Loyola Consumer Law Review

Volume 10 | Issue 1 Article 12

1998

The Internet: An Introduction to Basic Legal Risks That Impact Consumers

Gary Fresen
Partner, Baker & McKenzie, Chicago, IL

The Internet: An Introduction to Basic Legal Risks That Impact Consumers

By Gary Fresen[1]

I. Introduction

The Internet's unprecedented connectivity among people throughout the world enables an exchange of ideas and information on a massive scale. It is a new medium, not just a new technology, which holds the potential for establishing innovative means of communication to reach consumers wherever they are located. The message to business is clear: to compete effectively in the global marketplace, organizations must embrace imaginative ways of conducting business that utilize the expansive connectivity that the Internet offers.

When consumers evaluate the many alternative methods businesses use to reach them, it is necessary to consider a host of liability, privacy, and security risks previously not encountered and on a scale not previously achievable. This article will describe some features of the Internet, highlight a number of its vulnerabilities, and discuss the legal implications for consumers.

Prior to 1995, the Internet was relatively obscure and hidden from public view. Residing primarily in universities, national laboratories, and the military, most consumers had no reason to be aware of its existence or understand its subtleties. By 1995, however, the Internet had burst into public consciousness. To accommodate this new medium, the legal system must adapt traditional doctrines and adopt new concepts to establish a framework of fairness in

Gary Fresen is a litigation partner of Baker & McKenzie's Chicago Office and a member of the Firm's Global Intellectual Property and Information Technology Practice Group. A graduate of Loyola University Chicago School of Law, he served on the American Bar Association Information Security Committee, which reviews technology issues such as the Digital Signatures Guidelines published in 1996, and he is Chair of the Electronic Evidence Subcommittee. He was an active participant in the Chicagoland Chamber of Commerce's National Information Commerce Committee. He has participated in numerous seminars dealing with the Internet, Digital Signatures, Year 2000 and other issues. In his eighteen years of practice, he has tried numerous cases to verdict in the federal and state courts in Illinois.

His paractice is concentrated in areas of commercial litigation and alternative dispute resolution, but recently he has devoted much of his time to counseling the Firm's clients regarding issues related to electronic commerce, encryption, the Internet, and information technology. Contact him at <gary.w.fresen@bakernet.com>.

assessing liability and protecting consumers' rights. For courts and legislatures struggling to address Internet issues, the primary difficulty occurs in finding the right analogy to apply when adapting existing laws to the Internet. In *American Libraries Association v. Pataki*,[2] Judge Preska illustrated this dilemma with these observations:

> The Internet may well be the premier technological innovation of the present age. Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity. Not surprisingly, much of the legal analysis of Internet-related issues has focused on seeking a familiar analogy for the unfamiliar. Commentators reporting on the recent oral argument before the Supreme Court of the United States, which [was] considering a First Amendment challenge to the Communications Decency Act, noted that the Justices seemed bent on finding the appropriate analogy which would tie the Internet to some existing line of First Amendment jurisprudence: is the Internet more like a television? a radio? a newspaper? a 900-line? a village green? [citations omitted.] This case, too, depends on the appropriate analogy. I find, as described more fully below, that the Internet is analogous to a highway or railroad. This determination means that the phrase "information superhighway" is more than a mere buzzword; it has legal significance. . . .[3]

As Judge Preska recognized,[4] the Internet represents a new consumer medium. The Internet is different from anything consumers have used in the past. Due the Internet's unprecedented speed of communication, consumers can interact with businesses virtually instantaneously. In addition, consumers can access products and services throughout the world with the click of a mouse. Thus, the Internet's speed and interconnectivity present new challenges to a legal system designed to protect consumers. A brief description of the size and growth of the Internet reveals the magnitude of these challenges.

A. Size and Growth of the Internet

The sheer size and growth of the Internet is astonishing. An estimated 40 million people around the world currently use the Internet.[5] The scope of information available boggles the mind. In 1996 AltaVista, an Internet search engine, claimed that it provided consumers access to a database of 11 billion words, collected from 22 million pages found on 225,000 servers, and 3 million articles from 17,000 Usenet groups.[6] Further, it claimed that users accessed its search engine over 8 million times daily.

Moreover, Internet usage keeps growing. The number of e-mail addresses doubles every year, the number of hosts doubles every six months, and the number of World Wide Web sites doubles every three months. Promoters constantly announce new services. A host of new software products offer a variety of multimedia interfaces to entertain the viewer and present information.

Whole categories of Internet usage expand and change with the imagination of entrepreneurs. A multitude of user-specific groups offer discussions on almost any topic. Users can access government documents, judicial opin-

ions, magazine articles, and, of course, e-mail. This unprecedented growth illustrates the importance of resolving legal issues raised by consumer use of the Internet. Given the sheer size and growth of the Internet, a basic definition is helpful.

B. Defining the Internet — What It Is (And Is Not)

The Internet is a voluntary association of computer network systems which comprise a "network of networks."[7] A history of the Internet is available from the "Father" of the Internet and President of the Internet Society, Vinton G. Cerf.[8] In addition, a technical description of this medium is readily accessible: the Internet is a collection of standard "protocols" which enable dissimilar computer systems and networks to exchange information. Some of the more popular protocols include: e-mail (electronic messaging), file transfer protocol (file transferring), World Wide Web (graphical interface utilizing links within hypertext documents), telnet (telephone network connections), IRC (Internet Relay Chat), and gopher (information organization).[9] A user links to his organization-specific network which, in turn, connects through the gateway of an Internet Service Provider ("ISP") to a network routing system that makes resources available regionally, nationally, and throughout the world. Although this description provides a technically adequate definition of the Internet, a simple, accurate description is difficult to formulate.[10]

In practical terms, the Internet allows millions of computer users to share information, execute data searches, send electronic mail, and access remote computers. However, "it isn't a program or even a particular computer resource. It remains only a means to link computer users together."[11] Furthermore, the Internet is not a service; rather, it is really a pipeline for providing services. Additionally, no individual owns the Internet. Various organizations pay for the telephone lines linking their computers, and individual consumers pay an ISP for access to the Internet via its server.

Although computer experts can describe the technical aspects of the Internet with some precision, the average consumer may experience some frustration in grasping the sheer magnitude of this new medium. This article attempts to help consumers discern the implications of this new consumer medium and to understand the legal issues raised by their Internet use. Section II provides a brief description of various Internet services. This article then explores the intellectual property issues raised by use of bulletin board systems, LISTSERV and Usenet groups, and domain names. In Section IV, the article analyzes the unique jurisdictional issues posed by Internet use. Section V examines potential criminal implications of Internet use, including obscenity, fraud, theft, and on-line gambling issues. The article then explains in Section VI how federal preemption of state defamation actions poses potential pitfalls for Internet users. Finally, Section VII analyzes how governments have utilized regulation as a partial solution to some of these issues. Before examining specific legal issues raised by the Internet as a new consumer medium, it is helpful to discuss some of the Internet's basic features and services.

II. Brief Description of Internet Services

A. E-mail — Electronic Mail Messaging

The Internet's most basic and popular form

of communication is e-mail — a message in digital form typically transmitted from one user's computer via modem to an organization which provides Internet access. The access provider, known as an internet service provider ("ISP"), might be one of the large on-line services (such as CompuServe, America Online or Microsoft Network), some other generally recognized access point (such as an academic institution), or even a local ISP set up in someone's basement.

The e-mail sender typically utilizes a piece of software, known as a mailer, to prepare a message. The mailer uploads the message to the appropriate ISP. The message may consist of text alone, as well as graphic images, sounds, or entire computer programs attached to the text as files.

When creating an e-mail message, the author assigns a destination address. The mailer then breaks the message down into smaller pieces known as packets. The packets travel separately across the networks but ultimately recombine at the destination. During the trip, the packets bump along from router to router through bridges and switches. Each router or switch looks at the packet's destination, without inspecting its contents, and decides the best way to pass it along.

B. LISTSERV and Usenet Groups

While e-mail allows one-to-one messaging, it also permits a one-to-many mode of operation. "LISTSERV"[12] and "Usenet"[13] groups are variations on basic e-mail.

"LISTSERV" is a distribution list management package. LISTSERV servers maintain lists of computer users' names and electronic mail addresses. Any member of a list can utilize the LISTSERV server to send an e-mail message to all members of the list. This service provides a convenient means for the exchange of ideas and information between list members. Many different lists exist; each one contains members who share a particular interest.

Usenet has evolved to include over 10,000 separate newsgroups covering a myriad of topics. While some newsgroups are "moderated" so that messages must be approved before users can access them, most newsgroups are unmoderated. Anyone can place and read messages in an unmoderated news group.

C. File Transfer Protocol

Another major feature of the Internet is File Transfer Protocol ("FTP"),[14] which allows users to access and download files from thousands of Internet archives. Typically, an organization creates a directory or a database to allow remote access to its data files. Using FTP, a remote Internet user can download a wide variety of files, usually free of charge.

D. World Wide Web

Today, the World Wide Web is virtually synonymous with the Internet. The Web works like file transfer in the sense that consumers accessing a home page are downloading files onto their own computer hard drives. On the Web, most files are written in Hyper Text Mark-Up Language ("HTML"). When a computer receives an HTML file, a user's "browser" software[15] immediately interprets the file and creates an image on the user's screen. The file will invariably include the addresses of other "sites" on the Web that a user can access simply by "clicking" on a highlighted description of the other site. From the consumer's point of view, the Web thus allows users to jump effortlessly from one site to another or "surf" the Web.

E. Bulletin Boards

A computer "bulletin board" system ("BBS")[16] represents another type of e-mail communication. A consumer "posts" a message to a computer that houses the bulletin board and is controlled by the Systems Operator. The message may be simply text or may include other file formats. The computer housing the bulletin board (the "host computer") may automatically forward the message to users who have subscribed to the board. Alternatively, subscribers may obtain the message by accessing the host computer and downloading the file into their computers' hard disks. There are thousands of different bulletin boards available on the Internet, ranging from discussion of Star Trek[17] to law and the information superhighway.[18] Some bulletin boards restrict those who can subscribe while others are open, although the user may have to register.

This brief discussion of Internet services highlights the unprecedented accessibility and global reach it offers. Despite the claims of some theorists that the Internet exists in cyberspace, a land without rules, there is no doubt that law will govern activities that transpire on the Internet. The Internet exists in the real world and is used by real people doing real things. Thus, the question is not *whether* law will prevail. Instead, the more difficult issues involve *whose* law will govern, and how traditional doctrines will be adapted to the new medium. In this uncertain legal environment, the Internet poses many traps for the unwary consumer.

III. Intellectual Property Law and the Consumer

A. Copyright Infringement

Perhaps the most interesting legal issues for consumers relates to intellectual property generated by Internet use. In a short span of time, the Internet evolved into a powerful global communications medium, and intellectual property laws protect much of the material transmitted over the Internet.

The forms of material transmitted over the Internet are not unfamiliar to the intellectual property lawyer, so why does transmission over the Internet generate novel legal issues? The Internet reflects two key attributes. The first is the ease of use and nominal cost associated with transmitting files over the Internet. Copyright law was born during the age of the printing press. Development of the printing press enabled people to mass-produce copies of an author's work. The Internet represents an equally dramatic leap in technology. The Internet's ease of use and low cost of transmission render traditional copyright rules incapable of offering the same protection in the Internet era as they did for the printed word. Consumers access and distribute material on the Internet quickly and easily, sometimes without regard to a document's copyright protection.

The second key characteristic of the Internet is its global reach. The central problem posed by the Internet's trans-border reach is that laws of more than one jurisdiction may apply. This certainly holds true for intellectual property laws. The classic situation involves infringing consumers who legally obtain copies of a work in one jurisdiction and then distribute unauthorized copies in another jurisdiction. It is usually too expensive to proceed against all those who

obtain infringing copies. In these cases, enforcement of an owner's copyright may prove impractical to guard against consumers who receive and transmit illegal copies over the Internet.

1. Bulletin Boards and Illegal Copying

Bulletin Boards offer opportunity for wrongdoing by those seeking to misappropriate the property or persona of others. Certain BBS operators have openly encouraged unlawful copying by allowing subscribers to download copyrighted pictures and computer programs. Several high-profile cases illustrate the danger of these practices.

For example, in *Playboy Enterprises, Inc. v. Frena,*[19] a copyright owner sued a BBS operator for copyright infringement. Playboy claimed that the BBS operator copied and distributed unauthorized copies of Playboy's copyrighted photographs.[20]

The BBS operator admitted that he displayed Playboy's photographs on his BBS and that each of the graphics files containing photographs was downloaded by his customers. However, the BBS operator claimed that he never personally uploaded any Playboy photographs onto the BBS. Instead, he claimed that unidentified customers uploaded the photos.

To prove the BBS operator infringed its copyrights, Playboy had to establish that it owned the copyright and that the BBS operator copied the copyrighted photographs.[21] The BBS operator did not dispute Playboy's ownership of the photo copyrights. However, the court explained that "direct evidence of copying is rarely available in a copyright infringement action."[22] As a result, the court allowed Playboy to "inferentially" prove the BBS operator copied its photos.[23] To accomplish this, Playboy had to show that the BBS operator "had access to the allegedly infringed work, that the allegedly infringing work is substantially similar to the copyrighted work, [citation omitted] and that one of the rights statutorily guaranteed to copyright owners is implicated by [the BBS operator's] actions."[24]

Next, the court explained that "access to the copyrighted work" and "substantial similarity" were undeniable in this case.[25] The court then considered whether the BBS operator violated a right statutorily guaranteed to copyright owners by 17 U.S.C. § 106.[26] The court held that "[p]ublic distribution of a copyrighted work is a right reserved to the copyright owner, and usurpation of that right constitutes infringement."[27] Applying this concept, the court found that the BBS operator implicated Playboy's right to distribute copies of its photographs, regardless of whether the BBS operator personally made the copies.[28] In addition, the court held that the BBS operator infringed upon the Playboy's right to publicly display its copyrighted works.[29] Accordingly, the court granted Playboy summary judgment on its copyright infringement claim.

Another case, *Sega Enterprises, Ltd. v. MAPHIA,*[30] provides an example of the pitfalls BBS operators and subscribers encounter when they upload and copy copyrighted works. In *Sega Enterprises,* a young BBS operator encouraged its subscribers to upload and download unauthorized copies of Sega video games. The court enjoined the BBS operator from continuing these practices.[31] In addition, investigators seized copies of Sega's copyrighted video games and deleted them from the host computer's memory. The court found that copying occurred when users uploaded and downloaded unauthorized copies of the games. Although the BBS operator argued that he was unaware of the infringement, the court held that his providing "facilities, direction, knowledge

and encouragement, amounts to contributory copyright infringement."[32] A contributory copyright infringer is "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[33] Thus, *Sega Enterprises* extends contributory copyright infringement liability to BBS operators who allow subscribers to utilize the BBS to make unauthorized copies.

Another provocative decision involved a different technology, hand-held pagers. In *National Basketball Association v. Motorola, Inc.*,[34] the United States Court of Appeals for the Second Circuit held that using a hand-held pager to transmit scores and other information during National Basketball Association ("NBA") games did not constitute misappropriation of information. The court noted that the Motorola service only reproduced factual information, which is not copyrightable expression. Anyone at an NBA game can obtain scores and statistics. Thus, the hand-held pagers did not infringe on the copyrighted broadcasts of the NBA games because those broadcasts are not considered original expressions.[35] Accordingly, *National Basketball Association* represents a key distinction between pagers and bulletin board systems. While pagers merely transmit facts, which are not copyrightable, bulletin boards pose a greater threat by allowing subscribers to copy complete programs or images.

3. LISTSERV and Usenet Groups and Copyright Infringement

LISTSERV and Usenet groups present some of the greatest challenges to copyright protection on the Internet. The one-to-many and many-to-many communications permit reproduction of an author's work on a scale never before available and at a cost that is almost non-existent. When consumers gain access to these tools—copyrighted works—derivative works and collective works are sent whizzing through cyberspace. The well-publicized legal battle over the works of L. Ron Hubbard in *Religious Technology Center v. Netcom On-Line Communications Services, Inc.* illustrates copyright owners' concern about widespread dissemination of copyrighted works, at a cost that can not be matched by any print medium.[36]

In *Religious Technology Center*, the plaintiff Scientologists held copyrights on the writings of L. Ron Hubbard, founder of the Church of Scientology. The Scientologists sued Erlich for copyright infringement after he posted portions of the copyrighted works on a Usenet group, which served as a forum for discussion and criticism of Scientology. Erlich was a former Scientology minister who had become a "vocal critic of the church."[37] The Scientologists also sued the BBS operator who connected Erlich to the Internet, and Netcom, which provided connection facilities for the BBS.[38] The court held that Netcom was not directly liable for copies made and stored on its equipment, but Netcom could be held liable for contributory infringement, such as the failure to prevent infringement once Netcom was adequately notified of the problem.[39] This case provides an example of how LISTSERV and Usnet Groups on the Internet are providing new challenges to copyright owners in protecting their copyrights.

B. Trademark Infringement

Trademarks are similarly affected. Trademarks arose from medieval origins to protect the distinctiveness of a particular product produced by a trade. A product's mark had meaning and value because consumers located

in nearby towns and villages were familiar with the work of the person or trade it represented. If a new product appeared with a similar mark, the customer might be fooled into buying a competing good. Indeed, even today "competitive proximity" and "actual confusion" between competing products remain two essential elements of a modern trademark infringement action.

Within the Internet, geographic proximity of competing products is no longer relevant. All goods compete simultaneously throughout the world. Theoretically, all consumers who log on to the Internet comprise the market for competing products. In such an environment, an argument can be made that brand names lose their importance because all products become more fungible; a consumer might be more likely to choose a product solely for its specific features rather than considering the product's brand name. However, an equally cogent argument can be made that brand names and trademarks increase their significance in this environment; specifically, these devices allow a vulnerable consumer to rely on them as seals of originality and quality.

Within the Internet, geographic proximity of competing products is no longer relevant.

1. Domain Names — Trademark Issues

Domain names, the addresses of the Internet (e.g., http://www.luc.edu), also raise intellectual property issues. Network Solutions Inc., the organization which assigned domain names, used to allow anyone to register a name on a first-come, first-serve basis. Under this system, several ambitious individuals registered such popular names as "mtv.com," "allstate.com," and "mcdonalds.com" without owning those trademarked names. Trademark owners complained that such actions diluted their good names by threatening their cyber-identities. In July 1995, Network Solutions announced its new policy on issuing domain names.[40] Among other procedural aspects, the policy suspends use of a domain name if the first individual to register the name refuses to relinquish it to a company owning the trademark. This new policy did little to stem the rising tide of trademark litigation concerning domain names.

Until Network Solutions made this change, several well-publicized trademark-infringement lawsuits emerged, but little case law developed because most matters were settled. However, several domain name cases have now reached decisions on the merits. In *Panavision International L.P. v. Toeppen* and *Intermatic, Inc. v. Toeppen,* two federal district courts held that registration of a famous trademark as a domain name for the purpose of selling the domain name to the trademark owner violates the new Federal Trademark Dilution Act.[41] In both the *Panavision* and *Intermatic* cases, the defendant was Dennis Toeppen, an Internet service provider with a side business of registering the established trademarks of various companies as domain names. Toeppen hoped that he could sell the domain names back to the trademark owners at a profit. In addition to the Panavision and Intermatic trademarks at issue in these two cases, Toeppen obtained domain name registrations for more than 240 other trademarks, including "deltaairlines.com," "neiman-marcus.com," "ussteel.com," "eddiebauer.com" and "yankeestadium.com."

In *Intermatic,* Toeppen registered the domain name http://www.intermatic.com, and used it in

connection with the sale of a software program. When the corporation demanded that Toeppen give up the domain name and stop using it to promote his software program, Toeppen partially acquiesced. Toeppen agreed to stop using the domain name, but he refused to relinquish the registration. The corporation then sued Toeppen for trademark dilution.[42]

The court characterized Toeppen as a "cyber-squatter," who "attempt[ed] to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark."[43] The court also outlined the elements of a cause of action founded on the Federal Trademark Dilution Act:

> In order to state a cause of action under the Act, a party must show that the mark is famous and that the complainant's use is commercial and in commerce which is likely to cause dilution. The statute defines the term 'dilution' to mean 'the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake, or deception.'[44]

Since Toeppen did not dispute that Intermatic was a famous mark, the court found the first element satisfied.[45] As to the commercial use element, the court held that Toeppen's attempt to profit from cyber-squatting on the "intermatic.com" domain name constituted commercial use.[46] Next, the court held that Toeppen's use of the Internet satisfied the Act's "in commerce" requirement because of the instantaneous and global transmission of Internet communications.[47] Finally, the court held that Toeppen caused dilution of the corporation's trademark by: (1) "lessen[ing] the capacity of [the corporation] to identify and distinguish its goods and services by means of the Internet";[48] and (2) by using the corporation's name on his website.[49] Accordingly, the court granted the corporation's motion for summary judgment on the trademark dilution issue.

The *Intermatic* decision is significant because it sends the message that courts will not tolerate domain name poaching or "cyber-squatting" with intent to sell the domain name to the trademark owner. This represents an important step forward for trademark owners. In the past, many companies have paid thousands of dollars to cyber-squatters to gain the rights to domain names matching their own trademarks. Consumers should thus be aware of the risk they run if they seek to profit as cyber-squatters. Furthermore, consumers lured onto a phony website by its "brand name" should notify the trademark owner.

The decision is also significant with respect to what it does not decide. The court limited its holding to resolving domain name conflicts between trademark owners and cyber-squatters. The decision does little to resolve domain name conflicts between competing bona fide user of the same trademark. Traditional trademark law has always permitted multiple users of a given trademark (e.g., Acme, United) to simultaneously use and register a mark as long as the competing uses deal with sufficiently different goods and services. However, the Internet's current domain name registration process allows only one company to operate on the Internet as "acme.com" or "united.com." Accordingly, consumers should not rely solely on a domain name when deciding whether to

engage in a transaction on the Internet. In this environment, what you see is not always what you get.

2. Consumer Confusion Arising from Similar Domain Names

Another problem on the rise regarding Internet products is confusion between unrelated products with similar names. In *Snap-on Tools Company v. C/Net, Inc.*, a famous and longstanding automotive product company sued a new company who was ready to launch an Internet service, which was unrelated to the automotive industry.[50] While the court's decision was decided on a technical procedural point, its discussion considered various trademark issues that affect consumers. The court commented that the plaintiff did not offer evidence that consumers would be confused between a wrench and an Internet service, or further, that plaintiff's well known trademark of "Snap-on" for automotive tools would be diluted by the defendant's introduction of an Internet service using the trademark "Snap! Online."[51]

Consumer confusion can also result when companies register their competitor's trademarks as Internet domain names. For example, in California, KCRA-Channel 3 reportedly registered the call letters of three of its competitors as Internet domain names: kvie.com (Channel 6), kpwb.com (Channel 31), and ktxl.com (Channel 40).[52] Similarly, arbitrators recently ruled that Princeton Review, Inc. must relinquish the Internet domain name of "kaplan.com" to Kaplan Education Centers, a test preparation subsidiary of the Washington Post, Company. Princeton Review registered the name of its rival, Kaplan.[53] In sum, consumers should use caution when surfing the Internet by domain name alone.

C. Hyperlinks

Hyperlinking and the use of frames technology — both methods to create interconnectivity by links from one website to another — has resulted in several lawsuits that pose legal questions stabbing at the heart of the World Wide Web. The most interesting development arises from the well-publicized media debate over the case of *Ticketmaster Corp. v. Microsoft Corp.*[54] Ticketmaster claimed that Microsoft should pay for the Internet traffic that Microsoft delivered to Ticketmaster via hyperlinks from visitors to the Microsoft Sidewalk website. The complaint stated that Microsoft "has unlawfully used hypertext links, including links which incorporate the unique addresses and URLs of Ticketmaster computers and documents."[55] Microsoft vigorously denied the allegations. In addition to filing suit, Ticketmaster has taken steps to block the traffic directed from Microsoft and Microsoft has removed the hyperlinks.

At first blush, Ticketmaster's contention seems completely at odds with the fundamental purpose of the Internet; that is, to allow web surfers to freely link from one website to another. Moreover, how could Tickemaster complain about a hyperlink that was directing traffic to its website to purchase its product — tickets to concerts and other events?

A more careful look suggests that Ticketmaster may be raising some legitimate questions. Should a company be allowed to control how visitors enter its website? For example, the Microsoft hyperlink connected websurfers directly to the forms for purchasing tickets. This method of linking was advantageous to websurfers because it delivered them directly to the ticket purchase window, bypassing Ticketmaster advertisements the surfers would have encountered by entering through the website's "front door." Thus, Ticketmaster

lost potential advertising revenue. Moreover, by entering the Ticketmaster website deep within a website page, the surfer also bypasses the terms and conditions controlling his or her conduct while visiting the site as well as any clickwrap disclaimers of liability.

The *Ticketmaster* case should cause us to contemplate the degree of consumer privacy that we are entitled to demand on our own homepages. Should anyone be allowed to hyperlink to any part of our website? On the other hand, should consumers be prohibited from linking to their favorite sites? For example, should courts stop consumers from linking fan-club sites to the appropriate movie or television show web pages? Lawyers have already started routinely sending letters to developers of such sites requesting that the sites be closed when they contain copyright materials such as pictures and trademarks of the television shows.

Both of the Internet's key attributes, ease of use and global reach, require adaptation of traditional copyright and trademark principles. From the United States perspective, all forms of intellectual property protection flow from the effort to balance simultaneously two competing interests. On one hand, we want to reward authors and inventors and encourage them to produce creative products and ideas and therefore provide copyright protection. On the other hand, we want to ensure that consumers achieve reasonable access to the creations to maximize societal benefit. The challenge presented by the Internet is to reach an optimal protection level for intellectual property. While the Internet's global reach permits authors to access larger markets of consumers for their ideas, this benefit comes at a price. It permits infringers to copy and distribute protected works to thousands or even millions of consumers without any compensation to the creators.

IV. Jurisdictional Issues

In its simplest form, jurisdiction represents a sovereign government's raw power to render judgment and enforce its authority. Jurisdiction is, and will remain, a difficult issue for courts to analyze in disputes arising from Internet contacts with consumers. Consumers may be forced to exercise their rights in far-off jurisdictions or be sued in such locales, depending on their Internet activities.

Doctrines of jurisdiction focus on the most significant contacts between the individual and the forum state or country. Courts must decide what contacts are significant, and this is a tricky business because the standard used to measure a particular contact is vague. Ultimately, every case is decided on its own facts, and this has led to a myriad of seemingly inconsistent decisions. The core issue of jurisdiction is whether subjecting a non-resident to personal jurisdiction comports with the demands of due process and does not offend traditional notions of fair play and substantial justice. One commentator summarized the process as follows:

> [a] three-part test [has been] developed to determine whether the assertion of specific jurisdiction is constitutional: (1) the defendant must purposefully avail itself of the privilege of conduct ing business in the forum; (2) the cause of action must arise out of the defendant's activities in the forum; and (3) the exercise of jurisdiction must be fundamentally fair. Further, in several recent opinions, the Supreme Court has listed five factors to consider in deter mining whether the assertion of jurisdiction is fundamentally fair: (1) 'the burden on the defendant'; (2) 'the

> forum state's interest in adjudicating the dispute'; (3) 'the plaintiff's interest in obtaining convenient and effective relief'; (4) 'the interstate judicial system's interest in obtaining the most efficient resolution of controversies'; and (5) 'the shared interests of the several states have in furthering fundamental substantive social policies.' Most importantly, it is the defendant's conduct that remains the central concern of the jurisdictional analysis. Once a defendant's conduct satisfies the minimum contacts threshold, few other considerations are likely to tip the balance in favor of rejecting jurisdiction as unfair.[56]

The Internet allows consumers to establish many "contacts" with jurisdictions in which they do not live — and which they may never physically visit. The informality and unpredictability of communications across interconnected networks may make it hard to determine when there has been a voluntary "contact" exposing a consumer to some local law. It is hard to determine "where" online act occur or even "where" some types of injuries are suffered.

To ensure fair rulings on jurisdiction requires courts to be educated about the Internet. An early trend is for courts, without much discussion about the Internet, to decide that jurisdiction exists just because a person logged on to the Internet or has a home page available to consumers in a particular state.[57] This trend represents a disturbing development in today's Internet environment. A better approach would be for courts to demonstrate more knowledge of the special problems posed by the Internet.

The decision in *Bensusan Restaurant Corp. v. King*[58] represents an example of the preferred approach. In a thoughtful decision, the court held that mere existence of a website available in a given jurisdiction is insufficient to vest a court with personal jurisdiction. In *Bensusan*, the plaintiff operated a New York jazz club known as The Blue Note. The defendant also operated a small club, known by the same name, in Columbia, Missouri. The court ruled that the defendant could not be brought into a New York court just because he operated a website promoting his Missouri club. The appellate court affirmed, stating:

> The acts giving rise to Bensusan's lawsuit — including the authorization and creation of King's web site, the use of the words 'Blue Note' and the Blue Note logo on the site, and the creation of a hyperlink to Bensusan's web site — were performed by persons physically present in Missouri and not in New York. Even if Bensusan suffered injury in New York, that does not establish a tortious act in the state of New York. . . .[59]

Another leading case is *CompuServe Inc. v. Patterson*[60] in which the United States Court of Appeals for the Sixth Circuit overturned a district court's finding that Ohio lacked personal jurisdiction over a Texas resident. The Sixth Circuit found that the Texas subscriber to the CompuServe network created substantial connections with Ohio because he entered into the subscriber agreement and used the CompuServe network to distribute his software product. The teaching of the *CompuServe* case and others like it, is that conducting electronic commerce with consumers in a particular state is strong evidence of jurisdiction.

Numerous cases decided in 1997 followed the reasoning of *Bensusan* and *CompuServe*. These cases indicate that merely establishing an Internet presence will not users to jurisdiction

everywhere in the country. However, once users take additional steps to transact business in a particular state, courts are more likely to submit them to jurisdiction in that state.

For example, in *Hall v. Leronde,* the California Court of Appeals for the Second District Held that "the long arm of the Internet reaches from California to New York."[61] In this case, the plaintiff and defendant contacted to develop a software product together. Through e-mail messages, the defendant established contact with California. The court found that communication through e-mail and telephone from another state to California may establish sufficient minimum contacts with California to support personal jurisdiction. In particular, the court noted:

> Much has happened in the role that electronic communications plays in business transactions since Interdyne was decided more than 20 years ago. The speed and ease of such communications has increased the number of transactions that are consummated without either party leaving the office. There is no reason why the requisite minimum contact cannot be electronic.[62]

Courts continue to tackle this issue of whether jurisdiction is proper over the Internet. The results depend of the facts of each case. The decisions described above highlight the potential traps awaiting Internet users. Even though a user may be physically situated in one jurisdiction, his Internet activities may subject him to the laws of another jurisdiction. Potential criminal liability for some Internet activities heightens this risk.

V. Criminal Liability

Pictures as well as text can be transmitted over the Internet. Hard core pornography is widely available. Adults may engage in chat groups[63] posing as children to talk to real children about their prurient agendas.

In the first cyberspace obscenity case, *United States v. Thomas*, BBS operators were charged with criminal conduct in the place where children received their obscene material, rather than the jurisdiction where their computer servers were physically located.[64] The BBS operators lived near Milpitas, California; they transmitted pornographic images as data files via the Internet. A postal inspector in Memphis, Tennessee received some of these data files.[65] The BBS operators challenged the criminal application of a standard based on Tennessee as the relevant community; instead, the BBS operators urged the court to judge them on a standard based on California as the relevant community.[66] The court looked to *Miller v. California*[67] where the United States Supreme Court set out a three-prong test for obscenity:

> (a) whether "the average person apply ing contemporary community standards" would find that the work, taken as a whole, appeals to the prurient interest . . . ; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifi - cally defined by applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[68]

Particularly interesting to consumers is the Thomas case's analysis of the jurisdictional issue of cyberspace. The BBS operators argued that Internet's technology requires courts to go beyond the *Miller* relevant community standard. Specifically, the Internet requires:

> a new definition of community, i.e., one

> that is based on the broad-ranging connections among people in cyberspace rather than the geographic locale of the federal judicial district of the criminal trial. Without a more flexible definition, they contended that there will be an impermissible chill on protected speech because BBS operators cannot select who gets the materials they make available on their bulletin boards.[69]

According to the court, the defendants did not lack control over who received their materials; access to the defendants' BBS was limited. Membership was necessary and applications were submitted and screened before passwords were issued and materials were distributed. Thus, defendants had methods in place to limit user access in jurisdictions where the risk of finding obscenity was greater than that in California. They know they had a member in Memphis; the member's address and local phone number were provided on his application form. If defendants did not wish to subject themselves to liability in jurisdictions with less tolerant standards for determining obscenity, they could have refused to give passwords to members in those districts, thus precluding the risk of liability.[70]

These comments reflect a judicial attitude likely to emerge in commercial cases if materials are sent from one state or country to a consumer in a different one. Indeed, many state sales tax officials are currently investigating methods for measuring and collecting revenue derived from Internet operations.

Although the United States Congress attempted to set rules concerning pornography on the Internet with its Communications Decency Act of 1996,[71] ("CDA"), the United States Supreme Court has held several operative sections of the Act unconstitutional.[72]

A. Fraud and Theft

The voluntary nature of the Internet highlights another area of consumer vulnerability. Specifically, the use of packet switching technology, which is different from present public telephone switched networks, makes it difficult for consumers to dictate standards of service quality. This translates directly into concerns for reliability and speed, but also for information security and privacy for consumers.[73] Any individual or organization can place a router onto the Internet. Because a router is attached to the network, other routers will send it packets to load balance traffic. The operator of the router can attach a device, know as a "sniffer," to its router.[74] The sniffer will capture any packets that flow by and examine their contents. Obtaining all packets of a long message may not be possible, but unscrupulous routers may able to isolate certain information, such as credit card numbers, and collect them. Other pieces of valuable personal consumer information could also be accumulated. Thus, a consumer must seriously evaluate the security risks that are reported in the media. Unfortunately, most consumers do not have the technical know-how to make informed decisions about security issues.

For example, these recent news stories reveal the sophistication and cunning demonstrated by modern "cyber-criminals:"

> They called themselves the world's first Internet bank — secrecy guaranteed, high interest rates, no taxes . . . and no insurance. But last month, the European Union Bank Antigua (EUB) collapsed. It was created by two young Russians who controlled hundreds of millions of dollars while coming of age during the frenetic transition of their native country

from communism to guns-and-connections barreled capitalism.[75]

A former graduate student at Nova Southeastern University was arrested on Tuesday and charged with wire fraud for allegedly trying to fraudulently obtain 174 credit cards via the Internet, federal officials said. . . . [He] used legitimate student names and identification to apply for cards using his home computer. None of the cards were delivered to the post office box he listed.[76]

'Hello,' read the e-mail. 'My name is David Lawitts and I have severe lung and throat cancer due to second-hand smoke. This chain was a final attempt to help solve my problem. For every one person that this letter is sent to, the National Lung and Cancer Association will donate three cents to help me, and other people like me, become healthy again'. . . .Why didn't I trust this message . . . ? First, because a quick search showed that there's no such thing as the 'National Lung and Cancer Association'. . . . So what is that message about? It's either some weird revenge, or else it's a scam, intended to collect as many addresses as possible of soft-hearted and soft-headed Internet users. My money's on the second option. Scams such as this demonstrate to me how the Internet's rapidly becoming unusable.[77]

On Thanksgiving weekend in 1995, someone (presumably a critic of a book my wife and I had just written about computer hackers) forwarded my home telephone number to an out-of-state answering machine, where unsuspecting callers trying to reach me heard a male voice identify himself as me and say some extremely rude things. . . . It seemed funny at first, at it gave us a swell story to tell on our book tour. But the interloper who seized our telephone line continued to hit us even after the tour ended. And hit us again and again for the next six months. The phone company seemed powerless. Its security folks moved us to one unlisted number after another, half a dozen times. They put special pin codes in place. They put traces on the line. But the troublemaker kept breaking through.[78]

Oh, what a tangled Web we weave: Two former Glendale residents were arrested Aug. 13 and accused of run ning a credit-card scam on the Internet. [They operated an investing club that] had taken orders for credit cards at its Web site, promising an unsecured 6.95% interest rate and a $5,000 credit line 'regardless of credit history . . . even bankruptcy!' in exchange for a $100.00 fee . . . ."[79]

Just as Americans are getting comfort able with the idea of using their credit cards on the Internet, along comes the story of Carlos Felipe Selgado. According to an FBI affidavit, Selgado has confessed to one of the biggest ripoffs yet seen on the Internet - the theft of up to 100,000 credit card numbers from a computer in San Diego. . . . The FBI says the investigation began in late March when an Internet service provider in San Diego discovered an outsider had broken into its

> system and installed a 'packet sniffer' - a program that detects and records passwords used by subscribers to the system.[80]

These "war stories" and others like them warn consumers to be very cautious in relying upon the Internet for business transactions. Wide-ranging opportunities to engage in electronic commerce over the Internet also pose the risk that crooks will access and misuse credit or debit card accounts. Cash equivalents on the Internet are more vulnerable than existing electronic funds transfer systems. Consumers should be wary of any offers made over the Internet. Moreover, security experts express concern over whether most companies are prepared to deal with even basic security issues. Therefore, consumers providing personal information over the Internet face substantial risks.

For example, a 1996 computer crime survey by the Computer Security Institute of San Francisco, California found that many organizations experienced computer system break-ins. Specifically, the survey found that 41 percent of the organizations experienced some form of intrusion or other unauthorized use of their computer systems in 1995.[81] Current employees of these organizations accounted for more than half of those intrusions. Remote dial-in sources and Internet connections also suffered frequent unauthorized probes. Furthermore, unauthorized alteration of data — known as "data diddling" — comprised the most frequent form of attach reported against medical and financial institutions. Surprisingly, more than half of the survey respondents did not have a written policy dealing with network intrusions, and more than 20 percent did not even know if they had been attacked. This survey highlights the risk of how a consumer's personal information may be compromised or improperly accessed due to badly implemented security systems.

B. Internet Gambling

In late 1997, the U.S. Senate Judiciary Committee considered the Internet Gambling Prohibition Act of 1997, which would establish fines of up to $2,500 and jail terms of up to six months for even casual gamblers. A similar bill was introduced in the House, which stated:

> Several states, led by Minnesota, Missouri and Wisconsin, are suing virtual casino operators for enticing their citizens into remote gambling sites. Such sites typically allow customers to establish a wagering account using bank checks or credit cards. Then, winnings and losses are credited or debited to the account, and, in theory, the gambler can cash out at any time. Unlike regulated casinos in the United States, however, virtual casinos typically are not subject to strict controls over ownership, financial reserves, or fairness of games.[82]

While Congress considers the enactment of the Internet Gambling Prohibition Act of 1997, state governments have already taken steps to get a handle on Internet casinos. Minnesota has assumed an aggressive posture by indicting operators of out-of-state casinos that take bets from Minnesota residents. In *State of Minnesota v. Granite Gate Resorts, Inc.,*[83] the court found jurisdiction for a criminal action against the operators of an Internet casino. The operators advertised a forthcoming on-line gambling service on the Internet, and developed from the Internet a mailing list which included Minnesota residents. The court held these activities sufficient to subject the defendants to personal

jurisdiction in Minnesota because they purposefully availed themselves to the privilege of conducting commercial activities in the state.[84] This thoughtful decision represents one example of a state court taking an active role in fighting illegal on-line activity.

VI. Federal Pre-emptions of State Common Law Defamation Actions Poses Potential Pitfalls for Internet Users

Another issue of particular concern to consumers is defamation. In general, a plaintiff trying to establish a cause of action for defamation must first show that an allegedly defamatory statement was "of and concerning" the plaintiff.[85] Second, the statement must be one of fact rather than opinion.[86] Opinion is determined when the court considers the statement under the totality of the circumstances from which it was made.[87] Specifically, a court should consider: the specific language at issue, whether the statement is verifiable, the general context of the statement, and the broader context in which the statement appeared.[88] Finally, if the plaintiff is a public figure, actual malice must be shown.[89] Courts traditionally hold that jurisdiction follows the defamatory statement to wherever the injury occurs. Consumers contemplating conducting business over the Internet potentially subject themselves to lawsuits throughout the world. Accordingly, such consumers should be wary of the court's comments in *Edias Software International, LLC v. Basis International Ltd*:[90]

> Unlike communications by mail or telephone, messages sent through computers are available to the recipient and anyone else who may be watching. Thus, while modern technology has made nationwide commercial transactions simpler and more feasible, even for small businesses, it must broaden correspondingly the permissible scope of jurisdiction exercisable by the courts. . . . The court held that Basis, a software products manufacturer, could not utilize the Internet by circulating a libelous statement in the forum state while simultaneously trying to escape the jurisdiction of the state.[91]

As consumers participate and operate interactive Internet services, they may become "publishers." Cases involving defamation by publishers have focused attention primarily on the liability of service providers for defamatory material that makes its way onto the Internet via their onramps. Several of the leading cases discussed below demonstrate the different ways in which courts analogize existing legal principles to the new medium of the Internet. More significantly, however, these cases caused Congress to consider the unreasonable extent to which a service provider may be liable. In response, Congress included provisions limiting liability for service providers in the Communications Decency Act of 1996 (the "CDA"). Although the United States Supreme Court held certain portions of the CDA unconstitutional, the liability provisions protecting service providers remain in force. To appreciate the development of the law on this point, we first review the pre-CDA cases.

In *Stratton Oakmont, Inc. et al. v. Prodigy Services Co. et al.*,[92] Stratton Oakmont, Inc. and its president sued Prodigy Services Company for libel after a Prodigy subscriber allegedly defamed the company and its president by accusing the firm of fraud stemming from one of its initial public offerings.[93] The subscriber's posting suggested that "criminals" ran the company. Furthermore, the subscriber was an

attorney who offered to represent shareholders in litigation.[94] The court held that: (a) Prodigy was a "publisher" responsible for the content of postings on its bulletin boards; and (b) the system operator, "board leader," who moderated the selection of items placed on the board was an "agent" of Prodigy.[95] Therefore, the court attributed the board leader's conduct to Prodigy, despite a contract purporting to negate any principle/agent relationship. Accordingly, the court granted Stratton Oakmont partial summary judgment.

In another example, *It's In The Cards, Inc. v. Fuschetto*,[96] the Wisconsin Appellate Court examined whether an Internet provider was required to publish a retraction of incorrect information. The court considered the applicability of state laws that require certain media to print retractions.[97] The court held that the state retraction laws did not apply to computer BBS postings because they were not "periodicals."[98] The court admonished the legislature "to address the increasingly common phenomenon of libel and defamation on the information superhighway."[99]

Unfortunately for consumers, the United States District Court of Virginia struck another blow against state common law defamation in *Zeran v. America Online, Inc.*[100] In *Zeran*, the court held that the CDA's limited liability provisions immunize Internet service providers from state law actions. This result left defamed consumers with little recourse. The plaintiff in *Zeran* was the victim of a malicious hoax perpetrated via America Online, Inc. ("AOL"). The plaintiff brought a state law action against the online service, claiming AOL negligently allowed defamatory notices to remain and reappear on an AOL bulletin board even after the victim notified AOL and complained repeatedly.[101] The court held that the CDA, which expressly insulates an interactive computer service from being treated as a "publisher or speaker," preempts the imposition of common law liability against online services such as AOL for negligent distribution of defamatory material.[102] The court reasoned that allowing such liability would contravene Congress' purpose in enacting the CDA — to encourage development of technologies, procedures, and techniques designed to block or delete objectionable material.[103]

The limited nature of this opinion, however, should be noted. The court stated that Congress intended through the CDA neither to displace state regulation of the Internet in general nor to preempt state regulation concerning defamatory material on an interactive computer service in particular.[104] To the contrary, the court recognized that the express language of Section 230(d)(3) reflects Congress' desire to retain state law remedies, so long as they do not conflict with those provided by the CDA.[105] The court's ruling, therefore, falls far short of accepting the broader principle offered by AOL's counsel — that the CDA precludes liability against an online service for any information appearing on its system unless that information was provided by the online service itself.

A Florida state trial court followed *Zeran* in holding that the CDA preempted the plaintiff's state law claims. In *Doe v. America Online, Inc.*,[106] the plaintiff sued AOL on state law causes of action. The plaintiff alleged that AOL permitted a chatroom subscriber to advertise and arrange for the distribution of pornographic videotapes and photographs depicting the plaintiff being sexually assaulted. Since the subscriber did not transmit the pornographic materials via the AOL network, the court applied the CDA retroactively, and found that the CDA preempted the state law claims.

Both the pre-CDA and post-CDA cases illustrate that the CDA is a double-edged sword. While upholding consumers' fundamen-

tal right to free speech and protecting service providers from overwhelming liability, preemption of state law actions precludes enforcement against even heinous abuses of the Internet.

VII. Regulation as a Partial Solution

A. U.S. Government Efforts

The Internet is not immune from governmental regulation.[107] The Federal Trade Commission ("FTC") and the Securities and Exchange Commission ("SEC")[108] are just two of the federal agencies devoting resources to police the Internet. For example, the FTC settled an enforcement action with internet marketers, which promoted a deceptive "credit repair services" advertisement that was posted on about 3,000 Internet news groups. The order banned the defendants from engaging in fraudulent credit repair practices, required them to warn customers that consumers have no legal right to have accurate information removed from their credit reports, and fined them $17,500.

Similarly, the SEC obtained a permanent injunction against an individual accused of using newsgroups and Internet ads to conduct fraudulent securities offerings.[109] The defendant, a convicted felon and repeat securities law violator, solicited investments through over forty advertisements in over twenty Internet newsgroups. The defendant consented to the permanent injunction without admitting or denying the SEC's allegations.[110]

On a more positive note, the SEC approved Spring Street Brewing Company's request to sell its stock over the Internet in 1996. Using a novel Internet trading mechanism, "Wit-Trade," the company can conduct transactions between buyers and sellers of its own stock.[111] To facilitate this process, the company formed Wit Capital Corporation, which claims it is the world's first investment bank dedicated to arranging the public offering of securities through the Internet's World Wide Web.[112] The SEC seems willing to encourage and expand this trend of "cyber-investing." In 1996, the agency issued a legal opinion allowing investors to buy and sell stock on the Internet, bypassing federal registration requirements and brokers.[113]

Other federal agencies have also demonstrated a new affinity of Internet technology. For example, the Commodity Futures Trading Commission ("CFTC") announced its Division of Enforcement webpage, which enables the public to contact the Enforcement Division's electronic mailbox with the click of a mouse. The CFTC hopes the Internet link will encourage investors to report suspected commodities-related wrongdoing to the agency.[114] These examples reveal the federal government's attempts to address consumer Internet issues.

B. Foreign Governments Efforts

The United States government is not alone in seeking to harness the enormous potential of the Internet by regulating its use. Around the world, issues of Internet censorship are a hot topic. Unfortunately, may foreign governments seem to utilize censorship to limit the material its citizens can access on the Internet. For example, in 1996, Singapore's Ministry of Information and the Arts announced a plan to filter all national Internet use through government proxies. The Ministry's stated intent was preventing access to posts critical of Singapore's government, "misleading" news, content that promotes "religious deviations," "dangerous" material, "hate speech," pornogra-

phy, information about homosexuality, and "exploitation" of violence or "horror."[115]

Similarly, German Internet users experienced governmental censorship in 1996. At the behest of, and in response to legal threats from the German government, German Internet providers blocked the Dutch Website Access For All (www.xs4all.nl), removing German users' access to the entire xs4all system. The German government demanded this action because xs4all hosts a Web "home page" featuring "left-wing" political content that, though fully legal in the Netherlands, is allegedly illegal in Germany. As a result of this action, all xs4all websites, including several thousand that have nothing to do with the offending home page, are unavailable in Internet users in Germany.[116]

VIII. Conclusion

The exponential growth and breadth of the Internet has resulted in the ability of an individual computer user to circumnavigate the globe at the speed of light. One can buy and sell, entertain, inform, educate, defame, infringe, invade privacy, or engage in obscene behavior, all in "real time." These capabilities have accelerated the efforts of technologists, business people, policy makers, law enforcement and legal scholars to understand and react to the sometimes profound changes that vast interconnections are making to traditional commerce, communication, legal concepts and the sense of community.

Initially, e-mail drove the installation of distributed networking systems throughout the market place. Now that networks are the established means of doing business, a myriad of other new devices and application wait to follow e-mail. All forms of electronic methods of doing business that utilize networks are ready for universal acceptance. Thus, without even allowing us time to catch our collective breath, consumers must be ready for another onslaught of technology.

It is clear that the technological, commercial, legal and governmental communities have only begun to explore the implications of the positive, neutral, and negative aspects of the network environment created by the Internet. Veterans of this ground-breaking industry welcome the challenge of working with the best minds to bring the optimum results to society and its various constituents. However, consumers must endeavor to advance the Internet's state of the art by taking a proactive role in local and national Internet legislation. Participation in consumer rights groups, lobbying for local or state legislation, or simply writing a local congressman are several ways in which a consumer can make her opinion count. With proactive participation in the Internet regulation, consumers can help ensure that the Internet is a more rewarding, productive, challenging and safe place to be.

Endnotes

1. This article was prepared with assistance from Michael Mensik, Chicago Office; Susan Nycum, Palo Alto Office; Robbie Downing, London Office; David Davis, Chicago Office; and other members of the Baker & McKenzie Global Intellectual Property/Information Technology Practice Group.

2. 969 F. Supp. 160 (S.D.N.Y. 1997).

3. *Id.* at 161.

4. *See id.*

5. Barry Fraser, *Regulating the Net: Case Studies in California and Georgia Show How Not to Do It*, 9 LOY. CONSUMER. L. REP. 230, 230 (1997).

6. Statistical information was obtained from ‹http://

altavista.digital.com› (visited May 6, 1996).

7. For reference information about the Internet, see Fraser, *supra* note 5, at 230.

8. The phrase "surfing" the Internet was originally spelled "cerfing" in reference to Vinton Cerf. For the history of the Internet, see Vinton Cerf, *How the Internet Came to Be* ‹http://www.forthnet.gr/forthnet/isoc/how.internet.came.to.be.cerf›, and Vinton Cerf, *A Brief History of the Internet and Related Networks* ‹ http://www.skywriting.com/cerf.html›.

9. For an excellent resource describing Internet software organized by type, see ‹http://tucoows.niia.net›.

10. *See generally* American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Penn. 1996) (discussing in detail the characteristics of the Internet), *aff'd* 117 S.Ct. 2329 (1997).

11. *Id.*

12. LISTSERV is a distribution list management package. LISTSERV servers maintain lists containing names and electronic mail addresses of computer users. Any member of a list can send electronic mail messages addressed to the list, which the server will forward to all other members of the list. This service provides a convenient means for the exchange of ideas and information between list members. There are many different lists, each containing users who share particular interests. LISTERV servers can also log mail traffic, store all the messages associated with their lists, and carry out database searches of archives and files. LISTSERV uses computer and network resources efficiently. *See* ‹http://www.earn.net/gnrt/listserv.html›.

13. Usenet was originally created in the late 1970s as a "poor man's ARPAnet," to distribute news about the Unix Operating System. It has since grown to include over 10,000 separate newsgroups about many different topics. Some newsgroups are "moderated" so that messages have to be approved before anyone can read them, but most newsgroups are unmoderated. In an unmoderated news group, anyone can place messages, and anyone can read them. Most messages are replies to other messages, and thus an endless discussion is formed. Posting to a news group is similar to writing e-mail. STEVE'S CYBERSPACE DICTIONARY ‹http://www.edmweb.com/steve/cyberdict.html›.

14. "File Transfer Protocol. The most common method of transferring files over the Internet. There are thousands of FTP archives on the Internet, with files that can (usually) be downloaded by anyone for free." STEVE'S CYBERSPACE DICTIONARY ‹http://www.edmweb.com/steve/cyberdict.html›.

15. Mosaic, Netscape Navigator, and Microsoft Explorer are examples of popular browser software.

16. "Bulletin Board System. A computer that people connect to, usually over the phone lines. Usually has e-mail and message conferences, as well as files and chat. A BBS may or may not have connections to other computers." STEVE'S CYBERSPACE DICTIONARY ‹http://www.edmweb.com/steve/cyberdict.html›.

17. *See* the Usenet news group <alt.startrek.creative>.

18. *See* the discussion group <cyberia-1@listserv.cc.wm.edu>.

19. 839 F. Supp. 1552 (M.D. Fla. 1993).

20. *See id.* at 1554.

21. *See id.* at 1556.

22. *Id.*

23. *Id.*

24. *Id.*

25. *Id.*

26. *See id.*

27. *Id.* (citing *Cable/Home Communications Corp. v. Network Productions, Inc.*, 902 F.2d 829, 843 (11th Cir. 1990)).

28. *See Id.*

29. *See Id.* at 1556-57.

30. 857 F. Supp. 679 (N.D. Cal. 1994).

31. *See id.* at 690.

32. *Id.* at 687.

33. *Id.* at 686 (citing Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

34. 105 F.3d 841 (2d Cir. 1997).

35. *See id.* at 846.

36. *See* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). Defendant Dennis Erlich was a former minister of Scientology, turned vocal critic of the Church, whose pulpit is now the Usenet group ‹alt.religion.scientology›, an on-line forum for discussion and criticism of Scientology. Plaintiffs claimed that Erlich infringed their copyrights when he posted portions of their works on the Usenet group. Erlich gained his access to the Internet through defendant, Thomas Klemsrud's BBS. Klemsrud is the operator of the BBS, which is run out of his home and has approximately 500 paying users. Klemsrud's BBS is not directly linked to the Internet, but gains its connection through the facilities of defendant Netcom On-Line Communications, Inc. ("Netcom"), one of the largest providers of Internet access in the United States. The case is now settled. *See Church of Scientology Settles Dispute with Internet Provider,* THE SEATTLE TIMES, Aug. 5, 1996.

37. *Religious Tech. Ctr.,* 907 F. Supp. at 1365.

38. *See id.* at 1365-66.

39. *See id.* at 1381.

40. See July, 1995 policy at ‹ftp://rs.internic.net/policy/internic/internic-domain-1.txt›.

41. Panavision Int'l L.P. v. Toeppen, 945 F. Supp. 1296 (C.D. Cal. 1996); Intermatic Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996). The Federal Trademark Dilution Act, 15 U.S.C. § 1125, was signed into law in early 1996. Both the *Panavision* and *Intermatic* courts noted that the legislative history of the Act suggests that the Act was intended to address Internet domain name issues. Senator Patrick Leahy (D-Vt.) stated that "it is my hope that this anti-dilution 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 CONG. REC. S19312 (daily ed. Dec. 29, 1995).

42. *See Intermatic,* 945 F. Supp. at 1229.

43. *Id.* at 1233.

44. *Id.* at 1238.

45. *See id.* at 1239.

46. *See id.*

47. *See id.*

48. *Id.* at 1240.

49. *See id.*

50. Snap-on Tools Co. v. C/Net, Inc., No. 97-C5803, 1997 U.S. Dist. LEXIS 14581, at *4-5 (N.D. Ill. Sept. 22, 1997).

51. *See id.* at *34.

52. *KCRA Pulls Fast One on Competition,* THE SACRAMENTO BEE, Oct. 19, 1995.

53. *Internet Name Game Gets Specific,* COMPUTERWORLD, Oct. 14, 1994.

54. Ticketmaster Corp. v. Microsoft Corp., CV 97-3055 RAP, slip op. (C.D. Cal. Apr. 28, 1997); see article and Amended Complaint at ‹http://www.ljx.com/LJXfiles/ticketmaster›.

55. *Id.*

56. Richard S. Zembek, Comment, *Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace,* 6 ALB. L.J. SCI. & TECH. 339, 352-53 (1996).

57. *See* Isnet Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D.C. Conn. 1996); Pres-Kap, Inc. v. System One, 636 So. 2d 1351 (Fla. Dist. Ct. App. 1994).

58. 126 F.3d 25 (1997).

59. *Id.* at 29.

60. 89 F.3d 1257 (6th Cir. 1996).

61. 56 Cal. App. 4th 1342 (Cal. Ct. App. 1997).

62. *Id.*

63. Electronic "chatting," which allows users to have conversations over the Internet in real time, is technically described as "messaging between nodes on a network. When your computer connects with a host on a LAN [local area network], the host sends a login prompt to which your computer responds so that the connection can be made." TOM FAHEY, NET.SPEAK: THE INTERNET DICTIONARY 35 (1994).

64. United States v. Thomas, 74 F.3d 701, 704 (6th Cir. 1996). Mr. Thomas was sentenced to three years and one month and Ms. Thomas was sentenced to two and one-half years in prison. Under federal sentencing rules they must serve their full terms.

65. *See id.*

66. *See id.* at 711.

67. 413 U.S. 15 (1973).

68. *Id.* at 25 (quoting Kois v. Wisconsin, 408 U.S. 229, 230 (1972)).

69. *Thomas*, 74 F.3d at 711.

70. *See id.*

71. Communications Decency Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-35, which constitutes Title V of the Telecommunications Act of 1996, was signed into law on February 8, 1996.

72. *See* Reno v. ACLU, 117 S. Ct. 2329 (1997).

73. A good introduction to Internet security issues is available. *See Netsurfer Focus*, COMPUTER AND NETWORK SECURITY (April 26, 1995) ‹http://www.netsurf.com/nsf/v01/01/nsf.01.01.html›; ‹http://www.cis.ohio-state.edu/hypertext/faq/usenet/security-faq/faq.html›; ‹ftp://nusun.jinr.dubna.su/FAQ/security.faq›; ‹http://www.nsu.nsk.su/FAQ/F-privacy-email/Q0-0.html›.

74. *See id.*

75. Jennifer Gould, *Gangster Bankers: A Young Russian Run-in with Organized Crime and Offshore Money Laundering*, THE VILLAGE VOICE, Sept. 16, 1997.

76. *Man Charged With Fraud*, FORT LAUDERDALE SUN-SENTINEL, Sept. 3, 1997, at 3B.

77. Charles Arthur, THE INDEPENDENT (London), Aug. 31, 1997, at 19.

78. Joshua Quittner et. al., *Invasion of Privacy*, TIME, Aug. 25, 1997, at 28-29 (discussing the balancing of privacy versus the utility of the Internet).

79. *Ex-Glendale Residents Accused of Net Fraud*, ARIZONA BUS. GAZETTE, Aug. 21, 1997, at 12.

80. Hiawatha Bray, *Tale of Hacker Puts Chill in 'Net Commerce Hopes*, THE BOSTON GLOBE, May 24, 1997, at F1.

81. Pamela Sebastian, *Business Bulletin*, WALL ST. J., May 9, 1996 at 1.

82. Peter H. Lewis, *Lawmakers Gear Up to Try to Control the Surging On-Line Gambling Industry*, N.Y. TIMES, Sept. 27, 1997, at 4D.

83. 568 N.W.2d 715, 721 (Minn.Ct.App. 1997).

84. *See id.*

85. New York Times v. Sullivan, 376 U.S. 254, 267 (1964).

86. *See id.*

87. *See id.*

88. *See id.*

89. *See id.*

90. 947 F. Supp. 413 (D. Ariz. 1996).

91. *Id.* at 420.

92. *See Stratton Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229, *1 (N.Y. Sup. Ct. May 26, 1995) (dismissed by settlement Oct. 24, 1995).

93. *See id* at *1.

94. *See id.*

95. *See id.*

96. 193 Wis. 2d 429 (1995).

97. *See id.*

98. *See id.*

99. *Id.*

100. 958 F. Supp. 1124 (E.D. Va. 1997).

101. *See id.* at 1124.

102. *See id.* at 1133.

103. *See id.* at 1134-35.

104. *See id.* at 1131.

105. *See id.* at 1132.

106. CL 97-631AE, (Palm Beach County Ct., June 26, 1997) (2 BNA ELECTRONIC INFO. POL'Y & LAW, No. 27, July 4, 1997.)

107. See Fraser, *supra* note 5, at 238-47.

108. *See generally SEC Enforcement and the Internet*, 52 BUS. LAW. 815 (May 1997) (FTC File No. 952-3236).

109. *See* SEC v. Sellin, Litigation Release No. 15,012, 62 S.E.C. Docket (CCH) 603 (S.D. Fla. Aug. 12, 1996).

110. Sellin, 1996 SEC LEXIS 2240, August 12, 1996, litigation release.

111. *See* ‹http://www.witcap.com/cap_1.htm›.

112. *See* ‹http://www.witcap.com/pr_2.htm›.

113. *See* ‹http://www.sjmercury.com/news/nation/netipo625.htm›.

114. The Enforcement Webpage, which is located on the CFTC's Homepage ‹http://www.cftc.gov›, also provides a brief summary of the types of abuses commonly investigated and prosecuted by the CFTC. *See CFT's Division of Enforcement Sets Up Interactive Internet Enforcement Webpage, Linked to the CFTC Home Page*, COMMODITY FUTURES TRADING COMM'N, OFFICE OF PUB. AFFAIRS, 1996 CFTC Ltr. LEXIS 62, at *1 (Aug. 9, 1996).

115. *See* ‹http://www.eff.org/pub/Censorship/HTML/hot.html#sing›.

116. *See* ‹http://www.eff.org.pub/Alerts/960929_germany_censors_.alert›.

CLR