara Cty., filed Apr. 29, 1998) (some versions of Quicken are defective because of inability to process dates after 1999); College v. Medical Manager Corp., No. 98-6401 (Fla. Cir. Ct., Hillsborough Cty., filed Aug. 25, 1998) (class action based on breach of warranty and violations of state deceptive trade practices act, alleging software manufacturer knew or should have known software was not Y2K compliant, yet is charging for upgrades); H. Levenbaum Ins. Agency v. Active Voice Corp., No. 98-3864 (Mass. Sup. Ct., Suffolk Cty.,
In addition, shareholders have brought lawsuits asserting that their companies exaggerated the company’s ability to generate Y2K-related business. For example, a stock purchaser filed a federal securities class action claiming that an information technology solutions and services provider made materially false and misleading statements in a public stock offering about its ability to obtain Y2K-related business and staffing.\footnote{Steinberg v. PRT Group, Inc., No. 98-Civ-6550 (S.D.N.Y., filed Sept. 16, 1998) (asserting claims under §§ 11, 12 & 15 of the Securities Act of 1933).}

C. Legislation

Recognizing the severity and imminence of the Y2K problem, state and federal governments are beginning to enact Y2K-related legislation. The Year 2000 Information and Readiness Disclosure Act\footnote{Pub. L. No. 105-271, 112 Stat. 2386 (1998). A California law signed on September 24, 1998, also provides limited liability immunity for companies that voluntarily share information to resolve Y2K problems. See Cal. Legis. Serv. ch. 860 (West) (codified at Cal. Civ. Code §§ 3269-71).} encourages companies to disclose and share information about Y2K problems by providing limited immunity for false statements and a limited exemption from antitrust laws. Specifically, a Y2K readiness disclosure statement is not admissible against the maker under federal or state law to prove the accuracy of any Y2K statement in the disclosure, unless it was made with (1) actual knowledge that the statement was false or misleading, (2) an intent to deceive or mislead, or (3) reckless disregard of its accuracy.\footnote{See Pub. L. No. 105-271, 112 Stat. 2386 (1998).} The immunity does not apply to documents filed with the SEC or banking regulators or written disclosures made in connection with the offer or sale of securities.\footnote{See id.}
Other legislation, designed to limit liability for Y2K losses, is sure to follow. In light of the anticipated flood of Y2K litigation, California legislators last year introduced several bills attempting to limit liability in Y2K litigation. Although none of these bills survived in committee, they reflect a variety of approaches to the problem.

Assembly Bill (AB) 1710 provided that the exclusive remedy in any lawsuit (except lawsuits for personal injury) resulting directly or indirectly from a Y2K computer date failure would be "deemed to be based solely in contract." Limiting available relief to contract remedies would reduce the potential recovery and thus reduce the attractiveness of bringing Y2K litigation. Computer or software designers or manufacturers would receive the benefit of this limitation of remedies only if they gave notice of a potential date failure and offered a free replacement or repair. Thus, computer and software companies would have an incentive to disclose potential date failures and offer free fixes, particularly since the notice could not be used to prove that the company breached a contract or otherwise acted culpably.

As written, however, AB 1710 probably would not have curbed much litigation. Statutes that award plaintiffs recovery for their attorneys' fees in cases enforcing important rights affecting the public interest provide incentive for plaintiffs and their counsel to pursue such litigation. AB 1710 would probably not have precluded the recovery of attorneys' fees, leaving the incentive for litigation. Interestingly, AB 1710 would not have discouraged the Y2K class actions to date, as the defendants apparently had not provided notice of potential computer date failure or offered a free Y2K fix. Furthermore, because AB 1710 did not


50. Damages for breach of contract are intended to put the injured party in as good a position as if the contract had been performed, and usually are limited to the harm reasonably contemplated by the parties when they signed the contract. By comparison, damages for torts, such as negligence or fraud, could include damages that the parties had not anticipated. See CAL. CIV. CODE § 3333 (West 1997). Consequential damages, such as lost profits, are therefore more difficult to recover in contract actions. Thus, a company or consumer that receives non-compliant Y2K products could sue the manufacturer for the costs of solving the problem, but might not recover for the business it lost due to the non-compliant product, or for the liability the company or consumer incurred to others. In addition, contract remedies usually do not include compensation for emotional distress. Nor do contract remedies include punitive damages, which might be imposed in other cases to punish the defendant for acting with malice or fraud. See CAL. CIV. CODE § 3294 (West 1997).

51. See CAL. CIV. PROC. CODE § 1021.5 (West 1980).
clearly identify the "exclusive remedies," plaintiffs would have tested the language and sought more extensive remedies until the courts ruled clearly to the contrary.

California AB 1934\textsuperscript{52} proposed to limit, in any action based on computer date failure, the recovery for non-economic losses to $250,000. Because the bill would have limited only non-economic losses, it would not have curbed business litigation. Furthermore, nothing in the legislation demonstrated that the availability of $250,000 for non-economic damages would discourage litigation.

While AB 1934 may have been too limited, California SB 2000\textsuperscript{53} would have been overbroad. SB 2000 would have provided immunity to public entities and their employees from any cause of action based on an incorrect date they "produced, calculated or generated," "regardless of the cause of the error." Although the bill by its terms would not have affected liability based on breach of contract, the legislation would have apparently immunized public entities from damages for all date errors, even if not caused by Y2K problems.

D. Conclusion

Predictions of the effect of the Y2K problem range from minor inconvenience to the catastrophic collapse of world economies and massive personal injuries from failing equipment. Whatever the Y2K effect, litigation will surely arise in the absence of legislation that effectively discourages lawsuits. Most of the Y2K problems will derive from decades-old legacy systems, but litigation will be least effective against the parties responsible for those systems because Y2K was not an issue at the time. Corporate officers and directors must therefore be vigilant in taking prompt steps to assess company systems, remediate Y2K problems, test to assure Y2K compliance, investigate the compliance of vendors, and develop contingency plans.

II. The Internet

In 1969, the Department of Defense commissioned the development of a decentralized national communications network that would withstand a nuclear attack. The experimental network, called ARPANET, was designed so that if any hub in the network was destroyed, messages would be rerouted automatic-


cally through an alternative hub. ARPANET evolved into today's Internet, a comprehensive network of thousands of computer networks throughout the world.

The most popular segment of the Internet is the World Wide Web, which consists of thousands of multimedia Web pages that include text, graphics, sounds, and other files. These Web pages reside on host computers, or servers, which are located all over the world and communicate with each other according to a "hypertext protocol" ("HTTP"). Other segments of the Internet include electronic mail ("e-mail"), Bulletin Board Services ("BBS"), and UseNet newsgroups.

Users gain access to the Internet using an online service, such as America Online or Microsoft Network, or an Internet Service Provider ("ISP"). Although the distinction between online services and ISPs is beginning to blur, as a general matter online services, unlike ISPs, offer third-party content and interactive services such as e-mail, "chat" rooms, bulletin boards, home pages, and directories. Most users connect to the online service or ISP using their computer modem and a standard telephone line or special high speed connection.

Users navigate the Web with the help of "browser" software, which provide a graphic interface to the Web. A user who wants to visit a particular Web site types into the browser the desired site's address or Uniform Resource Locator ("URL"), often known as a "domain name." A domain name takes the form of

---


55. Bulletin board services are computer systems that enable users to post messages on an electronic "billboard," upload and download files, and participate in electronic discussions, often called "chats." See id. at 19.

56. The UseNet, short for User's Network, is a network of computers distributing "newsgroup" information. Newsgroups are discussion groups dedicated to a particular topic. See Harle Hahn & Rick Stout, The Internet Complete Reference 22-23 (1994).

57. When uploading information onto the Web, the user's modem changes the computer's digital data into analog form for transmission over analog telephone lines to the service provider. The modem at that end then changes the analog data back into digital form and passes it on to its ultimate destination in cyberspace, often by way of one or more switches or routers. Downloading information from the Web takes the reverse course. See id. at 36. ISDN (Integrated Services Digital Network) service transfers data in its original digital format, improving the speed of transmission. See Allison, supra note 54, at 334. Faster still is TI service, which runs from the customer to the central communications office of an ISP. See id. at 338.

58. Each Web site actually has two addresses: (1) a numerical IP (Internet Protocol) address, comprised of four groups of numbers separated by decimals,
letters and numbers, such as "http://www.orrick.com." If the user does not know the site's address, the user may search for the site, or for other sites on the same subject, by accessing a site called a search engine or online directory and typing in words that describe the desired site.

Users may also "surf"—moving from site to site—by means of hyperlinks, which appear on a Web page as words in a different color or other differentiated text or image. When a user clicks the computer's mouse on a hyperlink, the user is connected to another Web page, which may be part of the same site or part of a different site.

The Internet has grown dramatically in the last few years. In 1994, three million people, most of them in the United States, used the Internet. In 1998, 100 million people from around the world used the Internet. It is estimated that one billion people may be connected to the Internet by 2005.

The Internet provides unparalleled opportunities for communication, education, entertainment, and commerce, crossing international boundaries in a split second at a fraction of the cost which identifies the site's host computer; and (2) for the convenience of users, a unique Uniform Resource Locator, commonly called a "domain name." See Hahn & Stout, supra note 56, at 49, 57. Specialized computers known as "domain name servers" maintain tables linking domain names to IP numbers. See Daniel P. Dern, The Internet Guide for New Users 75-76 (1994). See also Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 952 (C.D. Cal. 1997).

In this example, "http" refers to the hypertext protocol, and "www" refers to the World Wide Web. See Allison, supra note 54, at 354. The actual domain name is "orrick.com." The word "orrick" is the "second level" domain, which is chosen by the owner of the site to identify the site's content or owner. The abbreviation "com" is the "top level" domain, which identifies the owner as a commercial entity. See Hahn & Stout, supra note 56, at 53.

A similar means of moving from site to site is a "button bar." A button bar is a row of pictures, called icons. When a user clicks on the icon, the user is linked to another part of the site or a different site.


See Secretariat on Electronic Commerce, supra note 61, at 7. By 2002, the Internet may be used for more than $300 billion worth of commerce. See id.
of traditional media. Colleagues in different parts of the world can share and edit documents simultaneously, and have conversations online in real time. There is, however, no center or command station for cyberspace. Nor is there any uniform set of laws or central source of governance. To the contrary, the Internet has been developed largely by entrepreneurs and visionaries who relish the blossoming of cyberspace without the interference of government regulation.64

Technological differences between cyberspace and the "brick and mortar" world of traditional jurisprudence, as well as the philosophical differences between the frontier of cyberspace and regulations designed to protect property rights, combine to create new and as yet unresolved legal issues. While by no means an exhaustive list, the primary issues may be divided into four categories: (1) personal jurisdiction; (2) domain names; (3) Web site content; and (4) electronic commerce, including online contracting and privacy.

A. Personal Jurisdiction

For a court to exercise jurisdiction over a defendant, both constitutional due process requirements and any applicable state

64. In 1990, Mitchell Kapor and John Perry Barlow, founders of the Electronic Frontier Foundation, described the early nature of the Internet as follows:

In its present condition, Cyberspace is a frontier region, populated by the few hardy technologists who can tolerate the austerity of its savage computer interfaces, incompatible communications protocols, proprietary barricades, cultural and legal ambiguities, and general lack of useful maps or metaphors.

Certainly, the old concepts of property, expression, identity, movement, and context, based as they are on physical manifestations, do not apply succinctly in a world where there can be none. [¶] Sovereignty over this new world is also not well defined. . . .

Our financial, legal, and even physical lives are increasingly dependent on realities of which we have only the dimmest awareness. We have entrusted the basic functions of modern existence to institutions we cannot name, using tools we've never heard of and could not operate if we had.

As communications and data technology continues to change and develop at a pace many times that of society, the inevitable conflicts have begun to occur on the border between Cyberspace and the physical world.

"long arm" statute must be satisfied.65 Under the Constitution, a defendant in one state may be subject to litigation in another state if the defendant has "minimum contacts" with that other state, such that the maintenance of jurisdiction does not offend "traditional notions of fair play and substantial justice."66 Some state statutes employ this same standard,67 while others are more restrictive.68

A non-resident defendant may be subject to "general" jurisdiction or "specific" jurisdiction. General jurisdiction arises if the defendant conducts "continuous and systematic" activities in the state, and permits litigation against the defendant for any cause of action, whether or not the cause of action is related to the defendant's activities in the state.69 Specific jurisdiction may arise if the defendant had one or more contacts with the state, but permits lawsuits against the defendant only for causes of action arising out of those contacts.70 Specific jurisdiction exists if the defendant actually committed a tort within the state, or if the defendant's out-of-state activities were purposefully directly toward a state resident and caused injury.71

In deciding whether the exercise of general and specific jurisdiction will "comport with fair play and substantial justice,"72 considerations include the extent of the defendant's purposeful activities in the forum, the burden on the defendant, the forum state's interest in adjudicating the dispute, the plaintiff's interest

65. See Aanestad v. Beech Aircraft Corp., 521 F.2d 1298, 1300 (9th Cir. 1974) (starting point in analysis of personal jurisdiction in federal court is long arm statute of state in which the federal court is located).


67. See, e.g., CAL. CIV. PROC. CODE § 410.10 (West 1998).

68. See, e.g., N.Y. C.P.L.R. 302 (McKinney 1997).


70. See Burger King Corp. v. Rudzewicz, 471 U.S. 462, 472 (1985); Von's, 926 P.2d at 1092.

71. See Burger King, 471 U.S. at 476; Calder v. Jones, 465 U.S. 783, 789-90 (1984). The Ninth Circuit employs a three-part test to determine whether a non-resident defendant is subject to specific jurisdiction: (1) the defendant must perform an act or transaction within the forum or purposefully avail himself of the privilege of doing business in the forum; (2) the claim must arise out of the defendant's forum-related activities; and (3) exercise of jurisdiction must be reasonable. See Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 416 (9th Cir. 1997).

72. Burger King, 471 U.S. at 476.
in obtaining convenient and effective relief, and the existence of an alternative forum. 73

1. General Jurisdiction Based on Web Site

Conceivably, a Web site could create such continuous and systematic contacts with a state that it would establish general jurisdiction, especially if the site generated substantial sales. 74 Courts have held in more traditional contexts, however, that merely placing advertisements or toll-free numbers in nationally distributed periodicals does not subject a non-resident to general jurisdiction. 75 Communicating regularly with Californians on a national computer-based information service has been held not to establish general jurisdiction. 76 Furthermore, even if the Web is akin to a telephone system by which users communicate with one another, most courts hold that merely making telephone calls to residents of another state is insufficient in itself to confer general jurisdiction. 77

2. Specific Jurisdiction for Claims Arising out of Web Site

A Web site is more likely to give rise to specific jurisdiction, where statements on the Web site are the basis for the plaintiff's causes of action. For example, the Web site itself may give rise to claims such as breach of contract, false advertising, or trademark or copyright infringement. Under a constitutional analysis, the issue is usually whether the defendant purposefully availed itself of the benefits and protections of the laws of the forum state. Under state long arm statutes, the issue is whether the defendant's activities fall within the provisions of the statute.

73. See id. at 476-77. This article focuses on the purposeful availment aspect of specific jurisdiction. The "reasonableness" of the exercise of jurisdiction is well discussed in Panavision Int'l L.P. v. Toeppen, 141 F.3d 1316, 1322-24 (9th Cir. 1998).


77. See, e.g., Far West Capital Inc. v. Towne, 46 F.3d 1071, 1077 (10th Cir. 1995).
a. Decisions Under Constitutional Due Process

Whether a defendant, through its Web site, purposefully availed itself of the benefits of the forum state turns on "the nature and quality of commercial activity that [the] entity conducts over the Internet."78 It is not required that the defendant be physically present or have physical contact with the forum, so long as its actions were "purposefully directed" at residents of the forum.79

In asserting specific jurisdiction over claims arising out of a Web site's content, courts have relied in part on features of the Internet that distinguish it from traditional media. In Maritz, Inc. v. Cybergold, Inc.,80 the court suggested that Web site advertising more likely amounts to purposeful availment than advertising by direct mail or an "800" telephone number, noting the "different nature" of electronic communications. In EDIAS Software International, L.L.C. v. BASIS International Ltd.,81 the court exercised jurisdiction over a nonresident software producer for defamatory Web site postings and e-mail messages, explaining that information on a Web site is more accessible than traditional advertising. In exercising jurisdiction over a non-resident who advertised on the Internet, the court in Inset Systems, Inc. v. Instruction Set, Inc.82 suggested that Web site advertising may more likely constitute purposeful availment than other advertisements because "advertisements over the Internet are available to Internet users continually, at the stroke of a few keys of a computer."83

The primary consideration in determining if a Web site constitutes purposeful availment has been whether the site is "interactive," rather than a "passive" display akin to traditional advertisements and solicitations. In Maritz, the Web site was deemed "active" because it encouraged users to add their names to a mailing list, even though the business of the Web site itself was not yet operational. In EDIAS, an electronic bulletin board

79. For certain tort claims, purposeful availment may be demonstrated under a so-called "effects test" by (1) intentional actions, (2) expressly aimed at the forum state, (3) causing harm in the forum state, where the defendant knows harm will likely be suffered in the forum state. See Calder, 465 U.S. at 786; Panavision, 141 F.3d at 1321; Core-Vent Corp. v. Nobel Industries AB, 11 F.3d 1482, 1486 (9th Cir. 1993).
83. Id. at 163.
on which defamatory e-mail messages appeared was deemed interactive, because it allowed the Web page owner or visitor to post as well as read messages.

The distinction between interactive and passive sites was well chronicled by the Ninth Circuit in *Cybersell, Inc. v. Cybersell, Inc.* In *Cybersell*, an Arizona corporation provided Internet advertising, marketing, and consulting services under the service mark Cybersell. A Florida company of the same name provided Web site construction services and maintained a Web site “cybersell.com.” Plaintiff filed suit in Arizona, alleging that the Florida company infringed its service mark. The Florida company had not used its site to conduct commercial activity, such as inviting residents to subscribe to a service or accepting money from Arizona residents. Characterizing the site as essentially passive, the court ruled that the mere fact that the site could be accessed anywhere did not give rise to an inference that the defendant had deliberately directed its marketing toward Arizona. The defendant’s posting of the site was therefore insufficient to constitute purposeful availment.85

If a Web site is not interactive, it may still give rise to jurisdiction if the owner conducted additional activities in the forum. For example, in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, the court exercised jurisdiction over a California defendant who not only advertised on the Internet, but also sold subscriptions to 3,000 state residents and entered into contracts with Internet service providers in the state to download the electronic messages which formed the basis of the suit.86

84. 130 F.3d 414 (9th Cir. 1997).
85. See id. at 419-20. The court explained that the “effects” test set forth in *Calder v. Jones*, 465 U.S. 783 (1984) and *Core-Vent Corp. v. Nobel Industries*, 11 F.3d 1482 (9th Cir. 1993), did not apply. That test permits jurisdiction with respect to intentional torts directed at the plaintiff, causing injury where the plaintiff lives. See *Calder*, 465 U.S. at 789; *Core-Vent*, 11 F.3d at 1486. The court reasoned that the effects test was inapplicable because the plaintiff was a corporation, rather than an individual, and a corporation “does not suffer harm in a particular geographic location in the same sense that an individual does.” *Cybersell*, 130 F.3d at 420; Panavision Int’l, L.P. v. Toeppen, 141 F.3d 1316, 1322 n.2 (9th Cir. 1998).
87. See also *Panavision*, 141 F.3d at 1316 (holding that specific jurisdiction existed over defendant who purposefully registered plaintiff’s trademarks as domain names to force plaintiff to pay defendant money, where the brunt of harm to plaintiff was in California and defendant knew plaintiff would suffer harm in California); *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996) (holding that entry into contract governed by Ohio law and electronically transmitting files to Ohio database gave rise to jurisdiction). But see *SF Hotel Co. L.P. v. Energy Invs., Inc.*, 985 F. Supp. 1032 (D. Kan. 1997) (holding that
In summary, the nature and extent of a Web site's interactions with residents of another state, and possibly the extent to which the company conducts related activities in the state, will determine whether the company has purposefully availed itself of the benefits of the forum. Provided that the exercise of jurisdiction is otherwise reasonable, such purposeful availing will satisfy constitutional due process requirements for personal jurisdiction with respect to claims arising out of those contacts.\textsuperscript{88}

\textit{b. Decisions Under State Law}

Even if a Web site or e-mail reflects purposeful availing and satisfies the constitutional due process requirements for personal jurisdiction, jurisdiction may not be exercised unless the requirements of the forum state's long arm statute are also met.

Some state laws, for example, require physical presence of the defendant or other requirements not necessary for due process. In \textit{Bensusan Restaurant Corp. v. King},\textsuperscript{89} a Missouri defendant maintained a Web site promoting a jazz club called "The Blue Note." The use of the name allegedly infringed the trademark of the plaintiff, who operated a jazz club of the same name in New York. Initially, the site included a hyperlink to the plaintiff's own Web site. After the plaintiff objected, the defendant changed the Web site and disclaimed affiliation with the plaintiff. The plaintiff brought suit in federal court in New York, asserting that jurisdiction existed under two provisions of the New York long arm statute: C.P.L.R. 302(a)(2), for tortious acts committed within the state, and C.P.L.R. 302(a)(3), for out-of-state activities causing injury within the state, where the defendant derived substantial revenues from interstate commerce. The Second Circuit Court of Appeals held that the Missouri resident's Web site, although accessed in New York, did not give rise to jurisdiction under New York's long arm statute. C.P.L.R. 302(a)(2) did not grant jurisdiction because the defendant's creation of the site, use of the words Blue Note and the Blue Note logo, and creation of the hyperlink were performed by persons physically in Missouri, not New York. There was no jurisdiction under C.P.L.R.

\textsuperscript{88} See also \textit{Conseco, Inc. v. Hickerson}, 698 N.E.2d 816 (Ind. Ct. App. 1998) (holding that defendant did not purposefully avail himself of the benefits and protections of Indiana law where his only contact with Indiana was his Web site that asked if anyone knew of fraud or unfair treatment caused by the Indiana company's subsidiary).

\textsuperscript{89} 126 F.3d 25 (2d Cir. 1997).
302(a)(3) because the defendant did not have substantial revenues derived from interstate commerce.\textsuperscript{90}

Other states do not condition jurisdiction on the physical presence of the defendants. In \textit{Hall v. LaRonde},\textsuperscript{91} a California plaintiff had entered into a contract with a New York business that would license the plaintiff's software to the public and forward royalties to the plaintiff. The parties negotiated the contract via e-mail and telephone from their respective states. When a dispute arose, the plaintiff sued in California. The court, noting that California's long arm statute permitted exercise of jurisdiction coextensive with constitutional due process requirements, held that the defendant was subject to jurisdiction even though he was never physically in California. Citing the changing "role that electronic communications plays in business transactions," the court concluded that "[t]here is no reason why the requisite minimum contacts cannot be electronic."\textsuperscript{92}

In \textit{Telco Communications Group, Inc. v. An Apple a Day, Inc.},\textsuperscript{93} a Missouri corporation posted defamatory press releases about the Virginia plaintiff. Plaintiff sued in federal court in Virginia. Virginia's long arm statute permits the exercise of jurisdiction over a defendant who causes injury within the state if, among other things, the defendant regularly conducts business in the state. The court found that the defendant met this standard by posting two or three press releases which advertised its firm and solicited investment banking assistance, and which Virginia residents

\textsuperscript{90} See id. at 28-29; cf. Hearst Corp. v. Goldberger, 1997 U.S. Dist. LEXIS 2065 (S.D.N.Y. Feb. 26, 1997) (holding that no jurisdiction existed under N.Y. C.P.L.R. 302(a)(2) because defendant, who created a Web site merely announcing a future business, was not present within the state).

\textsuperscript{91} 56 Cal. Rptr. 2d 399 (Cal. Ct. App. 1997).

\textsuperscript{92} Id. at 402. The defendant relied on Interdyne Co. v. SYS Computer Corp., 31 Cal. App. 3d 508 (1973), which held that a California resident who deals with nonresident purchasers only through out-of-state agents or interstate mail and telephone cannot compel the nonresident to come to California for litigation. The court in \textit{Hall} disagreed with the \textit{Interdyne} decision, concluding that jurisdiction should not be determined by whether the defendant's communications were made in person, particularly in light of the expansion of commerce in the electronic age. The court stated:

Much has happened in the role that electronic communications plays in business transactions since \textit{Interdyne} was decided more than 20 years ago. The speed and ease of communications has increased the number of transactions that are consummated without either party leaving the office. There is no reason why the requisite minimum contacts cannot be electronic.

\textit{Hall}, 56 Cal. Rptr. 2d. at 402.

\textsuperscript{93} 977 F. Supp. 404 (E.D. Va. 1997).
could access twenty-four hours a day. The court distinguished the Second Circuit's holding in Bensusan, because, unlike New York's long arm statute, Virginia's long arm statute does not predicate jurisdiction on the defendant being physically present in the state.

3. Conclusion

In general, the more interactive a Web site is, the more likely it will give rise to jurisdiction. As in EDIAS and Maritz, inviting consumers to sign on for services, post messages, and order products from a Web site will increase the chances that a court will find purposeful availment.

The irony, of course, is that interactivity is what sets the Internet medium apart from other media. Companies may therefore attempt to limit their vulnerability to jurisdiction in distant forums by other means, without unduly compromising interactivity. First, the site could limit the ability of residents in distant states to access the site. By requiring users to identify their state or zip code, it may be possible to preclude access to the site in certain states, or preclude on-line orders from residents of those states. Second, the site may expressly state that it is for the benefit of residents of the company's home state only, disclaiming any intent of purposeful availment. Third, the site may dictate that litigation arising out of transactions or communications with the site must be brought in a particular court. These tactics have not yet been tested in a reported decision, but may help companies reconcile the attributes of Internet technology with the law of personal jurisdiction.

94. See id. at 406.
95. See id.
96. Under federal law, forum selection clauses are generally presumed valid and will be enforced unless unfair, unreasonable, or induced by fraud, or the other party did not receive at least constructive notice of the selection. See Carnival Cruise Lines, Inc. v. Schutte, 499 U.S. 585, 594-95 (1991); Burger King v. Rudzewicz, 471 U.S. 462, 472 n.14 (1985). A forum selection clause has been enforced even where the parties did not have any other contacts within the forum. See Zenger-Miller, Inc. v. Training Team, GMBH, 757 F. Supp. 1062, 1069 (N.D. Cal. 1991).
97. As the United States Supreme Court articulated decades ago: "As technological progress has increased the flow of commerce between the states, the need for jurisdiction has undergone a similar increase." Hanson v. Denkla, 357 U.S. 235, 250-51 (1958).
B. Domain Name Disputes

As discussed above, Web sites are identified by domain names. Domain names consist of (1) a second level domain—the word(s) located to the left of the "dot"—which is often the name of the site owner, and (2) a top level domain—the abbreviation to the right of the "dot"—that identifies the type of entity owning the site. Currently, the Web is "divided" into top level domains of "com" for commercial or other entities or individuals, "net" for networks, "edu" for educational institutions, "gov" for government entities, and "org" for non-profit organizations.

Domain names are currently registered by the Internet Network Information Center ("InterNIC"), which operates in the United States through a company called Network Solutions, Inc. ("NSI"). NSI does not make any independent determination of an applicant's right to use a domain name. Instead, it registers domain names on a "first come, first served" basis and screens domain name applications against its registry to prevent repeat registrations of the same name. Although NSI has a "domain name dispute policy," disputes involving the assertion of trademark rights usually resort to the courts.

Most businesses on the Internet like to have second level domain names that include the name of their company because many Web users attempt to find a company on the Web by typing in the name of the company (e.g. Pepsi) in the form of a domain name (i.e. "pepsi.com"). The nature of Web technology further increases the incentive of companies to use a particular domain name.

98. See supra note 58 and accompanying text.
99. There are also top level domains that are two-letter country codes.
100. The domain name registration system is currently in transition. By now, the "com" top level domain has become quite crowded, inspiring thoughts of adding new generic top level domains ("gTLDs"). At the same time, the administration of the system is changing hands. Pursuant to a June 5, 1998 White Paper entitled "Management of Internet Names and Addresses" issued by the National Telecommunications and Information Administration, domain name registration and new top level domains are under the direction of a new U.S. non-profit corporation, The Internet Corporation for Assigned Names and Numbers ("ICANN"), with an international board of directors. NSI presently registers top level domains, but will have to open its registration system to competitors in the spring of 1999.
103. The latest version of this dispute policy can be obtained at the NSI Web site located at <http://www.netsol.com/rs/dispute-policy.html>. 
name. Under traditional trademark infringement laws, usually more than one company may use the same or similar name provided the companies' respective industries or geographic locations are sufficiently dissimilar that consumers will not be confused as to the source of the goods or services. The problem created by the Internet, however, is that "[s]econd level domain names, the name just to the left of '.com,' must be exclusive." Because only one person or entity can maintain a given domain name, the right to maintain the name is extremely important.

Disputes over the right to use a particular domain name are usually based on theories of trademark infringement or trademark dilution under the federal Lanham Act. Trademark infringement exists if: (1) the plaintiff has a federally registered mark; (2) the accused infringer uses the mark "in connection with the sale, offering for sale, distribution or advertising of any goods or services"; and (3) the use is likely to cause confusion, mistake, or deception. Trademark dilution exists if: (1) the plaintiff owns a "famous" mark; (2) the accused makes a "commercial use in commerce of a mark or trade name"; (3) the accused's use began after the mark became famous; and (4) the use dilutes the mark by tarnishing it or blurring its distinctiveness.

Defendants in domain name disputes tend to fall into one of five categories: (1) cybersquatters, who intentionally register domain names using names similar to a trademark of another company, and then sell the rights to the domain name to the owner of the mark; (2) non-trademark holders disparaging a company through use of its trademark; (3) non-trademark holders...

---

104. A commonly cited example is Delta Faucets and Delta Airlines. Both may use the name Delta in commerce, but only one may have the domain name "delta.com."


106. See McCarthy, supra note 34, § 25:76, at 25-143 (citing Lanham Act § 32(1), 15 U.S.C.A. § 1114(1) (1994)). Infringement of an unregistered mark may also be actionable under the Lanham Act. The plaintiff must show: (1) a valid protectable mark (i.e. distinctive or suggestive with a secondary meaning and used before defendant used it); (2) the accused infringer's use is "on or in connection with any goods or services"; and (3) the use is likely to cause confusion, mistake, or deception as to the affiliation, connection or association of the accused infringer or as to the origin of the "goods, services or commercial activities" of the accused infringer. Id. (citing Lanham Act § 43(a)(1)(A), 15 U.S.C. § 1125(a)(1)(A) (1994)). At least one court has held that infringement does not arise from the use of another's trademark in a non-domain portion of the Web site address. See Patmont Motor Werks, Inc., v. Gateway Marine, Inc., No. 96-2703, 1997 WL 811770 (N.D. Cal. Dec. 18, 1997).

107. Id. (citing Lanham Act, § 43(c), 15 U.S.C.A. § 1125(c)).
ers capitalizing on a company's trademark; (4) innocent users; and (5) concurrent trademark holders.

1. Cybersquatters

Cybersquatters register a domain name that is the same or nearly identical to the name of a well-known company. This registration precludes the trademark holder from registering a domain name using its own trademarked company name. Furthermore, it means that a Web site sporting the company's name may include material that would affect the company's reputation or goodwill. Generally, the trademark holder will attempt to procure the right to the domain name from the registrant, and the registrant will demand a fee. Cybersquatters will often repeat this process for dozens of domain names and trademark holders.

Cybersquatters are typically sued for trademark dilution.\(^{108}\) In *Panavision International, L.P. v. Toeppen*,\(^{109}\) the plaintiff held registered trademarks to the name "Panavision" in connection with motion picture camera equipment.\(^{110}\) When plaintiff attempted to register the domain name "Panavision.com" with NSI,\(^{111}\) it found that the domain name was registered to defendant Toeppen, who was using the name to refer to a Web site displaying photos of the City of Pana, Illinois.\(^{112}\) When Toeppen was told to cease using the mark, Toeppen offered to turn over the domain name for payment of $13,000.\(^{113}\) Panavision refused and sued Toeppen for dilution of its trademark under the Federal Trademark Dilution Act of 1995\(^{114}\) and its California


\(^{109}\) 141 F.3d 1316 (9th Cir. 1998).

\(^{110}\) See id. at 1319.

\(^{111}\) See id.

\(^{112}\) See id.

\(^{113}\) See id.

\(^{114}\) 15 U.S.C. § 1125(c) (1994). The Federal Trademark Dilution Act provides in part:

The owner of a famous mark shall be entitled... to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark...

*Id.* § 1125(c)(1).
The district court granted summary judgment in favor of Panavision on both claims. On appeal, the Ninth Circuit upheld the district court's ruling. Toeppen did not contest that the Panavision mark was famous or that his use of the mark began after it became famous. Instead, Toeppen contended that the mere registration of a trademark as a domain name, without more, is not a commercial use. The court rejected Toeppen's argument, finding that Toeppen was in fact engaged in the "business" of registering trademarks as domain names with the intent to later profit by selling them to the rightful trademark owner.

Furthermore, the court found that Toeppen's actions amounted to dilution because the site "diminished the capacity of Panavision marks to identify and distinguish Panavision's goods and services on the Internet." The court explained that "[a] significant purpose of a domain name is to identify the entity that owns the [W]ebsite," and Toeppen's use of "Panavision.com" would lead those searching for the Panavision site to discover Toeppen's site and be discouraged from wading into it.

---

115. See Panavision, 141 F.3d at 1319; California Anti-dilution statute, CAL. BUS. & PROF. CODE § 14330 (West Supp. 1998). The California statute prohibits the dilution of "the distinctive quality" of a mark regardless of competition or likelihood of confusion. Panavision, 141 F.3d at 1324.

116. See Panavision, 141 F.3d at 1318. During the litigation, it was discovered that Mr. Toeppen had registered domain names for at least 100 other companies including Delta Airlines, Neiman Marcus, Eddie Bauer, and Lufthansa. He had also attempted to sell at least two other domain names for between $10,000 and $15,000. See id. at 1319.

117. See id. at 1327.

118. See id. at 1324.

119. See id. at 1319. The court noted that "[i]t does not matter that he did not attach the marks to a product. Toeppen's commercial use was his attempt to sell the trademarks themselves. Under the Federal Trademark Dilution Act and the California Anti-dilution statute, this was sufficient commercial use." Id. at 1325-26 (citation omitted).

120. Dilution usually involves "blurring" or "tarnishment." Blurring occurs when a defendant uses a plaintiff's trademark to identify the defendant's goods or services, creating the possibility that the mark will lose its ability to serve as a unique identifier of plaintiff's product. See Ringling Bros.-Barnum & Bailey, Combined Shows, Inc. v. B.E. Windows Corp., 937 F. Supp. 204, 209 (S.D.N.Y. 1996) (citing Deere & Co. v. MTD Prods., Inc., 41 F.3d 39, 43 (2d. Cir. 1994)). Tarnishment occurs when a famous mark is improperly associated with an inferior or offensive product or service. See McCarthy, supra note 34, § 24:104.

121. Panavision, 141 F.3d at 1327 (citing Panavision Int'l, L.P. v. Toeppen, 945 F. Supp. 1296, 1304 (C.D. Cal. 1996)).
through hundreds of other Web sites to find the true Panavision site.\textsuperscript{123}

In \textit{Avery Dennison Corp. v. Sumpton},\textsuperscript{124} defendants had registered over 12,000 domain names under common or trademarked company names. Defendants argued that they had registered the names, not for the purpose of selling them to corporations, but rather to rent them to Internet users as e-mail addresses.\textsuperscript{125} Skeptical of defendants’ assertions, the court found that defendants had nevertheless denied plaintiff the use of its mark as a domain name and had thus diluted plaintiff’s ability to identify its goods and services.\textsuperscript{126}

2. Non-Trademark Holder Disparaging a Company

Some register a domain name using the trademarked name of a company in order to lure users who believe they have accessed the company’s actual site. They then have the opportunity to disparage the company to those most interested in it.

Competitors may employ this tactic. In \textit{Green Products Co. v. Independence Corn By-Products Co.},\textsuperscript{127} defendant Independence Corn By-Products Co. (“ICBP”) registered the domain name “greenproducts.com” after its competitor, plaintiff Green Products Company (“Green Products”). Green Products sued ICBP for trademark infringement and sought a preliminary injunction forcing ICBP to turn over the domain name.\textsuperscript{128} The court held that ICBP’s use of the domain name created consumer confusion, noting that “ICBP is capitalizing on the strong similarity between Green Products’ trademark and ICBP’s domain name to


\textsuperscript{124} 999 F. Supp. 1337 (C.D. Cal. 1998).

\textsuperscript{125} \textit{See id.} at 1338.

\textsuperscript{126} \textit{See id.} at 1340-41. The legislative history of the Federal Trademark Dilution Act also indicates that “cyber-piracy” amounts to trademark dilution. Senator Patrick Leahy stated, “It is my hope that this antidilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others.” 141 \textit{CONG. REC.} S. 19312-10 (daily ed. Dec. 29, 1995) (statement of Sen. Leahy).

\textsuperscript{127} 992 F. Supp. 1070 (N.D. Iowa 1997).

\textsuperscript{128} \textit{See id.} at 1072-73.
 lure customers onto its [W]eb page."\textsuperscript{129} The court issued the injunction.\textsuperscript{130}

The tactic has also been used by those wanting to advocate views contrary to those of the trademark owner. In \textit{Planned Parenthood Federation of America, Inc. v. Bucci},\textsuperscript{131} the host of a daily "Catholic Radio" broadcast registered the domain name "www.plannedparenthood.com" for a Web site which stated, "Welcome to the PLANNED PARENTHOOD HOME PAGE!" Not only was the site unauthorized by Planned Parenthood, it contained advertising for an anti-abortion book called \textit{The Cost of Abortion}. Plaintiff sued defendant for trademark infringement and trademark dilution.\textsuperscript{132} The court found that defendant's use of the domain name was a commercial use, because the defendant was promoting his book, soliciting funds for political activities, and attempting to harm the plaintiff commercially.\textsuperscript{133} The court also concluded that defendant's use of plaintiff's name both diluted plaintiff's famous mark and presented a significant likelihood of confusion. The court issued the preliminary injunction.

In \textit{Jews for Jesus v. Brodsky},\textsuperscript{134} the defendant registered "jews-for-jesus.com" and "jews-for-jesus.org" as "bogus" Web sites designed to intercept potential converts through use of "deceit and trickery."\textsuperscript{135} The court found that defendant's use of plaintiff's mark and organization name was deceptive and confusing, and enjoined the defendant accordingly.\textsuperscript{136}

\section*{3. Non-Trademark Holder Capitalizing on a Company's Trademark}

Many individuals or companies register domain names similar or identical to the trademarked names of other companies, seeking to capitalize on the company's good name and reputation. The accused infringer solicits business from Internet users

\begin{itemize}
  \item \textsuperscript{129} See \textit{id.} at 1076.
  \item \textsuperscript{130} See \textit{id.} at 1082.
  \item \textsuperscript{131} No. 97 Civ. 0629, 1997 U.S. Dist. LEXIS 3338 (S.D.N.Y. Mar. 19, 1997).
  \item \textsuperscript{132} See \textit{id.} at *4.
  \item \textsuperscript{133} See \textit{id.} at *16.
  \item \textsuperscript{134} 993 F. Supp. 282 (D.N.J. 1998).
  \item \textsuperscript{135} \textit{Id.} at 286, 304.
  \item \textsuperscript{136} The court rejected the proposition that the domain name was constitutionally protected free speech under the First Amendment, stating that "the content of the speech of the defendant [was] not at issue" and that the defendant was free to publish on a site that did not infringe on the plaintiff's mark. \textit{Id.} at 287 n.1, 312.
\end{itemize}
who access the site believing it is sponsored by the trademark holder.

In *Cardservice International, Inc. v. McGee,* plaintiff owned a registered trademark on the name “Cardservice International.” Defendant thereafter registered “cardservice.com” as a domain name. The defendant provided services similar to those of the plaintiff, but on a much smaller scale. The court found “a likelihood of confusion between Cardservice International’s registered mark and McGee’s use of ‘cardservice.com,’” because customers visiting defendant’s site were likely to assume that it belonged to plaintiff due to the similarity of the services offered by the parties. The court issued a permanent injunction.

In *Toys ‘R’ Us, Inc. v. Akkaoui,* plaintiff sought to enjoin defendant’s use of “any colorable variation” on its “Toys ‘R’ Us” trademark. Plaintiff claimed that defendant’s operation of a Web site under the name “Adults ‘R’ Us” infringed and diluted its mark. The court found that “[b]ecause of Plaintiff’s promotional activity and because of the mark’s inherent peculiarity, the ‘R Us’ family of marks have acquired a strong degree of distinctiveness.” The court ruled that defendant’s use of “Adults ‘R’ Us” tarnished plaintiff’s mark by associating it with a line of sexual products inconsistent with the image Toys ‘R’ Us had “striven to maintain.” The court enjoined defendant from using any Internet domain name ending in “R Us.”

4. Non-Trademark Holder Innocently Using a Company’s Trademark

Another increasingly common domain name dispute occurs when a legitimate business innocently chooses a domain name that turns out to be trademarked by another company. The registrant may choose the domain name for business purposes, unaware of the superior trademark rights of another company, and thereafter invest considerable time and energy into developing and publicizing the Web site and its domain name.

138. See id. at 738.
139. Id. at 740-41.
140. See id. at 737. See also Lozano Enters. v. La Opinion Publ’g Co., No. CV-96-5969, 1997 WL 745036 (C.D. Cal. July 31, 1997).
The registrant's lack of guile is unlikely to insulate him from strict enforcement of the trademark laws. In TeleTech Customer Care Management, Inc. v. Tele-Tech Co., defendant had a registered domain name "teletech.com." Plaintiff had been using the mark "TeleTech" long before defendant's first use of the domain name. Defendant claimed that it selected the domain name "teletech.com" because it was unaware that "tele-tech.com" (with a hyphen) could be used as a domain name. The court found that "the reason why Defendant adopted the diluting domain name is not relevant" for purposes of the motion at issue. Although defendant had invested a considerable amount of resources in the domain name "teletech.com," the court enjoined defendant's use because of plaintiff's superior trademark rights.

In Interstellar Starship Services Ltd. v. Epix, Inc., Epix had registered the trademark "EPIX" with respect to "printed circuit boards and computer programs for image acquisition, processing, display and transmission." Interstellar Starship registered the domain name "epix.com" to publicize the activities of a theatre group called the "Rocky Horror Picture Show." Although Interstellar Starship also owned a consulting business in the field of "design for test" circuit boards, its "epix.com" site was used solely to publicize the Rocky Horror Picture Show. The court concluded it was therefore unlikely to confuse any actual or potential customer seeking to purchase printed circuit boards and computer programs from Epix. Accordingly, the court held that Interstellar Starship did not infringe Epix's trademark.

5. Concurrent Trademark Rights

Because trademark law recognizes that multiple parties may have trademark rights to the same mark, but the Internet domain name system permits only one user of a given domain name, disputes will inevitably arise between two concurrent

145. See id. at 1410.
146. Id. at 1413.
147. See id. at 1412. The court determined that the balance of hardships tipped sharply in favor of the plaintiff because "[d]efendant's use of the domain name 'teletech.com' prevents Plaintiff from using its company name and registered service mark as its domain name, while Defendant is free to use, and in fact has started using, the domain name "tele-tech.com" as an alternative domain name." Id.
149. Id. at 1333.
150. Id. at 1336.
151. See id.
trademark holders over the same domain name. Although there are no reported cases, these battles may be determined by traditional trademark infringement law. As long as the use of a mark as a domain name in no way confuses the public as to the source of goods or services, the courts may permit the prevailing "first come, first served" registration policy to govern the outcome of domain name disputes between concurrent trademark holders.

C. Content Liability

Web commerce and communication increase the potential for false advertising, defamation, and securities law violations because the Web provides relatively inexperienced users with easy access to global audiences and perhaps greater opportunities for consumer confusion. The nature of the Internet—providing instant digital copies anywhere in the world—also makes copyright issues particularly important. Because the perpetrators of defamation and infringement in cyberspace may be anonymous or pseudonymous, and those perpetrators receive their forum from online access providers or ISPs, those access providers and ISPs often find themselves named as defendants. At the same time, the need to vigilantly curb online abuses and hold culpable parties responsible must be tempered by the need to minimize regulations that will chill the free and constructive development of the Internet.

1. False Advertising, Securities Violations, and Defamation

Web sites that advertise products or services may be subject to liability if they are misleading. Federal challenges to false advertising and unfair business practices are usually brought under § 43(a) of the Lanham Act, which prohibits the use of a false or misleading description or representation in connection with goods or services. The FTC is presently determining the

---

152. "While courts have not yet decided such a case, there is no reason that they cannot be handled like any other traditional trademark infringement case." Chris Bovenkamp, Does the Bottle Need to Be Broken: The Future of Trademarks and Domain Names (Revised Nov. 18, 1996) <http://www.law.ttu.edu/cyberspc/jour11.htm#tech>.


154. Id. To prevail, a plaintiff must prove that the promotional statement was (1) false or misleading, (2) in interstate commerce, (3) in connection with goods or services, (4) in commercial advertising or promotion, (5) misrepresentative of the nature, qualities, or geographic origin of the goods, services, or commercial activities, and (6) actually or likely damaging to the plaintiff. See McCarthy, supra note 34, § 27:24, at 27-39.
extent to which it will apply consumer protection regulations of the FTCA to Internet commerce, including the form of consumer disclosures it will require in electronic advertising. In addition, because a Web site may be accessed anywhere in the world, its content may be judged under the laws of states or other countries which set forth their own false advertising and unfair practices statutes or specific requirements for Web commerce.

If the Web site is owned by a public company, statements on the site may also give rise to liability under state and federal securities laws, to the extent those statements are misleading, lack meaningful disclaimers or cautionary language, or provide stale information despite their appearance of being up to date.

Fundamental to the nature and promise of the Web are "links" and "frames," which permit Internet users to move from one site to another with the click of a computer mouse. Nevertheless, maintaining links to or frames of other sites may give rise to claims under the federal Lanham Act, Copyright Act, and state causes of action for false advertising or unfair competi-

---

155. The Federal Trade Commission Act ("FTCA"), prohibits "[u]nfair methods of competition" and "unfair or deceptive acts or practices in commerce." 15 U.S.C. § 45 (1994). The FTC will find deception if "there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." See Southwest Sunsites, Inc. v. F.T.C., 785 F.2d 1431, 1435 (9th Cir. 1986). See also supra notes 36-37 and accompanying text.

156. See, e.g., CAL. BUS. & PROF. CODE §§ 17200 (West 1997) (defining unlawful, unfair, or fraudulent business acts or practices); § 17500 (West 1997) (prohibiting false advertising); § 17506 (West 1997) (providing penalties for unfair competition); § 17538 (West 1997) (requiring vendors on the Internet, as well as vendors using traditional telephone, mail, and catalog media, to disclose their return and refund policies and legal name and address); CAL. CIV. CODE §§ 1770(a), 1780(a) (West 1997) (providing cause of action under Consumers Legal Remedies Act for misrepresentations concerning goods).


158. Clicking on a hyperlink (which appears as highlighted text on a Web page) transports the user to another site or another page within the same site. Clicking on certain other symbols or text does not actually transport the user to another site, but displays another site within a "frame" that often displays the original site's logo or advertising.


tion, particularly if the link or frame does not clearly distinguish between the original site and the linked or framed site.

Many Web sites host forums or bulletin boards on which subscribers or other visitors may post messages. The ability to communicate with vast numbers of readers at little or no cost—and often anonymously—has encouraged the widespread dissemination of offensive or defamatory material on the Internet. Although those who post such messages may be liable for defamation, their frequent anonymity, the relative deep pockets of the company hosting the forum or bulletin board, and the function of access providers as gatekeepers to cyberspace, often result in defamation lawsuits against ISPs, BBS operators, and other access providers.

Significant litigation has addressed whether an ISP may be liable for defamatory messages posted by subscribers. Courts have held that the ISP would be strictly liable if it exercised control over content and was thus a "publisher," but it would not be liable, absent knowledge of the defamation, if it were merely a "distributor" of the underlying message.

161. In Ticketmaster Corp. v. Microsoft Corp., Case No. 97-3055 (C.D. Cal., filed Apr. 28, 1997), Microsoft linked its Seattle Sidewalk Web site to internal pages of Ticketmaster's Web site. Ticketmaster sued Microsoft for trademark dilution, violations of the Lanham Act, and violation of state unfair trade practices laws. In Washington Post Co. v. TotalNews, Inc., Case No. 97 Civ. 1190 (PKL) (S.D.N.Y., filed Feb. 20, 1997), defendant owned and operated a Web site that framed the sites of plaintiff newspapers, while running its own advertisements on the site as well. Plaintiffs brought claims for, among other things, misappropriation, trademark dilution, trademark infringement, and copyright infringement. The case settled, with defendants agreeing to link, but not frame, plaintiffs' sites.

162. The resources and sophistication of online access providers vary greatly. America Online has over 10 million subscribers. See Chris Albritten, America Online Tops 10 Million Subscribers: Half of U.S. Households on Internet Use Service, WASH. POSR, Nov. 18, 1997, at D3. Some BBSs, on the other hand, are extremely small operations run from a home.

163. In Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) allegedly defamatory statements about plaintiff appeared on a forum sponsored by online service provider CompuServe. Plaintiff sued CompuServe. The court held that CompuServe was the equivalent of a library, was entitled to the same First Amendment protection as a news vendor, and therefore would be subject to liability for infringement only if it knew or had reason to know of the allegedly defamatory statements. The court held that CompuServe was not liable because it had no more editorial control over the publication than a library or bookstore or newsstand and it would not be feasible for CompuServe to examine and protect against potentially defamatory material. In Stratton Oakmont, Inc. v. Prodigy Services, Co., 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 26, 1995), Prodigy was held to be a "publisher" and therefore subject to liability for defamation regardless of actual or imputed knowledge, for allegedly defamatory messages posted by an anonymous Prodigy subscriber on a bulletin
Under § 230(c)(1) of the Communications Decency Act, ISPs are now immune from liability for information originating with a subscriber. Although § 230(c)(1) provides by its terms that ISPs and other providers or users shall not be treated as the “publisher or speaker” of information originating from someone else, the Fourth Circuit in Zeran v. America Online, Inc., has interpreted § 230(c) to bar liability for ISPs even if they could be characterized under prior cases as a “distributor.”

In Zeran, a subscriber to America Online ("AOL") posted plaintiff's name and phone number on advertisements for offensive t-shirts celebrating the bombing of the Oklahoma City federal building. Zeran complained to AOL, which removed the notice, but the notice reappeared repeatedly. Zeran was bombarded with hostile and offensive telephone messages. Zeran sued AOL for negligence on the ground that AOL knowingly distributed defamatory material. The court held that § 230(c)(1) preempted Zeran's state claim and provided immunity for ISPs. Although § 230 referred to "publishers," the court concluded that the term embraced all editorial functions, including

---


No provider or user of an interactive computer service shall be held liable on account of

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material [provided by another information content provider].


165. 129 F.3d 327 (4th Cir. 1997).


167. See id. at 329.

168. See id. at 331.
whether to publish, withdraw, postpone, or alter content. The court explained that the immunity of § 230(c) is intended to remove the disincentives ISPs would otherwise have to monitor the communications made by their subscribers, while avoiding the chilling effect on free speech that would result if ISPs had to regulate content under the specter of strict liability.

2. Copyright Infringement

The ease of copying material on the Internet, the quality of digital copies, and the global scope of distribution make copyright protection in cyberspace more important, yet more difficult. The technology of cyberspace also makes copyright analysis more complex, because a number of "copies" of works are made automatically (and often without the knowledge of users) during the transmission process.

Copyright protection subsists in original works of authorship fixed in any tangible medium of expression, including literary works, music, graphics, pictures, and video. With certain exceptions, the owner of the copyright to that work has the exclusive right to copy, distribute, perform, and display the work and prepare derivative works based upon it. A person who commits any of those acts without the permission of the copyright holder may be liable for direct copyright infringement. Thus, those who place an unauthorized copy of a copyrighted work on the Internet are liable for direct copyright infringement. In addition, the BBS operator or other third party that distributes the unauthorized copy may be liable for direct infringement of the copyright holder's exclusive right of distribution, whether the third party knew the material was infringing or not.

Technically, a BBS operator or Internet access provider makes a "copy" of an infringing document automatically during the process of transmitting the original infringer's message. These automatic copies, however, do not give rise to direct copyright infringement. Nonetheless, a BBS operator, ISP, or

---

169. See id. at 332.
other third party may still be liable for copyright infringement perpetrated by someone else, based on theories of contributory or vicarious infringement.

Contributory copyright infringement may arise if a BBS operator (1) knew of the infringement and (2) materially contributed to it (e.g., by providing the means and encouragement) or substantially participated in it (e.g., by failing to cancel the infringing message). In *Sega Enterprises Ltd. v. MAPHIA*,

[175] for example, defendants operated a bulletin board service on which subscribers were uploading and downloading unauthorized copies of Sega’s videogames. The court found that defendants could be liable for contributory infringement because they encouraged subscribers to upload and download the unauthorized copies and marketed hardware and software that could be used to make the unauthorized copies.

[176] In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, the court held that an online service provider could be liable for contributory infringement if it could be shown that the provider knew or should have known of a user’s copyright infringement after receiving notice from plaintiffs and failing to investigate.

Vicarious copyright liability may arise where the defendant (1) had the right and ability to control the wrongdoer (e.g., by shutting off access) and (2) received a direct financial benefit from the infringement.

Pending legislation may limit liability for contributory or vicarious copyright infringement. In May 1998, the Senate approved the Digital Millennium Copyright Act of 1998

[179] which, among other things, would limit the scope of service providers’ liability for copyright infringement. Essentially, ISPs would not be liable for merely transmitting infringing material. Additional legislation has been proposed to limit ISP liability on a similar basis.

[180] Netcom has caused the copying,” and direct infringement requires some element of volition).


[178] See Netcom, 907 F. Supp. at 1375. The court held that Netcom could not be vicariously liable because it did not receive a direct financial benefit from the infringement. See id. at 1377.


[180] See, e.g., the On-Line Copyright Infringement Liability Limitation Act, H.R. 2180, 105th Cong. (1997) (no direct or vicarious liability for copyright infringement for ISPs who did not place the material online, select or alter content, determine recipients of the material, benefit financially from the
D. Online and Shrinkwrap Contracting: Proposed UCC Article 2B

The Uniform Commercial Code ("UCC") provides a source of uniform contract law in the United States. All fifty states have adopted the UCC, albeit with slight variations.\(^1\) Article 2 of the current UCC addresses contracts for the sale of goods. Article 2A addresses leases of goods. Out of concern that the UCC still may not adequately address novel issues arising from electronic commerce, new provisions governing the sale or license of software programs and the license of other information may be added as UCC Article 2B.\(^2\)

At its core, proposed Article 2B attempts to adapt longstanding contract principles to the digital age, in which transactions are often consummated without the execution of a written agreement. First, Article 2B replaces the concept of a "writing" with the concept of a "record," which is defined as "information inscribed on a tangible medium or stored in an electronic or other medium and retrievable in perceivable form."\(^3\) Second, it expands the concept of "manifestation of assent," required under common law and existing UCC provisions for the formation of a contract. Under Article 2B, a person, or its electronic agent, manifests assent to a record or term in the record if, after the opportunity for review, the person or electronic agent (1) "authenticates" the record or term, (2) intends to engage in affirmative conduct and has reason to know the other party may infer assent, or (3) engages in affirmative conduct clearly indicating acceptance.\(^4\) A record or term may be "authenticated" by


\(^{182}\) Article 2B is a joint effort of the American Law Institute and the National Conference of Commissioners on Uniform State Laws. It may be added to the UCC by the summer of 1999, and may be before state legislators for adoption as state law a few months thereafter. The text of the current draft of proposed Article 2B may be found at <http://www.law.upenn.edu/library/ulc/ucc2b/2bALId98.htm>.


\(^{184}\) See id. § 2B-111. The requirement of an opportunity to review the record or term is met only if it is reasonably available and noticeable and, in some instances, there is a right to a refund if the term or record is rejected. See id. § 2B-112.
any commercially reasonable method, such as clicking on an on-screen button that says "I agree" or words to that effect.\textsuperscript{185} Under certain conditions, the contract may be formed entirely between "electronic agents"—computer programs or other automated means of initiating or responding to electronic messages\textsuperscript{186}—without the immediate knowledge or review of any human being.\textsuperscript{187} Parties can vary the effect of Article 2B's provisions by agreement.

One of the controversial provisions in proposed Article 2B confirms the enforceability of "shrinkwrap" or "click-through" license agreements. Shrinkwrap license agreements are often included inside prepackaged software, and set forth the terms of the purchase or license of the software. Although a sticker on the outside "shrinkwrap" of the package may notify the customer that use of the software is subject to further terms, the customer does not see those terms until after purchasing the software and opening it. A similar arrangement for transactions conducted online is often referred to as a "click-through" license agreement. A user or purchaser of software online must click "I agree" or make some other affirmative act, and thus become bound to the stated terms, before being able to access the software.

Arguably, a shrinkwrap license could be deemed unenforceable as an adhesion contract, forced upon consumers by vendors with superior bargaining power.\textsuperscript{188} At least one court has decided that, if the parties' negotiations have been sufficient to form a contract, the terms subsequently unveiled in a shrinkwrap format might be viewed as proposed modifications, which would not be enforceable without actual assent.\textsuperscript{189} Recent decisions, however, generally favor enforcement of shrinkwrap licenses, at least where the purchaser receives notice on the outside of the package that additional terms are included inside, and the purchaser has the option of receiving a full refund after reviewing those terms.\textsuperscript{190}

\textsuperscript{185} See id. § 2B-111, Reporter's Notes 4 & 5, Illustration 1. See also id. § 2B-114 (commercial reasonableness of attribution procedure).
\textsuperscript{186} See id. § 2B-102(a)(21).
\textsuperscript{187} See id. § 2B-119 & Reporter's Notes.
\textsuperscript{188} See Vault Corp. v. Quaid Software Ltd., 655 F. Supp. 750, 761 (E.D. La. 1987), aff'd, 847 F.2d 255 (5th Cir. 1988). An adhesion contract is a standardized contract imposed by a party of superior bargaining strength, on a "take it or leave it" basis.
\textsuperscript{189} See Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991).
\textsuperscript{190} In ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), the court enforced a shrinkwrap license which restricted use of data on an accompanying CD-ROM database to noncommercial purposes. The court reasoned that not
Article 2B addresses shrinkwrap and click-through license agreements under the rubric of "mass market licenses." Under Article 2B, a mass market license is a standard form that is prepared for and used in a "mass market transaction," which generally includes all consumer transactions and some transactions involving businesses.\(^1\) A party is bound by all of the terms in a mass market license, whether or not the terms were actually known or understood, as long as the party agrees or manifests assent at or before the initial use of or access to the information.

Article 2B would give customers greater protection than they have under current law. If the customer does not like the post-sale terms, under Article 2B it can return the product, and the licensor must bear the costs of return. Furthermore, Article 2B extends these protections to business customers as well as individual consumers.

On the other hand, Article 2B would expand the circumstances in which shrinkwrap and clickwrap licenses would be enforceable. While post-sale terms have been enforced when circumstances made it impractical to require all of the terms to be stated at the point of sale, post-sale terms could be enforced under Article 2B even where the licensor could have conveniently spelled out the terms before the sale. In addition, Article 2B permits contract terms to change continuously over the life of a mass market contract. Under Article 2B-304, a user must be notified of any such change, but this notice might be accomplished by merely posting changes on a Web page or other accessible location the user knows about, rather than providing notice to the consumer directly. Upon discovering the change, the customer may cancel the contract if the change is unacceptable and all the terms of a contract have to be spelled out at the outset, at least if the buyer may receive a full refund after reviewing the complete terms. The court also noted it would be impractical to require software vendors to state all terms outside the package at the point of sale. On similar grounds, the court in *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997), cert. denied, 118 S.Ct. 47 (1997), enforced an arbitration clause that was inside the package, based on the user's mere failure to object to the clause.

\(^1\) Specifically, the December 1998 draft of Article 2B-102(a)(33) defines a mass market transaction as "a consumer transaction" or "a transaction with an end-user license which transaction involves information or informational rights directed to the general public as a whole under substantially the same terms for the same information." The definition excludes certain transactions including customized work specially prepared for the licensee, public performances, site licenses, and redistribution and access contracts. *See U.C.C. § 2B-102(a)(32) (A)-(E) (Proposed Draft December 1998)* (visited Jan. 11, 1999) <http://www.law.upenn.edu/library/ulc/ucc2b/2bALId98.htm>.
the term is material, but apparently cannot opt to continue the contract upon its original terms.\textsuperscript{192}

Finally, Article 2B may be preempted by federal copyright law, which permits the public to use copyrighted material (including software) for certain purposes, such as the purpose of "fair use," without any license at all. By enforcing the terms of a shrinkwrap license, Article 2B would give licensors more power than they would have under the Copyright Act, and to that extent be contrary to the terms or intent of that Act. Indeed, in \textit{Vault Corp. v. Quaid Software Ltd.},\textsuperscript{193} the court refused to give effect to a Louisiana state shrinkwrap law purporting to validate license restrictions against backup copying, modifying software and reverse engineering, holding that the law was preempted by provisions of the Copyright Act which permit such uses.\textsuperscript{194} In \textit{ProCD, Inc. v. Zeidenberg},\textsuperscript{195} on the other hand, the court held there was no preemption because, whether the material was protected by copyright law or not, the parties could enforce the terms of private contracts.\textsuperscript{196}

\textbf{E. Privacy}

As transactions proliferate on the Web, customers grow increasingly concerned about privacy, especially when they are required to provide personal information in order to complete a transaction. While users are particularly concerned about the security of their medical or financial information, they are often unaware, and disturbed to discover, that personal information is also collected and stored without their knowledge in the form of "cookies." A "cookie" is a file generated by the Web browser on the user's hard drive in response to directions from a Web site the user has visited. The cookie keeps information about the user or the visit and provides it to the Web site each time the user revisits the site.\textsuperscript{197}

\begin{itemize}
\item \textsuperscript{192} Nevertheless, customers would still be protected against unconscionable terms under Article 2B-208(a)(1).
\item \textsuperscript{193} 847 F.2d 255 (5th Cir. 1988).
\item \textsuperscript{194} See \textit{id.} at 269-70.
\item \textsuperscript{195} 86 F.3d 1447 (7th Cir. 1996).
\item \textsuperscript{196} See \textit{id.} at 1454-55.
\item \textsuperscript{197} There is some benefit to these cookies, because they relieve users from having to re-enter certain information each time they visit the site. Some companies, however, sell the personal information obtained from users to third parties, or track the user's "click stream"—showing all the Web sites the user has opened. A service or access provider may maintain a record of a user's e-mail communications as well.
\end{itemize}
No federal statute specifically prohibits the collection or distribution of personal information collected online, Although numerous bills have been introduced in Congress, The FTC, however, has announced four elements critical to the protection of consumer privacy: (1) notice to consumers about how personal information collected online is used; (2) choice for consumers about whether and how their personal information is used; (3) security of personal information including reasonable steps by data collectors to guard against loss or misuse; and (4) access for consumers to their own personal information to ensure accuracy.

The FTC will apparently take an aggressive position with respect to the online collection of data from children. In July 1997, after investigating an interactive Web site that targeted children, the FTC set forth the following guidelines: (1) "[i]t is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose" when it will also be used for another purpose (such as marketing), without a disclosure; (2) any such disclosure must be made to the parent; (3) for a notice to be adequate, it should include "who is collecting the personally identifiable information, what information is being collected, its intended use(s), to

198. The Electronic Communications Privacy Act of 1986 prohibits, among other things, the interception of e-mail. 18 U.S.C. § 2510 (1994). It also prohibits unauthorized disclosure of or access to stored electronic communications. See id. § 2701.

199. The Communications Privacy and Consumer Empowerment Act, H.R. 1964, 105th Cong. (1997), would require the FTC to announce rules ensuring that consumers (1) have knowledge that consumer information is being collected about them, (2) receive conspicuous notice that the information could be provided to third parties for purposes unrelated to the transaction, and (3) be allowed to exercise control over the collection of personal information. The proposed Data Privacy Act, H.R. 2368, 105th Cong. (1997), calls for the computer industry to (1) develop voluntary guidelines for notifying customers before collecting information, (2) advise customers of third party recipients, and (3) allow customers access to verify their personal data and prohibit disclosure. See also Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong. (1997) (prohibiting disclosure of subscriber's personally identifiable information by a computer service without prior written consent); Children's Privacy Protection and Parental Empowerment Act of 1997, H.R. 1972 and S. 504, 105th Cong. (1997) (prohibiting sales of personal information about children without consent of a parent).

200. The FTC defines "personal identifying information" to include name, physical and e-mail address, phone number, and information that is identifiable to a specific individual. GeoCities; Analysis to Aid Public Comment, 63 Fed. Reg. 44624, 44625 (1998).

201. See BUREAU OF CONSUMER PROTECTION, FTC, PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE (1996).
whom and in what form it will be disclosed to third parties, and the means by which parents may prevent the retention, use, or disclosure of the information."  

In 1998, the FTC accused GeoCities, an ISP, of disclosing members' personal information to third parties in violation of GeoCities' stated privacy policy, misrepresenting to whom children's personally identifiable information would be disclosed, and failing to identify how it would use member information. GeoCities entered into a consent decree by which it agreed to post on its Web site a clear and prominent privacy notice that would (1) give adequate notice of GeoCities' information and disclosure practices; (2) provide users the ability to delete their personal information from GeoCities' databases; and (3) clearly identify its affiliation with third parties that may collect information. In addition, GeoCities will have to obtain parental consent before collecting and using personal information obtained from children under thirteen.

The laws of individual states and foreign countries may also impose obligations with respect to data collection. The European Union's Data Protection Directive, for example, is requiring member countries to maintain laws protecting personal information. It also prohibits companies operating in the EU from transmitting personal data electronically to countries lacking adequate protections for the information.

One means of helping to secure private information is data encryption. In general, encryption is a process that converts data into a form that cannot be read without a decryption key. The longer (and thus more sophisticated) the string of code in the decryption key, the more secure the information. Due to the Federal Government's national security concerns, however, federal laws currently prohibit the exportation of more sophisticated encryption technology unless law enforcement has access


204. See, e.g., CAL. CONST., art. I, § 1 (including privacy as a fundamental inalienable right); Porten v. Univ. of San Francisco, 134 Cal. Rptr. 839, 841-42 (1976) (recognizing private cause of action based on California Constitution, article I, § 1); RESTATMENT (SECOND) OF TORTS § 625B (1977).

Companies must therefore develop different encryption methods for domestic and export use, which is impractical, or offer only weak encryption, which may not generate the public confidence necessary for the future of commercial transactions. Meanwhile, foreign encryption products are proliferating, putting U.S. encryption products at a competitive disadvantage. Pending legislation known as the "Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act," would ease federal restrictions on the export of encryption products.

III. Conclusion

The turn of the century brings exciting opportunities for commerce, education, and entertainment as cyberspace grows larger and the physical world becomes effectively smaller. This potential, however, does not come without challenges. Companies must protect themselves from the disruption of the Y2K problem and the litigation that will inevitably occur. Web site owners must take care not to become unduly subject to foreign laws and distant forums and sacrifice the benefits of interactivity with users. There must be a fair process for allocating Web site domains, a balance of the Internet's frontier character and regulations protecting against abuses, and privacy measures sufficient to assure the public that Internet commerce is secure.

In particular, companies should expect a number of legal developments in the dawning of the twenty-first century. First, it will be increasingly important for companies to document their diligence in assessing Y2K problems (including those caused by the Y2K shortcomings of vendors, information suppliers, and others), establishing and implementing Y2K solutions, testing them, and developing contingency plans. Second, as companies fail to meet business obligations due to Y2K problems, they will seek to shift losses and deflect responsibility by bringing claims for negligence, breach of contract, fraud, and indemnification against third parties. Third, Y2K problems will provide plaintiffs' lawyers further ammunition in arguing that the securities of public companies were sold without adequate disclosure of material facts. Fourth, companies will need to be more vigilant about the content of their Web sites, guarding against stale information, misleading information, trademark and copyright infringement,

and inappropriate links. Fifth, false advertising claims under common law and the FTCA will increase, particularly in the areas of Y2K disclosures, online privacy, and advertising on the Web. Sixth, legislators will attempt to address Y2K and online commerce by introducing legislation, but they will likely find that technology moves too quickly for the legislative process. Only as the law and industry resolve these issues, will the promise of twenty-first century technology come to fruition.