

# TrademarkThoughts

Trademark  
and  
Copyright  
Group

Fall 2009

Published by  
Fish & Richardson

Trademark  
use in  
strategic  
business  
policy

fr.com  
800-818-5070  
info@fr.com

## Defeating Cybersquatters

Many unsuspecting American businesses are losing sales and facing intellectual property rights erosion due to an unwelcome Internet presence: the cybersquatter. Cybersquatters reportedly have already cost businesses approximately \$175 billion worldwide in lost revenue.<sup>1</sup> This article will discuss the parameters of anti-cybersquatting laws and various legal and practical options for companies to combat these modern-day outlaws.

### The Early Days of Cybersquatting

Cybersquatters register domain names that are the same as or confusingly similar to existing brands. Similar to traditional “squatters,” cybersquatters stake claims to unused Internet domain names, and refuse to leave without compensation. In the mid-1990’s, a virtual gold rush on domain name registrations was fueled by tales of regular folks striking it rich, armed only with the clothes on their backs and dial-up AOL accounts.

Perhaps the most notorious of the early cybersquatters, Dennis Toeppen, registered domain names similar to Delta Airlines, Neiman Marcus, Eddie Bauer, and more than 100 other marks. His comeuppance resulted from his registration of panavision.com and his clever, or so he thought, posting of photographs of the city of Pana, Illinois, on the Web site. Toeppen offered to sell the domain name to Panavision for \$13,000, asking in his “offer” letter: “why do you want to fund your attorney’s purchase of a new boat (or whatever) when you can facilitate the acquisition of ‘Panavision.com’ cheaply and simply instead?”

Panavision instead filed one of the first cybersquatting lawsuits.<sup>2</sup> As no statute or common law specifically addressed cybersquatting at the time, Panavision relied upon the Federal Trademark Dilution Act (FTDA). FTDA protected against the tarnishment, or loss of distinctiveness, of famous trademarks, whether or not there was likelihood of confusion or competition. In a decisive victory, the Ninth Circuit ruled for Panavision, unpersuaded by Toeppen’s argument that his use of panavision.com was neither commercial nor in bad faith. “Toeppen’s commercial use was his attempt to sell the trademarks themselves,” so it “does not matter that he did not attach the marks to a product.”<sup>3</sup> Also of significance was the court’s recognition that a domain name is “more than [an] address” and carries with it the significant purpose “to identify the entity that owns the Web site.”<sup>4</sup>

### Modern Remedies Against Cybersquatting

Notwithstanding the *Panavision* decision, trademark laws were not well suited to address various nuances of cybersquatting. Other district court decisions refused to hold that mere “warehousing” of a domain name for the purpose of selling it constituted “use in commerce” of an infringing trademark, thus leaving a legal loophole for cybersquatters in most jurisdictions. Accordingly, in 1999 Congress enacted the Anticybersquatting Consumer Protection Act (ACPA).<sup>5</sup> The same year, the Internet Corporation for Assigned Names and Numbers adopted the Uniform Domain Name Dispute Resolution Policy (UDRP), a low-cost administrative procedure specifically designed to resolve cybersquatting issues. Since the adoption of ACPA and UDRP, numerous court rulings and administrative decisions have defined the scope of these laws and confirmed their effectiveness in curbing unlawful Internet activities.

While there are now multiple strategies one can pursue to ensure that trademark rights are not infringed online, by no means has the Wild West of cyberspace been completely tamed. Choosing the best approach for a specific situation is more crucial than ever. Reaping a ransom for transfer of the domain is less common now than in the past, but present-day cybersquatters still generate illicit revenue by hosting “parked” Web pages that contain advertisements and links to goods and services that compete with the brand-holder’s business. Each click on a banner or link will result in profit for the cybersquatter and the loss of a potential sale to the brand owner.

Cybersquatters also may use their domain names to redirect to a competing Web site, again resulting in a loss of business to the brand-holder. Along with this tangible harm, this causes significant damage to the targeted owner’s intellectual property rights. As consumers searching for an official company Web site are led to unrelated pages, the brand becomes increasingly diluted. This is especially true if consumers are led to believe that an unauthorized Web site is endorsed by or affiliated with the brand-holder itself, resulting in a diminution of consumer trust in the brand.

*A guide to options that should be considered (with counsel) to defend against cybersquatting:*

### First Steps:

#### ◆ *Be the First to Register*

Sometimes the best defense is a good offense. Domains can be obtained for as little as \$1.99 each. By preemptively registering all of the top-level domains (e.g., .com, .net, .info, .biz) that relate to any existing or planned brand names, one limits vulnerability and the likelihood of a costly encounter with a cybersquatter. Planning in advance to accommodate the inattentive Web-surfer by registering domains with commonly misspelled words is an additional step. In the long term, this planning can be expected to save both time and money.

#### ◆ *Contact the Cybersquatter*

Through various online tools, it is generally possible to track down almost any domain registrant. Having a trademark attorney send a cease and desist letter to a cybersquatter, advising of legal rights and requesting the voluntary transfer of the domain, will sometimes work. If the cybersquatter complies, potentially expensive legal action is avoided; if not, little is lost.

### Available Legal Action:

Generally, legal options are administrative remedies through the UDRP or a federal lawsuit under the ACPA.

#### ◆ *Elements of a Cybersquatting Claim*

The basic elements of the UDRP and the ACPA are virtually identical. Under the UDRP, the plaintiff must prove: 1) that the domain is confusingly similar to its trademark; 2) that the registrant does not have a legitimate interest in the domain name; and 3) that the registrant registered and is now using the domain in “bad faith.” Under the ACPA, the plaintiff must prove: 1) that the domain is confusingly similar (or dilutive) of its trademark; and 2) that the registrant has registered, trafficked in, or used the domain name in “bad faith.”

#### ◆ *Basic Differences Between the UDRP and the ACPA*

In determining whether it makes more sense to file a complaint for cybersquatting under the UDRP or the ACPA, one should consider the following differences between the two legal mechanisms:

A company should consider proceeding under the UDRP when it seeks the relatively speedy and low-cost transfer of an offending domain name. As compared to a federal lawsuit, which can last anywhere from six months (for a default judgment) to three years, the average UDRP proceeding lasts approximately six weeks. Legal fees for the administrative proceeding will be considerably lower, as the entire UDRP process consists of a single complaint and an optional reply brief. Unlike formal litigation, there is no discovery, no motion practice, no in-person hearings, and no trial. However, the UDRP mechanism affords a limited remedy. A successful plaintiff can only obtain the transfer of the infringing domain name. There is no possibility of recovering monetary damages.

In especially egregious cases in which a cybersquatter has registered numerous infringing domains that have caused measurable financial damage to a business, it often is advisable to choose the ACPA option, which allows for up to \$100,000 in damages per domain as well as costs and attorney’s fees. Further, in contrast to the UDRP, which requires that the plaintiff prove bad faith registration and use of the domain name, the ACPA only requires bad faith registration or use. A company should bring a federal action under the ACPA in cases in which the cybersquatter initially procured the domain innocently but subsequently commenced using the corresponding Web site in a manner designed to capitalize on the goodwill of the company’s trademark.

#### ◆ *Typosquatting—The Registration of Confusingly Similar Domains*

Note that both laws require only that the infringing domain be “confusingly similar,” not “identical” to an existing trademark. This distinction is key, as more than a decade has passed since the initial “gold rush” on Internet domain names, and the majority of domains that are identical to established trademarks have been taken. The days of stumbling upon an available domain such as walmart.com or mcdonalds.com are long over. But a new form of cybersquatting called “typosquatting” is alive and well. Typosquatting involves the registration of domains with a slight misspelling of a brand name in an attempt to capture careless Web-surfers (e.g., walmart.com or mcdonalds.com). Another variation of typosquatting involves the addition of common generic terms to the trademark in an effort to lure unsophisticated Internet users who type in descriptive search terms in their Web browser (e.g., walmartsales.com, mcdonaldschickennuggets.com). Both types of domains are considered infringing, so long as the trademark owner can prove “bad faith” on the part of the domain name registrant.

“By preemptively registering all of the top-level domains (e.g., .com, .net, .info, .biz) that relate to any existing or planned brand names, one limits vulnerability and the likelihood of a costly encounter with a cybersquatter.”

*“It is considered bad faith to use a domain name that is confusingly similar to an existing trademark in order to attract customers to a Web site that offers and sells goods and services in direct competition with the trademark owner.”*

◆ *What Constitutes Bad Faith?*

In addition to the registration of a confusingly similar domain, under both the UDRP and the ACPA, the concept of “bad faith” is fundamental to establishing a successful claim for cybersquatting. In determining whether a domain name registrant is a cybersquatter or is simply an innocent party, any one or more of the following types of behavior may support the mandatory “bad faith” element:

1. *The registrant has attempted to sell the domain for profit.*  
The registrant must attempt to sell the domain “for profit;” an offer that merely amounts to the original purchase price of the domain is not “bad faith.” “Respondent’s general offer of the disputed domain name registration for sale establishes that the domain name was registered in bad faith...”<sup>6</sup>
2. *The registrant used false information when registering the domain.*  
Many cybersquatters use incorrect names, addresses, telephone numbers and e-mail addresses on the “whois” registry in order to avoid detection. Cases hold that providing false or misleading information in connection with the registration of the domain name is evidence of bad faith under the UDRP<sup>7</sup> and under the ACPA.<sup>8</sup>
3. *The registrant has a history of cybersquatting.*  
To discover whether a registrant has a history of cybersquatting, one should conduct a “reverse whois” search to determine whether the registrant owns numerous other domains incorporating third-party trademarks. Both UDRP and ACPA cases have consistently found bad faith where there existed a pattern of registering domain names that incorporate well-known third-party trademarks.<sup>9</sup> One also may search the public records of the National Arbitration Forum at <http://domains.adrforum.com/decision.aspx> to see if the registrant has been a defendant in other UDRP proceedings.<sup>10</sup>
4. *The registrant receives revenue from “click through” advertisements.*  
Using a domain name consisting of a confusingly similar variation of another’s mark for the purpose of providing links to third-party commercial Web sites constitutes bad faith.<sup>11</sup> Whether or not the registrant is in fact profiting from the generation of “click through” fees, the law presumes that he or she is doing so in order to unfairly profit from the goodwill associated with the plaintiff’s mark.<sup>12</sup>

5. *The registrant offers competing goods and services.*  
It is considered bad faith to use a domain name that is confusingly similar to an existing trademark in order to attract customers to a Web site that offers and sells goods and services in direct competition with the trademark owner. This is the case whether the defendant directly offers goods and services for sale or whether it leads consumers to other third-party sites through links or search results listing the plaintiff’s competitors.<sup>13</sup>
6. *The registrant “transfers” the domain name to a new registrant after receiving a cease and desist letter or after being served with a complaint.*  
In most cases, such a “transfer” is simply a fraudulent name-change designed to avoid liability, and the original registrant retains full control of the domain name. This too is considered evidence of bad faith.<sup>14</sup>
7. *The registrant refers to the plaintiff or its goods and services on its Web site.*  
The express use on the registrant’s Web site of the plaintiff’s logos or references to its goods and services also constitutes registration and use in bad faith. For example, the plaintiff prevailed in a recent ACPA action in which the defendant prominently featured the plaintiff’s trademarks and logos on his site in connection with the unauthorized sale of branded merchandise.<sup>15</sup>
8. *The registrant has knowledge of the plaintiff’s trademark rights.*  
The registrant’s knowledge may be “actual” or “constructive.” The former is established either by direct acknowledgment by the registrant or more commonly, through evidence that the registrant received the plaintiff’s cease and desist letter.<sup>16</sup> The latter may be established by the fact that the plaintiff possesses a federal registration with the U.S. Patent and Trademark Office for the trademark in question.<sup>17</sup>

### Conclusion

Above is much of the information necessary to take on and defeat the cybersquatter, scourge of the Internet. Those who encounter cybersquatters should, of course, consult an experienced trademark attorney, and together, protect the valuable goodwill in their company’s trademarks!

By Andrew M. Abrams

- <sup>1</sup> Howard, Theresa, *Cybersquatting Crooks Profit on Marketers' Brand Names*, USA TODAY May 11, 2009.
- <sup>2</sup> *Panavision Int'l. v. Toepen*, 141 F.3d 1316 (9<sup>th</sup> Cir. 1998).
- <sup>3</sup> 141 F.3d at 1325.
- <sup>4</sup> *Id.*
- <sup>5</sup> Codified at 15 USC 1125(d).
- <sup>6</sup> *Bank of Am. Corp. v. Nu. Free Cmty. Access*, FA 180704 (Nat. Arb. Forum Sept. 30, 2003); see also *Virtual Works, Inc. v. Volkswagen of America, Inc.* (finding bad faith where the defendant offered the <vw.net> domain name for sale to Volkswagen).
- <sup>7</sup> *Victoria's Secret et al. v. Tri X Group, Ltd.*, FA 96540 (Nat. Arb. Forum Feb. 1, 2001).
- <sup>8</sup> *DaimlerChrysler v. The Net Inc.*, 388 F.3d 201 (6<sup>th</sup> Cir. 2004).
- <sup>9</sup> *Sony Kabushiki Kaisha v. Anderson*, FA 198809 (Nat. Arb. Forum Nov. 20, 2003) (finding a pattern of registering domain names in bad faith when the respondent previously registered domain names incorporating well-known third-party trademarks); and *E. and J. Gallo Winery v. Spider Webs Ltd.*, 129 F.Supp.2d 1033 (SD Tex. Jan. 24, 2001), *aff'd*, 286 F.3d 270 (5<sup>th</sup> Cir. 2002) (Court ordered defendant to transfer <ernestandjulio.gallo.com> to plaintiffs, noting that defendant had registered approximately 2,000 other domain names, including those involving the names of many famous companies and places).
- <sup>10</sup> *Westcoast Contempo Fashions Ltd. v. Manila Indus., Inc.*, FA 814312 (Nat. Arb. Forum Nov. 29, 2006) (finding bad faith registration and use where the respondent had been subject to numerous UDRP proceedings where panels ordered the transfer of disputed domain names containing the trademarks of the complainants).
- <sup>11</sup> *The Leather Factory, Inc. v. Virtual Sky*, FA 611781 (Nat. Arb. Forum Feb. 1, 2006) (finding bad faith registration and use because "Registrant is using the disputed domain name to provide links to third-parties offering commercial products and services...similar to those provided by Complainant"); and *Citigroup, Inc. v. Chen Bao Shui*, 611 F.Supp.2d 507 (E.D.Va. 2009) (Court found violation of the ACPA where the defendant registered <citybank.org> and used the site to garner click-through revenue).
- <sup>12</sup> *Intel Corporation v. M. Macare aka M. Macar*, FA 660685 (April 26, 2006) ("[T]he Panel infers that Respondent receives click-through fees for each consumer it diverts to these other websites[,] finds that Respondent is taking advantage of the confusing similarity between the domain names and Complainant's marks in order to profit from the goodwill associated with the marks, and holds that Respondent's registration and diversionary use of the disputed domain names constitutes bad faith...").
- <sup>13</sup> *Lahoti v. Vericheck, Inc.*, 2007 WL 2570247 (W.D. Wash. Aug. 30, 2007) (finding bad faith where the defendant's Web site directed consumers to another site that provided search results listing some of plaintiff's competitors); and *Ritchie Bros. Auctioneers (Canada) Ltd. v. Stargateway*, FA 616234 (Nat. Arb. Forum Feb. 6, 2006) (finding for complainant and ordering transfer of domain name where "Respondent's use of the ritchiebrother.com domain name in association with a website that offers similar products and services to those of Complainant suggests that Respondent is attempting to attract Internet users to its website through a likelihood of confusion").
- <sup>14</sup> *A. H. Belo Corp. v. King TV and 5 Kings*, D2000-1336 (Dec. 8, 2000 WIPO); and *Cricket Communications, Inc. v. Louise Oliver*, FA 954005 (Nat. Arb. Forum May 29, 2007) (bad faith found where the registrant transferred the domain names immediately after being served with the UDRP complaint, a transaction that the Panel found to be "almost certainly a sham").
- <sup>15</sup> *Audi AG v. D'Amato*, 381 F.Supp.2d 644 (E.D. Mich. 2005) (plaintiff prevailed in ACPA action where defendant prominently featured the AUDI trademarks and logos on his <audisport.com> site in connection with the unauthorized sale of AUDI-branded merchandise); see also *World Wrestling Federation Entm't, Inc. v. Ringside Collectibles*, D2000-1306 (WIPO Jan. 24, 2001) (concluding that the respondent registered and used the <wwfauction.com> domain name in bad faith because the name directed users to a commercial Web site that the complainant's customers were likely to confuse with the source of the complainant's products, especially because of the respondent's prominent use of the complainant's logo on the site).
- <sup>16</sup> *Silpada Designs, Inc. v. O'Malley*, CA No 04-2303-CM (D. Kan 2006) (affirming statutory damages where domain name was registered after cease and desist letter was received).
- <sup>17</sup> *Orange Glo Int'l, Inc. v. Blume*, FA 118313 (NAF Oct. 4, 2002) (finding that respondent had constructive notice of the complainant's trademark rights where the complainant possessed a federally registered trademark).