Marketers' Boon in Cyberspace: The Anticybersquatting Consumer Protection Act

Michael G. Walsh, Luh Luh Lan, May Lwin, and Jerome D. Williams

Cybersquatting continually has plagued Internet traders. The Anticybersquatting Consumer Protection Act is intended to protect trademark owners and consumers alike, especially in the Internet environment. This article evaluates the effectiveness of the act by reviewing recent cases that have interpreted the act, details remedies available to consumers and others under the act, and explains the defenses available to cybersquatters. The authors discuss the currently unresolved issues under the act, including those related to international protection of existing domain names. The act may have had an unintended consequence for Web site creators, however, considering that some corporations use it to bludgeon into submission former employees and others who have created Web sites critical of the respective corporation's policies and operations. A review of recent articles and court decisions casts light on whether the act is a help or a hindrance to marketers.

During the 1990s, the practice of cybersquatting made some people rich and other people furious. Cybersquatters are enterprising individuals who reserve one or more domain names—sometimes dozens or thousands (*Dennison Corp. v. Sumpton et al.* 1998)—with the expectation that owners of the equivalent trademarks or trade names will pay to have the names turned over to them. Cybersquatters' attempts to hold domain names for ransom were sometimes successful (see H.R. Rep. No. 106-412 at 5–7; S. Rep. No. 106-140 at 4–7 [1999]). By the end of the decade, few legal obstacles stood in the way of cybersquatters (*Panavision L.P. International v. Toeppen* 1998).

For those unfamiliar with the Internet, a domain name is a kind of "address" on the World Wide Web that typically ends in ".com," ".net," or ".org." As the World Intellectual Property Organization (WIPO) pointed out, domain names, initially created to perform a technical function, now represent business identifiers for certain brand names and companies. These domain names are of value regardless of the industry or the geographic region because each Web address is exclusive. Unlike trademarks, which are registered and regulated in most countries by government agencies, domain names are generally registered by a nongovernment-related body on a first-come, first-served basis. As such, anyone who has the necessary fee is able to register any domain name that has not already been reserved, merely by assuring the company that registers such names (e.g., Network Solutions) that third parties' rights are not being trammeled. Companies that register the domain names generally do not check whether a domain name request is related to existing trademarks, and they are not legally required to do so. According to Kopp and Suter (2000), there are approximately 200 domain name registrars worldwide. Therefore, any person was able to register as a domain name the mark of an established company and prevent the trademark owner from using the domain name. Cybersquatters frequently demanded a kind of ransom, sometimes up to millions of dollars (Mara 2000; Pollack 1999; *The Wall Street Journal* 1997), from the trademark owner so that the owner could use the related domain name. The lack of regulatory control over the registration of domain names resulted in an increasing number of cybersquatters in the late 1990s.

Called "the Internet version of a land grab" (*Virtual Works, Inc. v. Volkswagen of America, Inc.* 2001), cybersquatting became so widespread that it ultimately attracted the attention of the U.S. Congress. In 1999, Congress enacted the Anticybersquatting Consumer Protection Act (1999; codified at 15 U.S.C. § 1125 [c]). The act amends the Lanham Act (1946; 60 Stat. 427) and is intended to (1) protect consumers and U.S. businesses, (2) promote the growth of online commerce, and (3) provide clarity in the law for trademark owners.

Recent court decisions make it clear that the act is an effective weapon for the holder of a valid trademark to sue those who register identical or confusingly similar domain names (Hiller and Cohen 2002). For example, Brad Pitt filed suit against the National Football League (*The New York Times* 1999), Harvard University (Murphy 1999), and a Buffalo, N.Y., newspaper (Herbeck 2000) for the use of "brad-pitt.com" and "bradpitt.net." Before the passage of the act, the available legal remedies were viewed as "expensive and uncertain" (H.R. Rep. No. 106-412 at 6 [1999]). Cybersquatters proved adept at getting around the strictures of the Federal Trademark Dilution Act (15 U.S.C. § 1125

MICHAEL G. WALSH is Associate Professor of Business Law, College of Commerce and Finance, Villanova University. LUH LUH LAN is Assistant Professor of Law, Department of Business Policy, and MAY LWIN is Assistant Professor of Marketing, Department of Marketing, School of Business, National University of Singapore. JEROME D. WILLIAMS is Anheuser-Busch/John E. Jacob Professor of Marketing and Director, Center for Marketplace Diversity, Howard University School of Business.

[c]), federal intellectual property laws, and state deceptive trade practices.

Asserting Rights Under the Act

The owner of a protected trademark or trade name now has a powerful weapon under the act. Previously, under the traditional federal trademark law, limited protection was afforded to businesses that intended to have or had a presence on the Internet. The 1946 Lanham Act did not protect similar businesses using similar names if those businesses operated in different geographic regions, nor did it disallow concurrent users across product categories. Because trademark law only protects registered trademarks that satisfy the test of distinctiveness as prescribed, common words and phrases deemed as descriptors that might be important to a company may not be registered. However, these common words and phrases can be registered as domain names and held ransom by a cybersquatter. It has been held that mere registration of a domain name did not constitute "use" under the Lanham Act to warrant protection (*Brookfield Communications, Inc. v. West Coast Entertainment Corp* 1999; *HQM v. Hatfield* 1999; Kopp and Suter 2000).

Under the act, the alleged cybersquatter can be held liable if it exhibits a "bad faith intent to profit from that mark ... and registers, traffics [sic] in, or uses" a domain name that is (1) "identical or confusingly similar to" a "distinctive mark" or (2) is "identical or confusingly similar to or dilutive of" a "famous mark" (15 U.S.C. § 1125 [d][1][A]). The act, however, does not give an owner "the right to fence off every possible combination of letters that bears any similarity to a protected mark" (*Virtual Works, Inc. v. Volkswagen of America, Inc.* 2001). A court has authority under the act to order the cybersquatter to forfeit or cancel the domain name or to transfer it to the owner of the mark, regardless of when the domain was registered (§ 1125 [d][1][C], § 3010). It can also award damages for violations of the act occurring after the date of its enactment.

A trademark or trade name is distinctive if it is unusual or extraordinary, famous, or well known (15 U.S.C. § 1125 [d][1][A]; *Nabisco, Inc. v. PF Brands, Inc.* 1999). A mark is identical even if it differs in unimportant respects from the domain name (e.g., *Brookfield Communications, Inc. v. West Coast Entertainment Corp.* [1999] holds that the difference between the trade name "MovieBuff" and the domain name "moviebuff.com" was inconsequential; *Sporty's Farm L.L.C. v. Sportsman's Market, Inc.* [2000] holds that the use of "sportys" in a domain name was indistinguishable from the word "sporty's" used in a trademark, because apostrophes cannot be used in domain names).

A domain name that varies by only one character from a trademark or trade name is likely to be regarded as "confusingly similar" under the act, as has often been the case in infringement actions brought under existing trademark law (*Northern Light Technology, Inc. v. Northern Lights Club* 2001). This affirms the district court's injunction requiring the posting of a specified disclaimer on the defendants' Web site to clear up confusion resulting from the single character distinguishing the two names. In the case of *Wella Corp. v. Wella Graphics, Inc.* (1994), the court decided under prior law that the new mark "Wello" was confusingly similar to the trademark "Wella."

Some cybersquatters have registered deliberate misspellings to take advantage of keyboard errors of people surfing the Internet. One notorious cybersquatter admitted that he had registered thousands of domain names, the majority of which were misspellings of famous names (*Shields v. Zuccarini* 2001). This growing species of cybersquatters, called "typosquatters," are also liable under the act. Typosquatters register domain names with misspellings or alternate spellings that users are most likely to type in when accessing a particular Web site. Such errors include misspellings (e.g., "silliconvalley.com"; *San Jose Mercury News v. Royal* 1999), alternative domain names (e.g., "whitehouse.com"), or omission of punctuations or symbols (e.g., "altavista.com," an online casino site, rather than "alta-vista.com," the search engine; Kopp and Suter 2000).

Proving that an alleged cybersquatter acted in bad faith with intent to profit from registering a domain name is not unduly difficult. A court can consider nine different factors that are enumerated in the act (15 U.S.C. § [d][1][B][i]), as well as any others that it considers relevant. The factors specified in the act include whether

1. The defendant has any rights in the trademark or other intellectual property rights in the domain name;
2. The domain name consists, to any extent, of the defendant's legal name or nickname;
3. The defendant used the domain name to offer goods or services before being approached by the owner of the mark and accused of cybersquatting;
4. The defendant made a bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
5. The defendant intended to divert consumers from the online location of the owner of the mark to a site accessible under the domain name that could harm the goodwill represented by the mark, regardless of whether the defendant sought commercial gain;
6. The defendant offered to transfer, sell, or otherwise assign the domain name to the owner or to anyone else for financial gain, without having used or intended to use the domain name in the bona fide offering of any goods or services or acted that way in the past;
7. The defendant misled the company that registered the domain name;
8. The defendant registered or acquired multiple domain names known to be identical or confusingly similar to, or dilutive of, marks of others; and
9. The mark incorporated in the defendant's domain name registration is distinctive and famous within the meaning of the act.

Remedies Under the Act

Depending on whether the cybersquatting occurred before or after the passage of the act, the owner of a trademark or trade name that is successful in court may require the transfer of the domain name to it or the cancellation of the name (for offenses before the passage of the act) (15 U.S.C. § 1125 [d][2][D][i]) or actual or statutory damages (the latter as much as $100,000 per domain name), profits, and costs (for violations occurring after the date of enactment) (§ 1117 [a][b][d], § 3003).

The victim of an alleged cybersquatter is not limited to suing under the act, however, and may incorporate any num-

ber of other theories under federal law, including trademark infringement and unfair competition (15 U.S.C. §§ 1114 [a], 1125 [a]; *Interstellar Starship Services Ltd. v. Epix, Inc.*1999).

Certain state law remedies, such as an award of damages or equitable relief, are also a possibility and can be included in the same lawsuit (see H.R. Rep. No. 104-374 at 4 [1995], reprinted in 1996 U.S.C.C.A.N. 1029, 1031; 15 U.S.C. § 1125 [d][3]). Most, if not all, states at some time enacted unfair or deceptive business practices statutes that would undoubtedly cover the actions of the typical cybersquatter. An injunction under state law may also be available to prevent further misuse of the domain name (*Mattel, Inc. v. Internet Dimensions, Inc.* 2000).

Defenses of the Alleged Cybersquatter

The best defense for an accused cybersquatter is the act's "safe harbor provision," if the cybersquatter can establish that he or she believed the use of the domain name was a fair use or was otherwise lawful and if the court concludes that this belief was reasonable under the circumstances (15 U.S.C. § 1125 [d][1][B][ii]).

Other attempted defenses by alleged cybersquatters, however, have met with little or no success. For example, courts have rejected defendants' assertions that the act did not apply to them because of the following:

- The domain name was pronounced differently from the identical trademark or trade name (*Interstellar Starship Services Ltd. v. Epix, Inc.* 2001, in which the court ruled that these differences "are not readily discernible to the reasonable consumer" because "[p]ronunciation is indistinguishable in printed advertisements").
- The domain name registered had significantly more characters than the trademark (*Mattel, Inc. v. Internet Dimensions, Inc.* 2000, in which the purveyor of an "adult" site on the Internet under the domain name "barbiesplaypen.com" was ordered to transfer the name to Mattel, Inc., the owner of the Barbie trademark).
- The act is unconstitutional because it applies retroactively to conduct that was legal when it was undertaken (*Sporty's Farm L.L.C. v. Sportsman's Market, Inc.* 2000).
- The act is unconstitutional because it infringes on the cybersquatter's First Amendment rights (*Lucent Technologies, Inc. v. Johnson* 2000, in which the creator of a site called "lucentsucks.com" did not succeed in having Lucent's suit dismissed, despite his argument that he only intended to embarrass Lucent when he registered the domain name "lucentsucks.com" and offered pornographic photographs and services for sale on the Web site).

International Considerations

In addition to facing liability under the act in U.S. courts, alleged cybersquatters can be taken to task by the WIPO through dispute resolution procedures under the Uniform Domain Name Dispute Resolution Policy. In the first decision of its kind, a federal appeals court recently ruled that a U.S. citizen found by WIPO to have been a cybersquatter under the Uniform Domain Name Dispute Resolution Policy and stripped of his domain name could sue in a U.S. federal court seeking (1) a declaration that he is not in violation of the act, (2) a declaration that he is not required to transfer the domain name to the party (in this case, a Brazilian soccer club) that instituted the WIPO action, and (3) the relief necessary to effectuate these ends. The alleged cybersquatter had registered the domain name "corinthians.com" and then contacted the Brazilian soccer club, called "Corinthians" in Portuguese, and offered to sell it the name. The Brazilian club succeeded in its action before WIPO in obtaining an order requiring the cybersquatter to turn over the domain name to it (*Sallen v. Corinthians Licenciamentos LTDA* 2001). The practical effects of this decision cannot yet be calculated, but it undoubtedly will lead to future clashes between international and U.S. forums in actions that seek to rein in cybersquatters.

International Situation

Because cybersquatters offer similar domain names registered in foreign countries with different top-level domains (".to" is the suffix specific for Tonga, or ".ma" for Mauritania) (Kopp and Suter 2000), it would be useful to take a cursory look at the situation in the rest of the world to determine how the issue of cybersquatting is handled. Currently, there is no equivalent legislation to the 1999 Anticybersquatting Consumer Protection Act that deals specifically with such World Wide Web blackmailing activities in other jurisdictions; however, the policy adopted in Sweden that requires that the applicant is a holder of a registered company name that distinctively and uniquely is reflected by the domain name applied for has efficiently hindered widespread cybersquatting under the ".se" top-level domain (Persson 1999). In most countries, however, parties that are threatened by the cybersquatters generally must resort to the traditional legal protections under the trademark legislations and other intellectual property rights, such as the law of passing off. In general, the authorities in charge of the registration of domain names in most countries adhere to the first-come, first-served rule and do not carry out any searches before assigning domain names. For example, when America Online moved into Brazil, it was forced to settle for the domain "br.aol.com" instead of the already taken "aol.com.br" (".br" for Brazil). In some countries, national registration authorities have set up special dispute resolution tribunals to resolve disputes involving ownership of domain names. For example, in the United Kingdom, if such a dispute arises, the parties can refer the matter to the Nominet Dispute Resolution Service. Nominet U.K. assists the parties in a dispute over an Internet domain name registered under a subdomain of the ".uk" top-level domain name, between the organization or individual and another laying claim to a stronger right to register it. Nominet has the power to go as far as suspending the delegation of an Internet domain name, and the dissatisfied party may pursue its case by litigation in the courts if it is still unhappy after a few rounds of mediation.

Cases in other jurisdictions show that it may not always be easy for a rightful owner of a trademark or company name to bring a successful action against a cybersquatter under the traditional trademark laws and other intellectual property laws. In some cases, the alleged cybersquatter may even be able to capitalize on loopholes in the law to assert claims. In the Canadian case *ITV Tech v. WIC Television Ltd.* (1997), WIC Television, the owner of a television sta-

tion operating under the name ITV and with an Internet Web site with the domain name "itv.ca," failed to obtain an injunction to restrain the defendant, ITV Technologies, which claimed to be a network provider involved in Internet casting of video productions, from using the domain name "itv.net" because WIC could not prove irreparable harm.

A similar approach was taken by the Canadian courts in *PEINET, Inc v. O'Brian* (1995). In this case, the plaintiff operated under the trade name Peinet, Inc. The defendant, a former employee of the plaintiff, registered the domain name "pei.net." The plaintiff sought an interlocutory injunction restraining the use of the domain name "pei.net" on the basis of passing off, but was denied by the court on three grounds: (1) the plaintiff failed to established sufficient goodwill in its trade name because it did not own a registered trademark, (2) the plaintiff failed to establish that the defendant's conduct deceived the public, and (3) the plaintiff did not establish damage.

In the U.K. case *Pitman Training Ltd v. Nominet U.K.* (1997), the court accepted Nominet's decision to grant the domain name "pitman.co.uk" to the first party that sought to register the name, even though the name was subsequently redelegated to another party. The other party confirmed with its service provider that the domain name was not subject to prior registration and began using the same domain name before the first party did.

However, if the plaintiff is able to prove harm or ill intent, the courts are more willing to find judgment for the plaintiff within the existing legal frameworks. In the U.K. case *British Telecommunications plc v. One in a Million Ltd*. (1999), the defendant had registered several well-known names such as "Harrods" and "Marks & Spencer." It was found that the defendant's purpose in registering the domain names was to blackmail the owners of the goodwill in those names. The court held that passing off had been established and that the domain names registered were instruments of fraud. It also held that the plaintiff had an alternative claim under the 1994 U.K. Trade Marks Act (§ 10 [3]) as there were threats to infringe.

The previous examples indicate that jurisdictions outside the United States are still struggling to find appropriate legal protection for owners of trade names and trademarks. The Anticybersquatting Consumer Protection Act thus serves as a blueprint for countries that want to enhance the legal remedies for rightful owners against cyberblackmailers.

Implications for Marketers

Undoubtedly, the Anticybersquatting Consumer Protection Act aims to protect honest traders and marketers by ensuring fair play in the marketplace. Marketers can view the act as a shield and not a sword for a rightful trademark owner. The act gives remedy to marketers that are victimized by the confusion of similar domain names; however, it is not meant to stave off competition, nor is it intended to be used as a tool for unscrupulous marketers that may want to reserve domain names even before establishing any business. On the basis of Stewart and Zhao's (2000) premise that the basic economic laws do not change on the Internet, Internet marketers need to ensure that cases against cybersquatters are physically grounded. One key element of the act is that the plaintiff must prove "bad faith" on the cybersquatter's part to "profit from" the mark, usually the company name or some brand names, belonging to the plaintiff when the registration occurred. As an example, a likely profiteering activity may include attracting visitors to the Web site using an existing mark and then selling advertising space on the basis of the large number of visitors.

In addition, an Internet trader must already have established some recognition in its company name or have some reputable brand names that it wants to protect before it can rely on the act. For example, America Online, Charles Schwab, Amazon.com, Yahoo, and eBay can be considered strong Internet brand names (Stewart and Zhao 2000), whereas large numbers of existing bricks-and-mortar firms remain almost unknown beyond their limited physical marketplaces. The court is unlikely to award a trader or marketer remedies just because another person happens to come up with a similar domain name at about the same time or proves to be unaware of the existence of the former. In a sense, the act does not change the rules of the game for marketers in cyberspace; it simply reinforces existing proprietary rights in a fairly new marketing environment. In summary, marketers that wish to seek recourse under the act should thus ensure (1) that the brand name or personal name enjoys a substantial amount of reputation and recognition such that the identical or confusingly similar domain name dilutes the distinctive or famous mark, and (2) the existence of the negative intent element on the cybersquatter's part (e.g., bad faith motive to profit from the mark, including a personal name).

Another implication arises from the global nature of the Internet, which has spawned additional jurisdictional issues. Internet marketers are likely to face greater difficulty in protecting their brand equity across borders. This is because the dichotomy of global strategies is central to product standardization (Mittelstaedt and Mittelstaedt 1997), and at the same time, such strategies increasingly restrict the extent to which domain names can be used synonymously in different countries. The act assures marketers that online reputation is just as important as reputation in the traditional physical markets and that consumers are entitled to associate domain names with a particular company or product just as they are with brand names. Conversely, because of the borderless nature of the World Wide Web and the rise of global e-commerce, the act may have the unintended effect of reaching out to protect marketers from jurisdictions outside the United States, as evident in the case of *Sallen v. Corinthians Licenciamentos LTDA* (2001). This may pose some difficulties to U.S. marketers that may want to register domain names similar to some foreign domain names even if customers in the United States have not heard of the names.

Finally, there may exist secondary consequences beyond mere inconveniences, such as reduced visits from Internet customers potentially being deceived by cybersquatters. Although it is not explicitly covered in the act, marketers may wish to consider the potential implications arising from customers who have faced negative experiences after being misled or misguided to cybersquatters' sites.

A Law of Unintended Consequences

This article would not be complete without a short discussion of some unintended consequences of this act. Even a

cursory reading of the act makes clear that it primarily is intended to prevent someone from registering a domain name solely to benefit unfairly from the notoriety of the owner of the equivalent trademark or trade name. Nevertheless, the act has been invoked by some owners not because the alleged cybersquatter was trying to hold the domain for ransom, but because the owners were embarrassed by the content of cybersquatters' sites.

Increasingly, the courts will be asked to rule on whether the act should be used to bludgeon into submission the "little fish" who is having fun at the expense of the "big fish" because the former was fired by the latter (as in the case of "lucentsucks.com," discussed previously) or because the former merely disapproves of the latter's philosophy. A recent case falling into the second category involved a former Internet executive, Michael Doughney, who registered several domain names, including "peta.org," in 1995. Doughney represented to Network Solutions, which registered the domain name, that the registration did not interfere with the rights of any third persons. He explained that "peta.org" stood for "People Eating Tasty Animals" and created a Web site encouraging, among other things, meat eating and the wearing of fur. He admitted that the site was intended to parody the activities of People for the Ethical Treatment of Animals (PETA), a well-known not-for-profit organization opposed to the use of animals for these purposes.

Under the act, PETA sued to force Doughney to turn over the name to it and sought other remedies in addition, though not damages. A federal district court granted PETA's motion for summary judgment, and a federal appeals court affirmed. The appeals court found that the act had been violated, because Doughney had exhibited bad faith and apparently had hoped to profit from his Web site, on which he stated that PETA should "settle" with him. The appeals court (*People for the Ethical Treatment of Animals v. Doughney* 2001, p. 369) approved the district court's finding that Doughney "clearly intended to confuse, mislead, and divert Internet users into accessing his Web site which contained information antithetical and therefore harmful to the goodwill represented by the PETA mark." Yet the district court stated that Doughney had registered the domain name "because he thought that he had a legitimate First Amendment right to express himself this way" (*People for the Ethical Treatment of Animals v. Doughney* 2001, p. 369). However, the court found that his state of mind was inappropriate and that, even if he had acted only partially in bad faith, he was in violation of the act. Bear in mind that the safe harbor provision of the act states that "bad faith intent shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful" (15 U.S.C. § 1125 [d][1][B][ii]).

The PETA case seems likely to stifle cyberspace use of parody, which historically has enjoyed broad protection on First Amendment grounds in the United States. It seems unlikely that Doughney ever expected to reap large financial rewards—or any, for that matter—from a not-for-profit such as PETA but was merely expressing philosophical differences in an attempt to embarrass PETA. Using the act to stifle his sophomoric humor seems extreme.

In the case of "lucentsucks.com," it remains to be seen whether this case might have turned out differently if the Web site had not been employed to display pornographic material. We can only hope that the decision turned on that sordid detail, as the rights of disgruntled former employees to speak out have long been protected under the First Amendment, and they should enjoy that protection on the Internet.

Conclusion

Early decisions under the act demonstrate that the courts do not hesitate to find the existence of cybersquatting and to deal harshly with its practitioners. Most consumers and marketers applaud this trend, though cybersquatters that attempt to cash in on the notoriety and hard work of owners of trademarks and trade names have few supporters. Online consumers' fear of cybersquatting has even prompted major Web sites (e.g., Yahoo) to start mass sales of personalized domain names.

From the marketers' perspective, especially those in the United States, the act provides for the defense not only of one's Web identity but also of the overall online reputation and company image. This is especially advantageous in cases in which genuine customers are purposely misdirected to profiteering Web sites or in which domain names are held ransom to companies.

The use of the act to suppress free speech that is not intended primarily to profit at the expense of its target should be watched closely, however. This is especially so in the case of Web sites that are created to parody or poke fun at organizations. There should be a place for parody on the Web, which has been a forum for free expression since its inception.

Finally, interesting issues will continue to arise when owners of trademarks or trade names assert their rights with international bodies such as WIPO, only to find themselves in federal court in the United States, forced to relitigate their claims under the act, as in the Corinthians case mentioned previously.

References

Anticybersquatting Consumer Protection Act (1999), Pub. L. No. 106-113, codified at 15 U.S.C. section 1125(c).

British Telecommunications plc v. One in a Million Ltd. (1999), 1 WLR 903.

Brookfield Communications, Inc. v. West Coast Entertainment Corp. (1999), 174 F.3d 1036, 1055 (9th Cir.).

Dennison Corp. v Sumpton et al. (1998), 999 F.Supp. 1337.

Federal Trademark Dilution Act (1996), 15 U.S.C. section 1125(c).

Herbeck, Dan (2000), "Judge Bars Web Site Used to Criticize the News," *Buffalo News*, (March 1), 4B.

Hiller, Janine S. and Ronnie Cohen (2002), *Internet Law and Policy*. Upper Saddle River, NJ: Prentice-Hall.

HQM v. William Hatfield (1999), 1999 U.S. Dist. Lexis 18598 (December 2).

Interstellar Starship Services Ltd. v. Epix, Inc. (1999), 184 F.3d 1107, 1110 (9th Cir.).

——— (2001), U.S. Dist. Lexis 100, *8 (D. Or. January 3).

ITV Tech v. WIC Television Ltd. (1997), 77 C.P.R. (3d) 486 (FCTD).

Kopp, Steven W. and Tracy A. Suter (2000), "Trademark Strategies Online: Implications for Intellectual Property Protection," *Journal of Public Policy & Marketing*, 19 (Spring), 119–31.

Lucent Technologies, Inc. v. Johnson (2000), U.S. Dist. Lexis 16002 (C.D. Cal. September 13, 2000).

Mara, Janis (2000), "What's in a Name?" *Brandweek*, (January 17), 52–54.

Mattel, Inc. v. Internet Dimensions, Inc. (2000), U.S. Dist. Lexis 9747 (S.D.N.Y. July 13, 2000).

Mittelstaedt, John D. and Robert A. Mittelstaedt, (1997), "The Protection of Intellectual Property: Issues of Origination and Ownership," *Journal of Public Policy & Marketing*, 16 (Spring), 14–25.

Murphy, Shelley (1999), "Harvard Seeks Rights to Own Name in Cyber Suit," *Boston Globe*, (December 8), B1.

Nabisco, Inc. v. PF Brands, Inc. (1999), 191 F.3d 208, 215–16 (2d Cir.).

The New York Times (1999), "Litigants Use Laws to Stake Their Claim in Cyberspace," (December 9), C2.

Northern Light Technology, Inc. v. Northern Lights Club (2001), 236 F.3d 57 (1st Cir.).

Panavision International, L.P. v. Toeppen (1998), 141 F.3d 1316 (9th Cir.).

PEINET, Inc v. O'Brian (1995), 61 CPR 334 (PEISC).

People for the Ethical Treatment of Animals v. Doughney (2001), 263 F.3d 359 (4th Cir.), 15 U.S.C. section 1125(d)(1)(B)(ii).

Persson, Fredrik (1999), "Sweden: Famous Brands As Domain Names," *Managing Intellectual Property*, 85, 53.

Pitman Training Ltd v. Nominet U.K. (1997), F.S.R. 797.

Pollack Andrew (1999), "What's in a Cybername? $7.5 Million for the Right Address," *The New York Times*, (November 30), C8.

Sallen v. Corinthians Licenciamentos LTDA (2001), 273 F.3d 14 (1st Cir.).

San Jose Mercury News v. Royal (1999), No. C-99-20931 (N.D. California, September 13).

Shields v. Zuccarini (2001), 254 F.3d 476 (3rd Cir.).

Sporty's Farm L.L.C. v. Sportsman's Market, Inc. (2000), 202 F.3d 489, 497 (2d Cir.), cert. denied, 120 S. Ct. 2719, 147 L. Ed. 2d 984 (U.S.).

Stewart, David W. and Q. Zhao (2000), "Internet Marketing, Business Models, and Public Policy," *Journal of Public Policy & Marketing*, 19 (Fall), 287–96.

Virtual Works, Inc. v. Volkswagen of America, Inc. (2001), 238 F.3d 264, 266 (4th Cir.).

The Wall Street Journal (1997), "U.S. School Wins French Web Suit," (June 10), 12A.

Wella Corp. v. Wella Graphics, Inc. (1994), 874 F. Supp. 54, 56 (E.D.N.Y.).