

Internet Corporation For Assigned Names And Numbers/Anticybersquatting Consumer Protection Act Of 1999: Dealing With Cyber Claims

Philip G. Hampton, II and Jennifer M. McCue

A. Introduction

1. Like the telephone and television before it, the Internet continues to evolve, as do the legal issues related thereto. The speed of the Internet's evolution makes it difficult for even the most sophisticated practitioner to keep abreast of the latest technological trends, commercial objectives, and attendant jurisprudence.
2. More than 25 years ago, the U.S. government began funding research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of

Philip G. Hampton, the former Assistant Commissioner for Trademarks at the U.S. Patent and Trademark Office, is a partner in the Intellectual Property group in the Washington, D.C., office of Dickstein Shapiro Morin & Oshinsky. **Jennifer M. McCue** is an associate in the Intellectual Property group of the Washington, DC office of Dickstein Shapiro Morin Oshinsky.

A complete set of the course materials from which this outline was drawn may be purchased from ALI-ABA by calling 1-800-CLE-NEWS and asking for customer service. (Have the order code CK102 handy). Or order online at www.ali-aba.org/aliaba/CK102.htm.

Defense's Advanced Research Projects Agency ("DARPA") in the 1960s. ARPANET was later linked to other networks established by other government agencies, universities, and research facilities. During the 1970s, DARPA also funded the development of a "network of networks"; this became known as the Internet, and the protocols that allowed the networks to inter-communicate became known as Internet protocols ("IP"). From its beginning as a basic science project, the Internet or "World Wide Web" has evolved into a system used by millions of people and businesses each day and generating hundreds of millions of dollars of commerce daily.

3. Within the commercial neighborhood of the Internet, a domain name is an online storefront. It is unique and permanent, *i.e.*, a web fingerprint. It can create, reinforce, and extend a brand and provide a single point of contact for customers, investors, partners, and suppliers. Although domain names are not trademarks, nevertheless, they function as "quasi-trademarks." Although they are not the name of a product, service, or corporate name, domain names serve as the primary way to reach a corporate location, albeit on the Internet. The fact that the domain name is unitary—it can serve as the address for only one company—creates problems not seen in the real world. For example, in the real world, several companies can share a trademark without any likelihood of confusion. On the Internet, there are no subtle distinctions: the address jones.com can be owned by only one company, no matter how many companies may rightfully be able to use the "Jones" trademark off-line. Domain names are, in essence, locations—they often do not act to designate the source or origin of goods and services, but instead exist as a unitary physical address that may or may not constitute a trademark at all.
4. This paper will discuss one's identity on the Internet—domain names—and the theft of that identity by cybersquatters and cybergrippers. It will compare and contrast the two principal weapons used to combat cyber thievery. The Internet Corporation for Assigned Names and Numbers ("ICANN"), the folks who run the Internet, have adopted a streamlined, mandatory procedure, the Uniform Dispute Resolution Procedure ("UDRP") for resolving disputes over the ownership of domain names. Similarly, the Anticybersquatting Consumer Protection Act of 1999 ("ACPA") grants a federal cause of action against the bad faith registration of, use of, or trafficking in domain names that are identical to or confusingly similar to another's trademark, or that are dilutive of another's famous trademark. Both the UDRP and the ACPA eliminate several of the substantive and jurisdictional problems that

trademark owners previously faced in trying to adapt traditional trademark law to the Internet.

B. Cybersquatting

1. Cybersquatting has been defined by the United States Congress as registering, trafficking in, or using domain names that are identical or confusingly similar to trademarks with the bad faith intent to profit from the goodwill of the trademarks. In many respects, cybersquatters are the modern equivalent of those early frontier settlers—the Sooners—who snatched up land before it could be legitimately claimed, and who then declared the property to be their own.
2. There are many different types of cybersquatters—some hold domain names for ransom, some use them for infringing purposes, and others have even more nefarious tricks up their sleeves. Cybersquatters fall into a variety of categories and engage in cybersquatting for a variety of reasons, ranging from pure greed, to political activism, to malevolence to innocent mistake. Sometimes cybersquatters believe they have done nothing wrong because they are not using the exact trademark itself, but a variation. Because there has been a pervasive, yet subtle acceptance of “pirate” activities on the Internet—some people believe that they can engage in any manner of infringing behavior on the Internet because “information wants to be free”—other cybersquatters believe that they have done nothing wrong since the ownership of proprietary rights is antithetical to the Internet itself.
3. A leading cause for cybersquatting and other cyber crimes is pornography, or at least the tremendous financial gains that often flow from pornography. The widespread, profitable distribution of pornography on the World Wide Web has changed the economics of trademark infringement. People believe—often correctly—that they can make a quick buck and disappear before they are found out by the trademark’s owner. Because of the fluid state of the law relating to the enforcement of intellectual property rights, particularly trademark rights on the Internet, cybersquatters, particularly those associated with smut, are often analogized to low-level extortion crews, leveraging their minimal efforts into cash.
4. Domain names are assigned without reference to who may be “entitled” to them. In other words, the domain name registrars are not required to confirm that a particular registrant of a domain name has the trademark rights asso-

ciated with that particular domain name. Consequently, it is easy for a third party to register a domain name that contains or embodies a trademark owned by another party. Moreover, several different individuals or companies may have overlapping trademark rights that are encompassed by a single domain name, thereby causing several entities to fight over a particular, limited resource.

5. Often cybersquatters successfully appropriate a trademark merely because it may be nearly impossible to find them. Many cybersquatters pay for bandwidth with money orders and disappear. Therefore, anonymous server warehouses are filled with hundreds of servers, owned by unknown individuals, whose identity and whereabouts usually cannot be uncovered by normal means.
6. Classic trademark theories, such as infringement and dilution, are largely ineffective in preventing cybersquatting. Traditionally, a trademark infringer wanted to confuse consumers into purchasing his “fake” product instead of the “real” product of a competitor. Or it might involve an infringer who wanted to catch a free ride on the established good will of a famous brand, so that consumers would “notice” its product in a crowded marketplace. For such traditional infringements, section 32 of the Lanham Act (15 U.S.C. §1114) provided sufficient bases for relief.

- a. Section 32 of the Lanham Act covers a variety of infringements:

Any person who shall, without the consent of the registrant—use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake or to deceive; or reproduce...a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints...or advertisements intended to be used in commerce.

- b. However, the statute requires use or an intention to use the infringed mark in commerce and several courts have held that the infringer must be using the mark on goods or services that would be confused with the goods or services upon which the registrant is using the mark. Consequently, the only cybersquatting cases easily won under section 32 of the Lanham Act are those where the nonholders of the trademark are not merely using a domain name, but are actively engaged in traditional trademark infringement.

7. In 1996, the Federal Trademark Dilution Act (“FTDA”) was enacted. Under this act, codified at 15 U.S.C. §1125(c), the owner of a famous mark is able to enjoin “another person’s commercial use in commerce of a mark or trade name... caus[ing] dilution of the distinctive quality of the [famous] mark....” If willful dilution is proven, monetary relief may be awarded. There have been several cases involving a cybersquatter named Dennis Toeppen. In *Intermatic Inc. v. Toeppen*, 947 F.Supp. 1227 (N.D. Ill. 1996) and *Panavision International, L.P. v. Toeppen*, 945 F.Supp. 1296, (C.D. Cal. 1996), *aff’d*, 141 F.3d 1316 (9th Cir. 1998), courts held that Mr. Toeppen was guilty of trademark dilution—in other words, his “use” of the domain names diluted the ability of the trademarks to act as trademarks.
8. The issue of use is crucial because the mere act of registering the domain name, without any actual use of the domain name in a website or e-mail address, and without an offer to sell the address, may not be enough to trigger the anti-dilution statutes. Simply registering the name is probably not “commercial use” of the domain name. Moreover, in light of the recent Supreme Court pronouncement that to prevail under the FTDA, a party must prove actual dilution, it is even less likely that cybersquatting can be successfully stopped under that act.
9. To lessen one’s susceptibility to an attack from a cybersquatter, one should:
 - a. Determine where he/she may be exposed. It is no longer possible to effectively circumscribe your own use of a trademark. Online trademark disputes between English, U.S., Australian, Canadian and South African companies are common. Cross-border liability is difficult to predict—and rights are difficult to enforce. Cybersquatters may take advantage of foreign registration bodies to engage in blatant acts of trademark infringement and dilution—with minimal risk;
 - b. Set priorities among types of objectionable conduct, and create an enforcement strategy;
 - c. Register trademarks, since registration provides several legal rights and procedural advantages and is particularly helpful in pursuing cybersquatters under the ACPA and/or the ICANN Uniform Dispute Resolution Policy;
 - d. Register, as domain names, as many variations as possible of important trademarks and corporate names;

- e. Consider acquiring country code domain names, which may prevent the unauthorized use of your trademarks and brand names as domain names, thereby reducing potential confusion and lessen the likelihood of losing your identity to a cybersquatter; and
 - f. Not wait for the cybersquatter—instead one should perform regular searches to determine if one or more cybersquatters are trying to rip you off. In other words, one should not find out about a cybersquatter in a news report about a child who found herself at a porn site instead of your site.
10. Upon encountering a cybersquatter, one should immediately perform a cost-benefit analysis. Does it make more sense for the company to pay off the cybersquatters, or should it fight them until the bitter end? Will the precedent be more of a problem, or will the distraction of litigation undermine your business? Is this an individual without assets or a substantial business operation?

C. Cybergrippers

1. Before the rise of the Internet and e-commerce, harsh comments from a vocal critic could easily be written off, since it was very difficult for such opinions to be publicly aired. For example, it was extremely unlikely that a disgruntled customer would purchase an advertisement proclaiming to the world his or her opinion about a particular company.
2. Now vocal critics of a company or an organization, with increasing frequency, use the Internet to complain. These websites often craft names intentionally similar to the domain names of their targets. This way, the critic, or “cybergriper,” gets to preach to those who might be legitimately searching for the company or organization. For the cost of registering a domain name, anybody may loudly proclaim their opinion about a particular company, whether warranted or not on a website that often includes or approximates the domain name or trademark of their target. In fact, the registration of “organizationsucks.com” domain names is widespread. The question facing a business owner confronted with this issue is what to do in response.
3. There are many reasons a person may register an *organizationsucks.com* domain name. A person may be a former customer or employee and may be using *organizationsucks.com* as a way to express his or her displeasure with the company. The most famous example of such a site was at issue in *Bally*

Total Fitness Holding Corp. v. Faber, 29 F.Supp.2d 1161 (C.D. Cal. 1998). There, the defendant created a “Bally’s Sucks” web site to complain about Bally’s service. He used the Bally’s trademarks and logos on the site, though he superimposed on them the word “Sucks.” The outcome of this case is discussed below.

4. Alternatively, a person could register such a domain name for the purpose of deriving revenue either from the traffic to the site or by holding the name hostage in hopes that the business will pay to have it transferred. The key to determining trademark infringement under the Lanham Act is whether there is a likelihood of confusion of the source of the goods or services that are being used in relationship to the mark. 15 U.S.C. §1114(1)(a).
5. Based on that standard, the Lanham Act may be of limited use when a cybergriper is truly expressing his or her displeasure with the company. More specifically, it is extremely unlikely that a company could successfully argue that true cybergripping creates a likelihood of confusion. In the *Bally’s* case, the court held in favor of the cybergriper, noting there was no commercial purpose to his site and that since the defendant was not in the fitness club management business, there would be no likelihood of confusion. More recently, in *Taubman Co. v. Webfeats*, 319 F.3d 770 (6th Cir. 2003), the Sixth Circuit ruled that a domain name that added the word “sucks” to a trademark does not create a likelihood of confusion, and was protected speech under the First Amendment.
6. Although the odds of successfully challenging a true cybergriper are low, the odds of successfully fighting a cybersquatter trying to make money as a cybergriper have greatly improved since the adoption of the Anticybersquatting Consumer Protection Act of 1999 (“ACPA”) and ICANN’s Uniform Dispute Resolution Procedure (“UDRP”) rules (See discussion, *infra*.) (For a short while, UDRP arbitrators found against alleged cybergrippers in several instances, including cases involving natwestsucks.com, wal-martsucks.com, and dixonssucks.com domain names. In the *Natwest* case, the arbitrator noted that the respondents had registered more than 18 other well-known British communications companies’ names appended with sucks.com with no legitimate reason to do so. <http://arbiter.wipo.int/domains/decisions/html/2000/d2000-0636.html>) Both the ACPA and the UDRP arbitration rules recognize that there is a distinction between individuals such as Dan Parisi, who spent over \$100,000 registering most of the 500 largest companies’ trade

names appended with sucks.com and the true cybergriper, who starts a web site following a bad experience with a company.

7. In *Lucent Technologies, Inc. v. lucentsucks.com*, 95 F.Supp.2d 528 (E.D. Va. 2000), Lucent Technologies sued a person who registered *lucentsucks.com* allegedly to host a pornography site at that domain. Although the case was dismissed on jurisdictional grounds, the court indicated that the key to whether this was a case of cybersquatting was how the domain name was being used. If the site was being used to parody Lucent, a holding that Lucent was the proper owner of the domain name registration might conflict with the First Amendment. Alternatively, the court left open the possibility that Lucent may have a legitimate anticybersquatting claim if the domain name was being used for other purposes.
8. Although companies faced with a genuine cybergriper situation may not have a strong legal claim, a number of non-legal responses are available. When Dunkin' Donuts was faced by a similar problem, it chose to co-opt the cybergriper's site. Dunkin' Donuts found the site a useful source of customer information, so they took over the operation of the cybergriper site and eventually incorporated it into one of its own sites. Similarly, Circuit City monitors the cybergriper's site, resolves some of the posted customer problems, and then posts the resolution on the cybergriper's site.
9. The Dunkin' Donuts and Circuit City approaches might be the best course of action in the case of an actual cybergriper. When a company tries to shut down someone who is complaining about its product, not only is it likely to be unsuccessful, but it may also drive more traffic to the cybergriper's site. Thus, in many cases, the best action may be no action at all, particularly if the company wants to avoid having its cease-and-desist letter to the cybergriper posted on the cybergriper's site.
10. The intent of the cybergriper should determine how a domain name holder deals with an *organizationsucks.com* situation. If the site is hosted by a cybergriper, the company should consider ignoring it. If, however, the company is faced with an individual or entity attempting to profit from the use of the company's mark under the pretext of cybergripping, it might make a good case under the ACPA.
11. Related to the *organizationsucks.com* situation is one in which the cybergriper modifies the domain name, or registers the domain name in a different global top level domain name ("gTLD"), to attract web traffic intended for the

organization's website. For example, in *Planned Parenthood Federation of America, Inc. v. Bucci*, 42 U.S.P.Q.2d (BNA) 1430 (S.D. N.Y. 1997), *aff'd*, 1998 U.S. App. LEXIS 22179 (2d Cir. Feb. 9, 1998), *cert. denied*, 525 U.S. 834 (1998), an anti-abortion activist registered the domain name *plannedparenthood.com*. (Planned Parenthood Federation of America, Inc.'s domain name is *plannedparenthood.org*.) At the activist's site, visitors were greeted ("Welcome to the Planned Parenthood Home Page") and then invited to read anti-abortion texts. The court found that confusion did exist and ordered the domain name holder to relinquish the domain.

D. The Uniform Dispute Resolution Procedure ("UDRP")

1. Background

- a. In 1993, Network Solutions, Inc. ("NSI") won an NSF contract to be both the registrar and the registry of the Internet. Almost immediately, there were disputes between domain name holders and the owners of trademarks. In 1995, NSI established a dispute resolution system, but because of the following features, it was cumbersome:
 - i. Registration requirement;
 - ii. Identicality requirement;
 - iii. Time-consuming (i.e., domain name only "on hold");
 - iv. Requirement of suit/settlement agreement.
- b. In about 1997, the Internet Ad Hoc Committee ("IAHC") was formed. IAHC recognized that a mechanism was needed to address trademark owner concerns, including the discontinuity between the cost of domain name infringement and trademark enforcement and problems with jurisdiction and the determination of applicable law. During its existence, IAHC proposed protection for famous marks and understood any dispute resolution system had to be mandatory for both registrars and registrants.
- c. When ICANN was formed in 1998, it immediately recognized the need for an expedited dispute resolution procedure. At its meeting in August 1999, in Santiago, Chile, ICANN's Board of Directors adopted the UDRP, an expedited, electronic and inexpensive dispute resolution procedure to be applied informally by all gTLD registrars. To become a gTLD registrar, an

organization must adopt the UDRP as its procedure to resolve disputes. Since all gTLD registrars have adopted the UDRP, all domain name registrants are subject to its mandatory administrative procedures, *i.e.*, they cannot refuse to participate. Remedies under the UDRP are limited to the cancellation of the domain name or the transfer of the domain name registration to the complainant.

- d. ICANN approved the World Intellectual Property Organization (“WIPO”) as the first resolution service provider on November 29, 1999. ICANN has since approved several other dispute resolution service providers:
 - i. National Arbitration Forum, a Minnesota based organization, approved on December 23, 1999;
 - ii. Disputes.org/resolutions.ca, an international collaboration between eResolution.ca, an online arbitration service based in Montreal, and Disputes.org, an organization based in Amherst, Massachusetts, approved on January 1, 2000 (transferred solely to eResolution on October 16, 2000, and is no longer accepting proceedings commenced after November 30, 2001);
 - iii. CPR Institute for Dispute Resolution, approved on May 22, 2000; and
 - iv. Asian Domain Name Dispute Resolution Center (“ADNDRC”), with offices in Beijing and Hong Kong, approved on February 28, 2002.
- e. Under the UDRP, a mandatory arbitration proceeding is instituted if the complainant asserts that:
 - i. The domain name is identical/confusingly similar to its trademark.
 - ii. The domain name holder has no “legitimate interest” in the domain name.
 - iii. The domain name was registered and is being used in “bad faith.” To succeed, the complainant must prove that each of these elements is present.
- f. The arbitrators of UDRP disputes hail from all over the globe and bring widely differing understandings of substantive trademark law as well as procedural issues, such as burdens of proof. Moreover, the arbitrators are not required to follow any particular substantive body of law in reaching their decisions or to view previous arbitration decisions as precedent.

Consequently, some American practitioners have been reluctant to institute a UDRP arbitration.

2. *Identical/Confusingly Similar Requirement*

- a. Generally, the UDRP decisions interpreting whether the domain name at issue is identical or confusingly similar to the complainant's trademark, UDRP's first requirement, have been resolved in a manner consistent with U.S. trademark practice. For example, in *Microsoft Corp. v. Microsoft.com aka Ahmed*, WIPO Case No. D2000-0548 (July 21, 2000), the arbitration panel found that the domain name holder's slight variation in the "MICROSOFT" trademark did not overcome confusing similarity.
- b. In *Sallie Mae, Inc. v. Michele Dinoia*, WIPO Case No. D2004-0648 (Oct. 18, 2004), the panel found that there was no *confusing* similarity between complainant's mark and respondent's domain *sallie.com* because there was no actual confusion by consumers and because "sallie" is a commonly used name.
- c. In *Disney Enterprises, Inc. v. John Zuccarini, Cupcake City and Cupcake Patrol*, WIPO Case No. D2001-0489 (June 19, 2001), the issue of "typosquatting" is discussed. Typosquatting is defined as purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic off of the original site because of a user's misspelling of the name. In this case, respondent had registered several sites that were common misspellings of Disney's marks, such as: *disneychannel.com*, *disneyworld.com*, and *walddisney.com*. The panel found confusing similarity without question. They also pointed to the fact that all of the domain names at issue combined the mark "Disney" with misspellings of generic terms, such as "channel" or "world." They also stated that domain names that incorporate well-known trademarks can be readily confused with those marks. (See, *EAuto, L.L.C. v. Triple S Auto Parts d/b/a Kung Fu Yea Enterprises, Inc.*, WIPO Case No. D2000-0047 (March 24, 2000)).
- d. The WIPO arbitration panel has also found confusing similarity in cases where the disputed domain name:
 - i. Is phonetically identical or similar to complainant's mark. See, *Microsoft Corp. v. Mike Rushton*, WIPO Case No. D2004-0123 (April 27, 2004) (*mikerosoft.com*);

- ii. Is a translation or transliteration of the famous mark. *See, Microsoft Corporation v. J. Holiday Co.*, WIPO Case No. D2000-1493 (Feb. 20, 2001) (*Amicrosoft2000.com*);
- iii. Gives an overall impression of similarity to the famous mark. *See, Guinness UDV North America, Inc. v. Ukjent*, WIPO Case No. D2001-0684 (Aug. 9, 2001) (*s-m-i-r-n-o-f-f.com*);
- iv. Merely adds a prefix to a famous mark. *See, Ferrero S.p.A. v. Jean-Francois Legendre*, WIPO Case No. D2000-1534 (Feb. 22, 2001) (*mynutella.net*);
- v. Combines a famous mark with a geographical term. *See, Red Bull GmbH v. Chai Larbthanasub*, WIPO Case No. D2003-0709 (Nov. 11, 2003) (*thairedbull.com*); or
- vi. Is a combination of famous marks. *See, Societe Air France v. Daung Soo Ghim*, WIPO Case No. D2003-0891 (Feb. 13, 2004) (*airfrance-klm.com*).

3. *Legitimate Interest Requirement*

- a. UDRP decisions regarding the second requirement of the UDRP, *i.e.*, that the domain holder has no legitimate interest in the domain name, have been less congruent with U.S. law. The UDRP recognizes three defenses to UDRP complaints that are relevant to determining whether one has a “legitimate interest” in the domain name:
 - i. The defendant has made preparations for the bona fide use of the domain name before notice of complaint;
 - ii. The defendant is commonly known by the domain name *i.e.*, the domain name is a “nickname” for the domain name holder; and
 - iii. The defendant has a legitimate, noncommercial, or fair use of the domain name, without corresponding intent of commercial gain, market confusion, or tarnishment.
- b. These defenses all require an analysis of trademark concepts such as “fair use,” the standards for which vary from country to country.
- c. When a case requires such an analysis, arbitrators sometimes refuse to decide in favor of the complainant, instead referring the complainant to a national court of law. (*See, e.g., Weber-Stephen Products Co. v. Armitage*

Hardware, WIPO Case No. D2000-0187 (May 11, 2000)). Conversely, and contrary to most U.S. court decisions, arbitration panels have found in favor of trademark owners in cases regarding ****sucks.com* sites. See, e.g., *Wal-Mart Stores, Inc. v. Walsucks and Walmarket Puerto Rico*, WIPO Case No. D2000-0477 (July 20, 2000), where the arbitration panel found that the domain name holder did not have a “legitimate interest” in various *wal-martsucks.com* domains.

- d. In *General Motors Corporation v. Vette Owners*, WIPO Case No. D2000-0595 (Oct. 20, 2000), the panel transferred the domain name *corvette.com* after finding no legitimate interest. In the facts of the case, the only use that had been put to the website was to offer the domain name for sale. Although the respondent claimed to have plans for the use of the website as a forum for Corvette enthusiasts, there was no evidence that he had made a move toward doing so.
- e. However, in *Spirit Airlines, Inc. v. Spirit Airlines Pty. Ltd.*, WIPO Case No. D2001-0748 (July 25, 2001), the panel refused to transfer the domain *spiritairlines.com* because the respondent, an Australian airline, had incorporated under the name Spirit Airlines before registering the domain name, and was unaware of complainant, a low-cost U.S. airline, at the time of registration. The airline had a legitimate interest in the domain name.
- f. In *Windsor Fashions, Inc. v. Windsor Software Corporation*, WIPO Case No. D2002-0839 (Nov. 14, 2002), the domain name *windsor.com* was not transferred when respondent had been doing business using the domain name for many years, even though the complainant had a trademark registration in “Windsor” as related to fashions.
- g. In *SBC Communications v. Fred Bell*, WIPO Case No. D2001-0602 (July 8, 2001), the panel held that merely because the domain names (*bellinternet.com*, *bell-net.com*) included the respondent’s surname, “Bell,” this did not establish a legitimate interest in the domain name. They point specifically to the fact that the respondent did not do business and was not known commonly by the domain name, but only by his surname, without the additional terms included in the domain.

4. *Bad Faith Use And Registration Requirement*

- a. American trademark practitioners have been most perturbed by the UDRP decisions that turn on “bad faith use and registration,” the third

requirement of the UDRP. The UDRP provides that evidence of registration and use in bad faith shall include:

- i. Acquiring a domain name primarily for the purpose of reselling, renting, or transferring to the trademark or service mark owner for valuable consideration in excess of out-of-pocket costs; or
 - ii. Engaging in a pattern of such conduct designed to prevent a trademark or service mark owner from obtaining the domain name; or
 - iii. Registering a domain name primarily for the purpose of disrupting the business of a competitor; or
 - iv. Registering a domain name with the intent of creating a likelihood of confusion with the complainant's trademark or service mark and/or re-directing Internet traffic to the domain name holder's site through confusion.
- b. WIPO arbitration panels consider some of the following factors to determine whether, in fact, the registration of a domain name was done in bad faith:
- i. Offer to sell, rent, or license to complainant;
 - ii. Offer to sell, rent, or license to general public;
 - iii. Offer to sell, rent, or license for more than "out-of-pocket" costs;
 - iv. Pattern of conduct by respondent;
 - v. Disruption of competitor's business;
 - vi. Attracting Internet users and then automatically hyperlinking to other sites, i.e. pornography or competitor's sites;
 - vii. Giving of false contact information;
 - viii. Speculation in domain names;
 - ix. Inconceivable legitimate use;
 - x. Prior knowledge or notice of the mark;

- xi. Disclaimer;
 - xii. Prior relationship between parties;
 - xiii. Acquiescence of mark owner;
 - xiv. Cease and desist letters.
- c. On almost identical facts, arbitration panels found that the artist Sting should not have *sting.com* returned to him (*Sumner, p/k/a/ Sting v. Urvan*, WIPO Case No. D2000-0596 (July 24, 2000)), but that the domain name holder of *madonna.com* should transfer it to Madonna (*Ciccione p/k/a Madonna v. Parisi and Madonna.com*, WIPO Case No. D2000-0847 (October 12, 2000)). Arbitration panels have also been inconsistent in determining whether the ownership of a passive domain name constitutes a bad faith use of a complainant's trademark. *Compare, Telstra Corp. Ltd. v. Nuclear Marshmallows*, WIPO Case No. D-2000-0003 (February 18, 2000), with *Sporoptic Pouilloux SA v. Wilson*, WIPO Case No. D-2000-0265 (June 16, 2000).

5. UDRP Rules And Procedures

- a. The rules and procedures for UDRP actions are relatively straightforward:
 - i. Complainant selects a dispute resolution provider.
 - ii. Complainant submits a complaint to the dispute resolution provider.
 - iii. Complainant must submit to civil court jurisdiction where the registrar who registered the disputed domain name resides (if the domain name holder's residence is unknown); or where the domain name holder resides, if that can be established.
 - iv. Complainant chooses to have proceedings conducted by one or three panelists. If complainant chooses one panelist, respondent may elect a three-member panel; however, respondent must then pay part of the fees. (See below.)
 - v. The provider sends notice of the complaint to the domain name holder within three days, if the complaint is in compliance with the rules. Complainant has five days to correct the complaint if it is not in compliance.

- vi. The domain name holder has 20 days from the date of commencement of the proceeding to respond to the complaint.
 - vii. The provider appoints a dispute resolution panel of either one or three members, depending on the choice of complainant and respondent. For a one-member panel, the panelist is chosen by the provider. For a three-member panel, the complainant and respondent each provide a list of three potential panelists, one panelist being chosen from each list, and the third panelist being chosen by the provider.
 - viii. The provider sets a date for a decision of the dispute resolution panel.
 - ix. The dispute resolution panel renders a decision, usually referring solely to the complaint and the response. The decision shall be in writing and, in the case of a three-member panel, shall be made by a majority.
 - x. The dispute resolution provider sends the decision to both parties within three days of receiving it from the panel.
 - xi. Complainant pays fees (which vary depending on which resolution service is selected by the complainant) of the dispute resolution panel unless it chooses to have a one-member panel and the domain name holder wants a three-member panel. In that case, the fee is split 50/50 between the complainant and the domain name holder. The fees must be paid before the provider will take any action on the complaint.
 - xii. Only a civil court with jurisdiction over the complainant can stay the decision, and only within 10 days of the issuance of the decision.
- b. One should note, as well, that most of the providers have supplemental rules that must be followed for complaints filed with that particular provider.

E. The Anticybersquatting Consumer Protection Act

1. The Anticybersquatting Consumer Protection Act, codified as 15 U.S.C. §1125(d), creates a cause of action against the bad faith registration of, use of, or trafficking in domain names that are identical to or confusingly similar to another's trademark, or that are dilutive of another's famous trademark. Although the bad faith registration and use of domain names was previously actionable, the ACPA eliminates many substantive and jurisdictional prob-

lems that trademark owners were facing in trying to adapt trademark law to the cybersquatter situation.

a. 15 U.S.C. §1125(d)(1)(A) states:

A person shall be liable...if, without regard to the goods and services of the parties, that person—has a bad faith intent to profit from that mark..., and registers, traffics in or uses a domain name....

2. *Bad Faith Adoption*

a. Under the ACPA, cybersquatters who engage in the “bad faith” adoption of a domain name can be sued for infringement of a registered or unregistered mark, and the mere registration of a domain name, without a website or other activity, is now a statutory violation. Moreover, not only is a cybersquatter liable for ordinary damages, but the ACPA provides for statutory damages of up to \$100,000 per domain name, as well as attorney’s fees, as an additional deterrent against the warehousing of other domain name registrations obtained in bad faith. The ACPA also provides a cause of action for the bad faith registration of an individual’s name.

i. Damages are not available for domain names registered and used before the passage of the ACPA. However, the Third Circuit in *Schmidheiny v. Weber*, 319 F.3d 581 (3d Cir. 2003), recently ruled that re-registration of a domain name which was originally registered before the Act was passed activates the ACPA. *See also, Ford Motor Co. v. Catalanotte*, 342 F.3d 543 (6th Cir. 2003) (holding that the registrant can be liable for damages when he “trafficked” in the name, by offering to sell it to the car company, after the enactment of the ACPA even though the site was registered before).

b. The statute eliminates questions about whether a domain name is in “use.” Further, although the ACPA does not define “bad faith,” it does provide a list of factors that a court may consider in determining whether bad faith intent has been proven:

i. The trademark or other intellectual property rights of the person, if any, in the domain name;

- ii. The extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
 - iii. The person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
 - iv. The person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
 - v. The person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
 - vi. The person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
 - vii. The person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
 - viii. The person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
 - ix. The extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of section 43.
- c. The determination of bad faith intent will depend on the facts and circumstances of each individual case. A court is not limited to considering these nine factors when determining the presence or absence of bad faith.

The Second Circuit, in the first court of appeals case addressing the ACPA, noted that the most important grounds for finding bad faith “are the unique circumstances of this case, which do not fit neatly into the specific factors enumerated by Congress but may nevertheless be considered under the statute.” *Sporty’s Farm, LLC v. Sportsman’s Market, Inc.*, 202 F.3d 489, 499 (2d Cir.), *cert. denied*, 530 U.S. 1262 (2000).

- d. In *Domain Name Clearing Co., LLC v. F.C.F. Inc.*, 16 Fed. Appx. 108 (4th Cir. July 12, 2001), bad faith was found because DNCC did not own any trademark or intellectual property rights in Clarins; when it registered the domain *clarins.com*, DNCC was not commonly known by the domain name; DNCC never developed a web site at the domain name; it offered to sell the domain to the trademark owner at a high price; and it had registered over 70 domains and its primary business purpose was registering and selling domain names.
- e. In *Virtual Works, Inc. v. Volkswagen of America, Inc.*, 238 F.3d 264 (4th Cir. 2001), the court found bad faith intent in the registration of *vw.net* because Virtual Works had no right to or interest in the VW mark; it had never been referred to or done business under the name VW; disparaging comments posted by Virtual Works harmed the goodwill of the VW mark; and the VW mark was so famous.

3. *Good Faith Defense To Bad Faith Adoption*

- a. However, there is a good faith defense available under the ACPA to the domain name holder to rebut a claim of bad faith. Specifically, the court can determine that the defendant 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). In addition, the ACPA creates a safe harbor for registration bodies, protecting NSI and its brethren, so long as they act in good faith through the process.
- b. In *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 359, 369 (4th Cir. 2001), the court stated that a defendant who acts even partially in bad faith cannot benefit from the safe harbor provisions of the ACPA.

4. *Resolution Of Jurisdictional Issues*

- a. With this Act, Congress also attempted to alleviate one of the main difficulties in bringing suit against a cybersquatter—obtaining personal juris-

diction—by providing for *in rem* jurisdiction. A trademark owner may pursue this option in two scenarios: (1) if the registrant is not subject to personal jurisdiction in the forum, such as when the cybersquatter is located in a foreign country, (*see, e.g. Cable News Network LP v. cnnnews.com*, 66 U.S.P.Q.2d (BNA) 1057 (4th Cir. 2003) (unpublished opinion)); or (2) when the trademark owner cannot locate the registrant through due diligence, such as when incomplete or inaccurate information was provided to the registrar. 15 U.S.C. §1125(d)(2). However, a plaintiff cannot proceed under both *in rem* and *in personam* jurisdiction, since it is not possible to prove *in personam* jurisdiction while also proving its absence for *in rem* jurisdiction. *See, Alitalia-Linee Aeree Italiane S.p.A. v. Casinoalitalia.com*, 128 F.Supp. 2d 340 (E.D. Va. 2001) (finding that the ACPA provides trademark owners with “two mutually exclusive avenues for relief”). Although *in rem* jurisdiction makes it easier for trademark owners to bring actions under the ACPA, damages for *in rem* proceedings are “limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.” 15 U.S.C. §1125(d)(2)(D)(i). A plaintiff bringing an *in rem* action under 15 U.S.C. §1125(d)(2) may, in appropriate circumstances, pursue infringement and dilution claims as well as bad faith registration claims under section 1125(d)(1).

- b. Now that the ACPA has been in effect for several years, courts are actively defining its scope and its boundaries. Notably, courts have found that the ACPA does not allow trademark owners with hundreds of cybersquatter problems to “clean house” by suing all the names in one court instead of filing hundreds of cases around the country. This type of multi-defendant case, brought under an *in rem* action, has been attempted in and rejected by both the Second Circuit in *Porsche Cars N. Am., Inc. v. Porsche.net*, 302 F.3d 248 (4th Cir. 2002), and the Fourth Circuit in *Mattel, Inc. v. Barbie-Club.com*, 310 F.3d 293 (2d Cir. 2002). In both cases, the courts found that plaintiffs seeking to bring an *in rem* action against a domain name owner must bring the case in the domain name registrar’s judicial district, and cannot just bring the action in any district they want. However, an *in rem* action does not require minimum contacts by the domain registrant, only that the registrar be located in the judicial district. *See, CNN v. CNNNews*, 56 Fed. Appx. 599 (4th Cir. Jan. 23, 2003) (unpublished opinion).

5. Application To Foreign Marks

- a. Also, courts have recently tackled the question of whether the ACPA applies to cybersquatting violations of foreign marks. In *Barcelona.com v. Excelentísimo Ayuntamiento de Barcelona*, 330 F.3d 617 (4th Cir. 2003), the Fourth Circuit reversed the Eastern District of Virginia in a case which held that the ACPA did apply to violations of foreign trademarks. The lower court had reasoned that the language of the ACPA made no distinction between U.S. and foreign marks and that Congress was well aware of the international nature of the Internet when the law was drafted. However, the Fourth Circuit reversed on that grounds that the ACPA expressly required that the registrant's claim be decided under U.S. trademark law, meaning the Lanham Act, and not under the Spanish law, which was applied by the district court, and remanded for proceedings consistent with its opinion.
- b. In *Harrod's Ltd. v. Sixty Internet Domain Names*, 302 F.3d 214 (4th Cir. 2002), Harrod's UK had the exclusive trademark rights to "Harrod's" in the United States and in much of the world, but the defendants, Harrods BA, had registered trademarks in much of South America. In this case, the court upheld a finding of bad faith in that Harrods BA had registered several variations of the Harrod's mark as domain names with the intent to market its goods to non-South American consumers in areas where Harrod's UK had exclusive trademark rights. The court transferred the rights in the domain names to Harrod's UK.

6. Other Cases

- a. That the domain name be confusingly similar to the mark is another requirement of the ACPA. In *Coca-Cola Co. v. Purdy*, 382 F.3d 774 (8th Cir. 2004), the district court upheld a preliminary injunction against Purdy prohibiting him from using domain names confusingly similar to plaintiff's. The court stated that the question under the ACPA is not whether the domain names are likely to be confused with a plaintiff's domain name, but whether they are identical or confusingly similar to a plaintiff's mark. It is the challenged domain name and the plaintiff's mark which are to be compared. The inquiry under the ACPA is thus narrower than the traditional multifactor likelihood-of-confusion test for trademark infringement. The fact that confusion about a website's source or sponsorship could be resolved by visiting the website is not relevant to whether the domain name itself is identical or confusingly similar to a plaintiff's mark.

- b. Courts have also found for the site holders in cases brought against cybergrippers under the ACPA, in cases where the defendant never offered to sell the site to the trademark owner. *See, for example, TMI, Inc. v. Maxwell*, 368 F.3d 433 (5th Cir. 2004); *Lucas Nursery and Landscaping, Inc. v. Grosse*, 359 F.3d 806 (6th Cir. 2004); *Mayflower Transit, LLC v. Prince*, 314 F.Supp. 2d 362 (D.N.J. 2004); *Northland Ins. Cos. v. Blaylock*, 115 F.Supp. 2d 1108 (D. Minn. 2000). However, when there was an offer for sale, courts have applied the ACPA and found in favor of the trademark owner. *See, Harrison v. Microfinancial, Inc.*, 2005 U.S. Dist. LEXIS 2804 (D. Mass. Feb. 24, 2005); *Coca-Cola Co. v. Purdy*, 382 F.3d 774 (8th Cir. 2004); *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 359 (4th Cir. 2001).

F. Conclusion

1. As jurisprudence relating to the UDRP and ACPA has developed, blatant acts of cybersquatting have diminished. However, cybersquatters and cybergrippers have not gone away; instead, they have ratcheted up the sophistication of their cyberpiracy. To combat cybersquatting, the owners of trademarks must be constantly vigilant and, as the need arises, demand that additional protections be afforded them under the UDRP and/or that the ACPA be revised to include expanded or additional causes of action.

To purchase the online version of this article,
go to www.ali-aba.org and click on "online".