NETWORKWORLD

Understanding the legal options used to fight cybersquatting

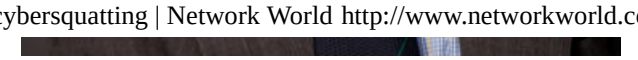
Cybersquatters jeopardize your exclusive trademark rights, and there are multiple ways to fight back.

By Gerald M. Levine, Esq.

Network World | Jan 14, 2015 8:49 AM PT

Compressed in as little as a word or two, or perhaps an expressive phrase, trademarks communicate powerful stories about who businesses are and what they stand for. They are at once guardians of reputations, ambassadors of goodwill and advocates of consumption. They have two principal functions: distinguishing one business from another and signifying sources of goods or services. Trademarks are accordingly highly prized, and not only by their owners. They are targeted by predators in both the physical and cyber marketplaces. Thus, the need for owners' constant vigilance to police their marks and protect their integrity. This cannot be done without having an informed understanding of venues and remedies for infringement.

There is, however, a distinction between trademark infringement, which is defined as the unlawful use of a business's mark that is likely to cause confusion as to the source of goods or services, and cybersquatting, which is defined as a violation of a business's right to exclusive use of its mark on the Internet. In combatting cybersquatting businesses have a choice of legal regimes, which we will focus on here.



Gerald M. Levine, Esq.

Until 1999 there was no quick or efficient remedy for removing infringing domain names from the Internet. In October of that year, the Internet Corporation for Assigned Names and Numbers, familiarly known by its acronym ICANN, implemented the Uniform Domain Name Dispute Resolution Policy (UDRP), which is an online, paper only arbitral forum for adhudicating claims of cybersquatting. In the same year, Congress passed and President Clinton signed into law a statutory regime to combat cybersquatting known as the Anticybersquatting Consumer Protection Act, or the ACPA. While the law is nested in the Trademark Act of 1946, commonly known as the Lanham Act, proof of cybersquatting is less demanding than proof of trademark infringement.

Expansion of the Domain Name Space

Based on the last Verisign Domain Industry Report, there are 280 Million registered domain names as of June 30th, 2014. On March 17, 2014 the World Intellectual Property Organization issued an assessment of the "unprecedented expansion of the Internet domain name space." This refers to the close to two thousand new domain name suffixes approved by the ICANN in 2013 that have steadily been entering the market in 2014 and will continue into 2015 and possibly beyond that.

The expansion, WIPO says, "is likely to disrupt existing strategies for trademark protection on the web." The new suffixes are mainly dictionary words like dot club, dot guru, dot photography and so on, and geographical locations such as dot NYC, dot London and numerous other city dots in the U.S., Canada, Europe, Australia, Russia, Africa and other countries and regions throughout the world.

WIPO's concern appears to have been prescient. A recent blog by a security officer at a Washington, D.C. law firm announced apocalyptically that, "The parade of horrors that we had envisioned are now starting to come to fruition…. Instead of allowing ICANN to continue to allow these registrations through, it is time for us to be reflective, especially given the security concerns we are having currently."

Judging by the number of reported cases there has been a significant increase in "cybersquatting" involving

the new TLDs.

In anticipation of the launching of the new TLDs, ICANN created the Trademark Clearinghouse (TMCH) which provides protective and defensive services to trademark owners for the so-called Sunrise periods and beyond, and implemented a new procedure, the Uniform Rapid Suspension System (URS), to combat cybersquatting using the new TLDs.

Legal Mechanism for Combatting Cybersquatting

The Lanham Act is the primary law on trademark infringement in both the physical and the cyber marketplaces. Although the UDRP is the overwhelming choice of regime for cybersquatting—in the 15 years of operation, Panels have handed down more than 45,000 decisions covering a multiple of domain names, the great majority of which favored trademark owners -- there may be reasons for preferring a civil action, reasons that lie in the differences between the two regimes.

While the ACPA and UDRP (and now the URS) have similar missions, they are differently constructed. The ACPA is an “either/or” model, which means that liability rests on proof that an alleged infringer *either* registered *or* is using the domain name in bad faith. The UDRP is an “and” model, which means that liability rests on proof that the alleged infringer registered *and* is using the domain name in bad faith.

There is one other distinguishing feature that is particularly important and rarely highlighted, which is that the ACPA is a symmetrical and the UDRP an asymmetrical regime. With the ACPA, the prevailing party is entitled to injunctive relief, damages and attorney’s fees. For trademark owners this could be a primary incentive for a civil action, although it is also a double edged sword because, if the trademark owner overreaches its statutory rights, it will pay a heavy price in the form of attorneys fees and damages.

With the UDRP each party bears its own costs and legal fees which are modest relative to a federal action. The asymmetry lies in the fact that only the complainant/trademark owner has an affirmative remedy, which is either cancellation or transfer of the domain name to its own name.

For the domain name holder, the best it can get is a clean bill finding it either has a right or legitimate interest in the domain name, in which case it wins outright; or, if it lacks a right or legitimate interest the trademark owner fails to prove abusive registration. If the trademark owner has overreached by attempting a reverse domain name hijacking the Panel is authorized to issue a declaration to that effect, but the sanction is without economic penalty.

The compensatory reasons for a trademark owner choosing the UDRP lie in the efficiency of its procedures and the quickness in resolving disputes. Reasoned decisions are generally delivered within 45 days of filing a complaint. Also, in the 15 years of its existence, the UDRP has developed an impressive jurisprudence that is partly based on trademark law, but which has essentially developed in much the same way as the common law, namely through successive decisions.

This makes for a fairly predicable outcome in most cases. There is no appellate procedure under the UDRP, but if either party is unhappy with the UDRP decision it may commence a *de novo* civil action under the ACPA.

Arbitrating Under The UDRP

The UDRP has a simple three part structure. For standing to maintain an administrative proceeding the

complainant has to prove two elements: the domain name is either identical or confusingly similar to the trademark; and complainant has to have a trademark right.

Applicants for trademark rights are ineligible. Other parties who may be aggrieved by a domain name registration but have no trademark rights (an individual personal name for example), have no standing to complain. If complainant has standing it must then prove that respondent lacks any right or legitimate interest in the domain name in issue.

Finally, the complainant has to prove that the respondent has registered *and* is using the domain name in bad faith.

The common denominator of bad faith is targeting a complainant's trademark with the intent of profiting from it. Bad faith is defined by the respondent's acts in either registering or using the domain name.

There are four nonexclusive circumstances that, in practice, cover a good bit of the the universe of possibilities. Bad faith is found on proof of 1) extortion, 2) expropriation, 3) competitor foul play, and 4) impersonation. The first three are distinguished by focusing on registration. The fourth targets mark owners through their use of the domain name.

In counterpoint to the acts of bad faith there are three circumstances in defense of the registration of the domain name, which are are also nonexclusive. Forfeiture is not warranted where the domain name holder is 1) making a *bona fide* offering of goods or services *before any notice of a dispute*; 2) commonly known by the domain name, and 3) using the domain name for noncommercial or fair use.

The concern about cybersquatting is particularly important to owners whose trademarks are on the weak end of the spectrum of protection. This is so because the evidentiary demands for shutting down monetized websites or inactive domain names are quite substantial.

Owners of strong trademarks are more likely to prevail on their claims because they have secure reputations in the physical marketplace but with the expansion of TLDs they will have to be particularly vigilant because of the increased opportunities for predation. This includes, on the horizon for launching in 2015, a "dot sucks" that is likely to prove particularly troublesome to trademark owners across the board and will bring into play a tension inherent in a defense of fair use.

Levine is an attorney practicing in New York City. He is the author of the forthcoming, definitive guide and go-to handbook, ***Domain Name Arbitration: Asserting and Defending Claims of Cybersquatting Under the Uniform Domain Name Dispute Resolution Policy****. He has a litigation and counseling practice and represents clients on a diverse range of legal and business matters from real property and commercial disputes to protection of intellectual property rights. He is on the panel of neutral arbitrators for the American Arbitration Association and a mediator for the Commercial Division of the New York Supreme Court, New York County; and the United States District Court for the Southern District of New York. He has published numerous articles on real estate, arbitration, trademark and cybersquatting. Reach him at gmlevine@researchtheworld.com.*

From CSO: 7 security mistakes people make with their mobile device