

Recent Trends in Domain Name Registrations and Cybersquatting

BY ALEXANDRE MONTAGU & THOMAS WALSH

Alexandre Montagu (alex@montagulaw.com) is a founding Partner of Montagu Law, P.C., New York City (http://www.montagulaw.com). Thomas Walsh (tom@montaguelaw.com) is an associate with the firm.

Introduction

The passage of the Anticybersquatting Consumer Protection Act (the “ACPA”) was heralded as a major weapon to combat cybersquatting. Yet, nine years later, cybersquatters are more prevalent than ever. In 2007, a record 2,156 complaints alleging cybersquatting were filed with WIPO.

In an increasingly digitized world, a company’s top level domain name may be more valuable than its physical address, a fact that has not escaped cybersquatters, who have become more prevalent than ever. In order to be prepared to offer competent advice in this area, practitioners must stay abreast of current practices by cybersquatters, as well as potential responses thereto.

This article will discuss some recent trends in the area of domain name registration practices, as well as the long-standing problem of cybersquatting related to new product names or company names following a merger.

Domain Name Tasting

After registering a domain through an ICANN-accredited registrar, there is a 5-day grace period within which a full refund can be obtained if the registrant

elects not to keep the domain. *Domain name tasting* is the practice of registering domains (often in bulk) for the purpose of using the 5-day grace period to determine whether sufficient pay-per-click revenue will be earned to offset the cost of registering a particular domain. The registrant will then drop any domains that do not provide sufficient revenue and obtain a full refund. It is likely that many of the “successful” domains incorporate the trademarks of others in some way, either through misspellings or in combination with other terms. This practice has become very com-

CONTINUED ON PAGE 4

Content HIGHLIGHTS

Russia Revises the Rules Applicable to State Registration of License

by Eugene Arieievich, Margarita Divina & Marina Sharaeva 7

Litigation

by Zachary Levine 10

Complete Table of Contents listed on page 2.

CONTINUED FROM PAGE 1

mon. The CEO of GoDaddy.com noted that “In February 2007, 55.1 million domain names were registered. Of those, 51.5 million were canceled and refunded just before the 5 day grace period expired and only 3.6 million domain names were actually kept.”¹

In January 2008, ICANN proposed several possible solutions; however, it could take years for any changes to be agreed upon and implemented. In the meantime, at least one company has attempted to combat this practice in court – Verizon commenced litigation in Federal District Court of the Central District of California against a company that had both tasted and registered a large number of domains that allegedly incorporated Verizon’s trademarks, as well as the company’s registrar (which is affiliated with the company). Verizon contended that the registration of these domain names violated the ACPA. On June 30, 2008, the Court rejected the defendants’ argument that they were merely reserving the domains during the tasting period as opposed to registering them, and found that the defendants’ conduct constituted bad faith intent to profit under the ACPA.² The Court also issued a preliminary injunction against the defendants prohibiting them from registering any domain names that are confusingly similar to Verizon’s marks.

This decision is important, as it is believed to be the first decision which has found liability for domain tasting, as well as the first time that a registrar has lost an ACPA lawsuit. Soon after this decision was issued, the parties reached a settlement whereby the defendants agreed to be permanently enjoined from registering any domain names that are confusingly similar to Verizon’s marks.

Front-Running

Front-running occurs when a domain name registrar (or a registrar insider) uses insider information to register domains that generate numerous lookup requests in an effort to either re-sell them or earn advertising revenue. This practice recently gained attention when Network Solutions was accused of front-running in connection with its policy of automatically reserving a domain name every time someone conducted a search for a do-

main on Network Solution’s website, and holding it for the 5-day grace period. The practical effect of Network Solution’s practice was that anyone who searched for a domain on Network Solution’s website and then attempted to register it through another registrar (many of whom offer cheaper prices than Network Solutions), would be prevented from doing so. In February 2008, a class action lawsuit was filed against Network Solutions in connection with the front-running allegations under the following theories: fraudulent concealment; aiding and abetting fraudulent concealment; and unjust enrichment. The lawsuit is currently pending.

Despite the long-standing suspicions by many people concerning the existence of front-running, an ICANN panel recently investigated 120 cases of alleged front-running and found that there was insufficient evidence that such practices exist in any appreciable measure³. Nevertheless, it is a topic that is sure to remain in the minds of many in the domain name industry, and companies should be cognizant of registrars’ policies in this area prior to performing any availability searches on the respective websites.

Use of Privacy Services

Another vexing issue confronting trademark owners who seek to recover unauthorized domains is cybersquatters’ use of privacy or proxy registration services. These services allow registrants to conceal their identity on the publicly available Whois records. This can potentially hinder trademark owners in various ways. First, it hinders the initial investigation into potentially infringing activity connected to unauthorized domain registrations. Second, it impairs communication with the registrant.

The first step in recovering a domain is usually to send the registrant a cease and desist letter. However, because the only publicly available address for the registrant is the privacy service address listed in the Whois record, the trademark owner cannot ascertain whether or not the notice was received. These services provide potential cybersquatters with a virtual carte-blanche to register infringing domains. Potential cybersquat-

ters know that, as opposed to litigation, it will be more cost efficient for a company to seek recovery of an infringing domain through the UDRP process. And at that point, the registrant can simply choose not to respond. Consequently, the only harm suffered by the registrant will be the loss of the domain. Therefore, if a particular company is a common victim of cybersquatters, it may elect to file a federal lawsuit under the ACPA because damages are available under the ACPA and a favorable decision could also have a deterrent effect on future cybersquatters.

Domain Name Warehousing

Domain name warehousing refers to the practice by registrars of obtaining control of domains after they expire and either auctioning them off or using them to generate advertising revenue. It was recently reported that GoDaddy had been warehousing domains by transferring ownership of some expired domains to one of its subsidiaries.⁴ GoDaddy had taken steps to hide this practice, such as incorporating the subsidiary in a different state and using a Whois privacy service when transferring the domains.

However, the subsidiary's connection to GoDaddy was revealed in a 2006 IPO. In response to the recent publicity surrounding their warehousing practices, GoDaddy's CEO indicated that they are shutting down the subsidiary and placing all of its domains up for auction.⁵ It appears that sometimes public shame may be the most effective way to combat unscrupulous domain name registration practices.

Cybersquatting Related to Mergers/ New Product Names

In situations such as mergers or new product launches, if companies are not careful, one simple oversight can cost them hundreds of thousands of dollars. It cannot be overstated that practitioners and their clients should be proactive and vigilant in connection with domain name registrations before a product is launched or prior to a merger being announced.

However, it is also important to recognize that there are certain instances where proactively registering such domains is not a viable option. For example, if a company is contemplating a merger, it will likely want to avoid leaking that information to the public. MCI WorldCom encountered this very situation in the days leading up to its merger with SkyTel Communications in 1999. After the domain name registration became public, SkyTel's stock rose 16 percent. MCI then denied that the domain name registration was an indication of the company's intention, and the share price dropped, only to rise again after MCI announced the acquisition a few days later. MCI was later sued for allegedly influencing the price of the stock.

Adding support to this notion is a recent study conducted by London's Cass Business School, which found that fewer than half of merger and acquisition transactions are completed if they are prematurely leaked, compared to a 72% completion rate for deals that are not leaked.⁶ Consequently, under merger or new product launch scenarios, companies should be proactive with their domain registrations, but cognizant of the way in which the domains are registered and the unintended consequences that could arise as a result thereof.

Recovery of Infringing Domains

There are a few ways in which those victimized by cybersquatters can attempt to recover their domains. The UDRP process is the fastest and most cost-efficient manner in which to recover such domains. In order to prevail, a complainant must demonstrate (i) that the domain name is identical or confusingly similar to a trademark in which the complainant has rights; (ii) that the registrant has no rights or legitimate interest in the domain; and (iii) that the domain name was registered and used in bad faith. In most cases, if the cybersquatter does not mount a defense, it will only take about a month-and-a-half to receive a decision after filing a complaint. And the vast majority of UDRP decisions are reached in favor of the complainant. However, there are some instances where the UDRP process may not be sufficient.

One example where the UDRP process may not suffice is when a UDRP decision has been challenged by the registrant. According to ICANN Rules, a UDRP decision will be stayed if the losing party initiates an action challenging the decision in a court of competent jurisdiction within ten days after the decision is reached. This can be especially burdensome for the complainant when the registrant initiates a court proceeding in another country. In this situation, the complainant may elect to bring an *in rem* proceeding in a U.S. Federal Court in the district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located.⁷ This option is only available, however, if the Court lacks personal jurisdiction over the registrant.

In addition to allowing for jurisdiction over a domain name that was registered by someone outside the United States, another benefit of the *in rem* approach is that a foreign cybersquatter may choose not to appear in a court in the United States. If this is the case, it should be relatively easy to obtain a default judgment within a short time period. It is also helpful to know that the Eastern District of Virginia may consider an *in rem* action even if the registrant has already initiated an action concerning the domain in a foreign country.⁸

One drawback to the *in rem* approach is that it does not allow for the recovery of damages. A traditional claim under the ACPA on the other hand allows for damages as high as \$100,000 per infringing domain. For instance, Verizon recently obtained a judgment against a cybersquatter in the amount of \$33 million (\$50,000 per domain).⁹ While it may be unlikely that Verizon will ever actually collect the money, the judgment may at least have a deterrent effect on other cybersquatters. In light of the above, it is clear that victims of cybersquatting must be cognizant of the available options and be able to balance various factors before deciding an appropriate response.

1. See <http://www.bobparsons.me/WhyyoucantgetthedomainnameyouwantGoDaddyrescuesRegisterflycustomers.html>.

2. See *Verizon California, Inc. v. Navigation Catalyst Systems, Inc.*, 2008 WL 2651163 (C.D. Cal. June 30, 2008).
3. See <http://www.icann.org/en/committees/security/sac022.pdf>
4. See Robin Wauters, "GoDaddy Uses Standard Tactics To Warehouse Domains," *Wash. Post*, Dec. 3, 2008, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/04/AR2008120400170.html>
5. See "Go Daddy To Shut Down Standard Tactics, LLC," available at <http://domainnamewire.com/2008/12/17/go-daddy-to-shut-down-standard-tactics-llc/>
6. See <http://www.intralinks.com/solutions/ma/information-leaks/information-leaks.pdf>
7. This will often be the U.S. Federal District Court for the Eastern District of Virginia, which possesses jurisdiction under the ACPA by virtue of the fact that the registry of all ".com" domain names, VeriSign, is located within its district.
8. See *NBC Universal, Inc. v. NBCUNIVERSAL.COM*, 378 F.Supp.2d 715 (E.D. Va. 2005).
9. See *Verizon California Inc. v. OnlineNIC Inc.*, 2008 WL 5352022 (N.D. Cal. Dec. 19, 2008).