GOODWIN | PROCTER

# Domain Name Disputes: To Sue or Not to Sue

**By Brenda R. Sharton**

The past several months have brought about a sea change of available options in the ongoing battle between trademark holders and the entrepreneurial "cybersquatters" who threaten their ability to do business on the world wide web. Cybersquatters are those "malfeasants" who register another's trademark with the thought of selling it back to its "rightful" owner for a profit. On November 29, 1999, Congress passed the Anticybersquatting Consumer Protection Act (the Anticybersquatting Act) C an amendment to the Lanham Act C that provides a separate cause of action against those who register a domain name with a "bad faith intent to profit."[1] Cheers arose from big business as the Act made it easier to sue even those who had registered an infringing domain name using fictitious contact information and provided added incentive for "traditional" cybersquatters to throw in the towel given the threat of monetary damages up to $100,000.[2] At the same time, Adam Smith proponents questioned the wisdom of offering full scale protection to established trademark owners (read techno phobic big business) versus those (cyber-entrepreneurs?) who had the foresight to recognize the growing power of the Internet and register important domain names early on with the intent of making a buck.[3] All of this occurred in the wake of the fledgling Uniform Dispute Resolution Policy put into effect as of January 3, 2000 by the Internet Corporation for Assigned Names and Numbers (ICANN).[4]

Domain names come in two sizes: top level domain names ("TLDs") and second level domain names. Familiar TLD's include .com, .net, .org, .edu, .gov, .mil, and country codes such as .uk, for the United Kingdom and .se, for Sweden. Second level domain names ("SLD's") are part of the domain name that comes between the "www" and the ".com." Domain names are registered through one of several registrants, the largest being Network Solutions, Inc. of Virginia which, until recently, served as registrant for nearly all domain names. The process is simple, cheap and fairly anonymous.

One can register a domain name simply by logging on to register.com. Names are assigned on an automated, first come-first served basis. No supporting materials are needed and no questions are asked. It is cheap C to register a top level domain name for two years, all you need is web access (your local library can accommodate) and seventy dollars ($70). It is easy to provide false contact information as one is registering online, that is with virtual anonymity. As the famous saying goes, on the Internet, no one knows if you're a dog. All of these conditions have made the area of domain name registration ripe for wrongdoers and, thus, for litigation.

While some have argued that a domain name is merely an "address," and, thus, its use not actionable, the recent legislation and case law indicate otherwise.[5] Recently, one court has stated that a domain name is "more than a mere

Internet address," finding infringement of the VW mark by a company that had registered vw.net, a fact that caught Volkswagen's attention.[6] The short answer is that use of a domain name can certainly constitute trademark infringement in the right circumstances. That is, if there is a likelihood of confusion with a trademark, dilution of a famous mark or simply traditional cybersquatting, liability will follow.

As we can see from the plethora of legislation and litigation in this area, domain names do not always end up in the hands of the rightful owner. What options are available to the legitimate trademark holder that finds itself too late in the race to register its domain name? The two most obvious options C other than a pay off to the cybersquatter C are to file suit under the Anticybersquatting Act (and include traditional claims of trademark infringement) or file a complaint with ICANN under the UDRP and wait for an arbitrator's decision.

On November 29, 1999, Congress passed the Anticybersquatting Act as part of an amendment to the Lanham Act. The Anticybersquatting Act provides a private cause of action against those who "register, traffic in or use" a domain name with a "bad faith intent to profit." The domain name must be identical or confusingly similar to a distinctive or famous mark or dilutive of a famous mark[7] (*e.g.* whitehouse.com, a pornographic site set up using that domain name to divert traffic from Pennsylvania Avenue's site). For determining "bad faith," the Act sets forth nine nonexhaustive factors for courts to consider.[8] The first four factors look for the absence of bad faith. The last five look for conduct that tends to indicate circumstances of bad faith.

The first factor is the extent to which the defendant has trademark or other intellectual property rights in the name.[9] If you have any claim to the name either through use in commerce or registration of the trademark, this factor will weigh in your favor. The first factor is meant to identify those situations where there are two (or more) rightful trademark owners both with dibs on a domain name. For example, Hasbro, the maker of the board game Clue, sued Clue Computing of Massachusetts for registering the domain name clue.com.[10] The court ruled in favor of the computer company as it was a rightful trademark owner and had registered the name first.[11]

The second factor looks to the extent that the domain name is the same as the registrant's own legal name or name by which a person is identified.[12] Again, this factor would tend to show the absence of bad faith (*e.g.* you register JC Penney and your name happens to be just that).

The third factor is the registrant's prior use of the domain name in the bona fide offering of goods or services.[13] Through this factor, a court will more readily recognize a legitimate business owner who happens to have used a domain name to which others may have rights and is not trying to trade off the goodwill created by the trademark holder. It also indicates whether the registrant had previously been selling goods or services using the name without causing confusion.

Fourth, courts should look to whether the registrant has put up a website that is accessible under the domain name and makes legitimate or fair use of the name.[14] Through this factor, courts can assess whether there is bona fide or fair use such that there really is no bad faith intent to profit. That is, if the registrant has put up a noncommercial site or offers a parody, the use may not run afoul of the statue. It still, however, can constitute trademark infringement in certain circumstances, where the use is tangentially linked to a commercial endeavor or affects the complainant's ability to sell goods in commerce.[15]

With the fifth factor, the analysis shifts to an assessment of whether there are indicators of bad faith.[16] Specifically, the courts look to whether the registrant intended to divert

customers from the trademark owner's site C either for commercial gain or to tarnish or disparage the mark by causing confusion as to its source or affiliation. Famous examples of this are the cases involving wwwpainewebber.com (without the . after www) and whitehouse.com, both of which attempted to divert legitimate investors and political constituents respectively to porn sites. Painewebber obtained a preliminary injunction claiming that its mark would be diluted, a claim that under traditional trademark law requires that the mark be famous. Under the Anticybersquatting Act, relief is available regardless of whether the mark is famous.

The sixth factor is designed to catch "traditional" cybersquatting C that is it looks to whether the registrant has offered to transfer, sell or otherwise assign the domain name to the mark owner or any other party for more than out of pocket expense ("substantial consideration") without having used the domain name in the bona fide offering of any goods or services or has engaged in a pattern of doing so.[17]

Seventh, the courts will look to whether the registrant has used false contact information when registering the domain name with NSI.[18] Like the sixth factor, in the legislative history, Congress made clear that this practice has been a common thread in abusive domain name registration.[19]

Eighth, the courts should consider if the registrant has engaged in a pattern of acquiring multiple domain names that are identical to, confusingly similar to, or dilutive of others' marks, without regard to the goods and services offered.[20] Finally, the courts will look at the extent to which the mark incorporated in the domain name is distinctive and famous under §43(c)(1) of the Lanham Act.[21]

The Anticybersquatting Act provides two major weapons previously unavailable to those trademark holders fighting to secure "their" domain name: election of statutory money damages in lieu of traditional Lanham Act damages[22] and in rem jurisdiction.[23]

First, the statute provides for monetary damages (excepting the in rem situation) of $1,000 to $100,0000 per domain name.[24] This is significant in that, previously, a cybersquatter had the upper hand even if the trademark holder had a dead to rights trademark infringement claim. The expense of litigation (and length of the process) made it more attractive for a trademark holder to simply pay up rather than fight as the best one could get at the end of the sometimes arduous litigation process was a transfer of the name. A cybersquatter had very little downside in waiting to wear the trademark holder down through the litigation process. Now, the trademark holder starts the battle armed with the threat of serious money damages (at least serious to the typically smaller company or individual who is holding the domain name) available if they litigate and win. The threat is sometimes enough to cause David to throw in the towel much earlier on in a domain name battle with Goliath than under the old rules. Some argue that the fight is now mismatched and that large companies with the resources can now "reverse hijack" domain names- even those they have no rights to but simply want C by using the threat against smaller companies and individuals who may not have the same litigation budget.

Second, the Anticybersquatting Act also provides for in rem jurisdiction when the abusive domain name registrant cannot be found.[25] The in rem action is filed against the name itself in the jurisdiction in which it was registered. As NSI registered nearly all domain names until recently, nearly all in rem litigation has been brought in the rocket docket of the Eastern District of Virginia, where NSI is located. This provision led to early problems in which trademark holders, unclear on how to proceed, erroneously named NSI as a defendant (they just need notice, not service) and a sorting out of how much due diligence is enough.[26] The

Eastern District of Virginia has determined that waiting 8 days for a response to a letter is not enough of a wait to invoke the in rem provision.[27] Even though that court has stated that it believes the provision to be constitutional, one questions whether it will indeed hold up under a minimum contacts due process analysis in the future.

There has been only one reported appellate decision since the statute's enactment, though there have been numerous suits filed under it including one by Harvard University against a cybersquatter who had registered several Harvard related domain names including harvardgraduate.com and harvardyardsale.com. In the sole appellate decision, the Second Circuit found cybersquatting in a case where a competitor of Sporty's, the famous aviation catalogue, had registered sporty's.com and, once discovered (*i.e.* after the litigation started), started selling Christmas trees on a site under the domain name.[28] The Second Circuit found the explanation used by the competitor's executive that he was simply thinking back fondly to a childhood dog named "Spotty" and chose the name on that basis "more amusing than credible" in upholding the lower court's decision to transfer the domain name.[29]

In lieu of, or indeed in addition to, litigation under the Anticybersquatting Act, disgruntled trademark holders can file a complaint under the relatively new (effective January 3, 2000) ICANN Uniform Dispute Resolution Policy (UDRP) for an arbitration proceeding. It is quick (30-60 days), cheap (under $1000 unless you choose a three member panel) and, by all first accounts, pro trademark holder. To succeed under the UDRP, you must establish three critical elements:

- That the domain name is identical or confusingly similar to a trademark or service mark
- That the registrant has no rights or legitimate interest in the domain names; and
- The domain name has been registered and is being used in bad faith

To determine "bad faith" under the UDRP, the panel will look to four nonexhaustive factors, many of which are the same as under the Anticybersquatting Act and, like that Act, are designed to ferret out cyberpiracy. They are: whether the name was registered for extracting payment in excess of out of pocket expense; whether the name was registered to prevent the trademark owner from being able to use it if the registrant has engaged in a pattern of such conduct with other domains; whether the name was registered for the purpose of disrupting the business of a competitor; or whether the registrant has used the name to divert commercial traffic to its web site by creating a likelihood of confusion among Internet users.

ICANN arbitrators are seemingly pro trademark holder C at least in the first few months of decisions. Moreover, bad faith under the UDRP has been found even where the registrant simply registered and did not have text up at the site.[30] Under the UDRP, available relief includes only a transfer or cancellation of the domain name. Unlike the Anticybersquatting Act, no money damages are available.

Which avenue is best when battling cyberpiracy? With ICANN's UDRP, the process is quick, cheap, nonbinding and presents no immediate jurisdictional problems (*i.e.* you don't have to sue in a jurisdiction that may be inconvenient to get personal jurisdiction over a defendant). However, jurisdiction can become a disadvantage if the cybersquatter decides to fight as the UDRP requires the parties to stipulate that they agree to submit for purposes of appeal, to the personal jurisdiction of a competent court in either the jurisdiction where the registrar is or where the registrant is located. Moreover, no money damages are available C just a transfer of the name as a best case scenario. Finally, to succeed as a complainant you need a defendant

who is actually using the name, whereas under the Anticybersquatting Act, registration alone is enough.

Choosing to litigate also presents its pros and cons. On the upside, at the end of the road you get a final decision. Discovery is available, which may be important if the defendant's wrongdoing is not clear on the surface. Money damages also are available and serve an important function in negotiations. Finally, one can control jurisdiction to a certain extent (assuming you have personal jurisdiction over the cybersquatter or can file in rem in the Eastern District of Virginia). On the downside, we all are aware of how expensive and slow litigation can be in some circumstances and the choice of where to file suit will sometimes be limited by personal jurisdiction requirements.

Perhaps the key is staying out of trouble in the first place. If you are representing a start-up, advise your clients up front to perform a search with the United States Patent and Trademark Office (PTO) before choosing a name and spending money on advertising. If the name does not run afoul of a registered trademark, go ahead and register a trademark that is identical to your second level domain name with the PTO as well as with the applicable state registry. Next, once you have the clearance from your PTO search, register the second level domain name with all TLDs (.com, .net and .org) and pertinent country codes too (as the world becomes "smaller," these names will become increasingly important). Finally, if despite all of your best efforts you get a "cease and desist letter" from a company intent on "reverse hijacking" the domain name, if that company is in a foreign and inconvenient jurisdiction, consider filing a declaratory judgment action in your home jurisdiction asserting your rights in the name. That way, if Goliath decides to fight, at least you have tried to ensure that the fight takes place on your home court.

If you represent an established trademark holder, see to it that your client registers all important second level domain names associated with the company and its products and does so early and often. Once a domain name lapses, its fair game for anyone out there to scoop up. Have your clients pay the extra money and register the second level domain for the longest period available. Make sure that every conceivable second level domain associated with the company and its products is registered to you, as well as any common misspellings or variations of those names. Be vigilant of infringers C sweep the net periodically to catch those bold enough to use one of your trademarks in their metatags to divert customers looking for you to their site. Finally, strange as it may seem, consider having your clients register [company name]sucks.com. to keep in their domain name stable. To register [company name]sucks.com has become a common practice for disgruntled customers and/or former employees for the display of a "hate" site C part of an Internet phenomenon known as "cybergriping."[31] The practice became common after a court upheld the registration and use of "ballysucks.com" by a registrant who had a less than favorable experience with the health club.[32]

---

*[1] The Anticybersquatting Consumer Protection Act of 1999, 15 U.S.C. § 1125(d) (amending § 43(d) of the Trademark Act of 1946).*

*[2] 15 U.S.C. § 1125 (d).*

*[3] See Professor Pamela J. Smith, Boston College Law School, Trademarks and Domain Names: An Imperfect Fit, 15th Ann. Spring CLE Prog.: Patent, Trademark and Copyright Law, 311 (2000).*

*[4] The policy can be found at http://www.icann.org/udrp/udrp.htm.*

*[5] See Virtual Works, Inc. v. Network Solutions, Inc., Volkswagen of America, Inc., Civil Action No. 99-1289-A (E.D. Va. March 10, 2000) (domain name is more than a mere Internet address).*

*[6] Id.*

*[7] See 15 U.S.C. §1125(d)(1)(B).*

*[8] Id.*

*[9] 15 U.S.C. §1125 (d)(1)(B)(i)(I).*

*[10] See Hasbro, Inc. v. Clue Computing, Inc., 66 F.Supp.2d 117 (D. Mass. 1999) (where two companies have legitimate trademark claims in a domain name, the first in time to register will prevail).*

*[11] Id.*

*[12] 15 U.S.C. §1125 (d)(1)(B)(i)(II).*

*[13] 15 U.S.C. §1125 (d)(1)(B)(i)(III).*

*[14] 15 U.S.C. §1125 (d)(1)(B)(i)(IV).*

*[15] See OBH, Inc. v. Spotlight Magazine, Inc., 86 F.Supp.2d 176(W.D. NY 2000); Jews for Jesus v. C. Brodsky, 993 F.Supp. 282 (D. N.J. 1998); Planned Parenthood Fed'n of Am., Inc. v. Bucci, 1997 WL 133313 at *3 (S.D.N.Y. 1997), aff'd 152 F.3d 920 (2d. Cir. 1998).*

*[16] 15 U.S.C. §1125 (d)(1)(B)(i)(V).*

*[17] 15 U.S.C. §1125 (d)(1)(B)(i)(VI).*

*[18] 15 U.S.C. §1125 (d)(1)(B)(i)(VII).*

*[19] See Panavision Int'l v. Toeppen, 141 F.3d 489 (2d Cir. 2000) (offer to sell domain names for an exorbitant amount to the rightful owners is evidence of bad faith); see also S. Rep. No. 1255 at 10515 (1999) (Senator Hatch's speech).*

*[20] 15 U.S.C. §1125 (d)(1)(B)(i)(VIII).*

*[21] 15 U.S.C. §1125 (d)(1)(B)(i)(IX).*

*[22] See 15 U.S.C. § 1116, § 1117(a).*

*[23] 15 U.S.C. § 1125(d)(2)(A).*

*[24] 15 U.S.C. § 1117(d).*

*[25] 15 U.S.C. § 1125(d)(2)(A); see Quokka Sports Inc. v. Cup Int'l Ltd. No. C. 99-5076-DLJ (N.D. CA 1999) (California court had in rem jurisdiction over a New Zealand-based company in an anticybersquatting suit).*

*[26]See Jennifer L. Alvey, In Rem Domain Suits Are Creating Confusion: Plaintiffs Give 'Notice' by Suing Registrar Too, BNA Electronic Commerce & Law Report, vol. 5 no. 13 at 315 Mar. 26, 2000.*

*[27] Lucent Technologies, Inc. v. Lucentsucks.com, 2000 WL 554567 *3 (E.D. Va. 2000).*

*[28] See Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d. 489, 499 (2nd Cir. 2000).*

*[29] Id. at 498.*

*[30] See Telstra Corp. Ltd. v. Nuclear Marshmallows, ICANN Case No. D2000-0003 (2000); see also M. Scott Donahey, The First ICANN Cybersquatting Decisions, Cyberspace Lawyer, April 2000 (highlighting ICANN's rejection of stockpiling domain names without using them).*

*[31] Lucent Technologies, Inc. v. Lucentsucks.com, 2000 WL 554567 FN9 (E.D. Va.).*

*[32] See Bally Total Fitness Holding Corp. v. Farber, 29 F. Supp. 1161 (C.D. Cal. 1998) (use of health club's "bally" trademark in site entitled ballysucks.com did not create a likelihood of confusion).*