

A Domain to Call Their Own

by Alan N. Harris

This article originally appeared in the July 2001 edition of The Michigan Bar Journal. The status of other TLDs is an ongoing process. For the most current information, please see www.icann.org and therein.

Despite the technological development and explosive growth of the Internet since the advent of the Web, one critical limitation remains – only one individual/company can register and use any particular domain name. As a result, identifying the trademarks and trade names that are or may be the lifeblood of a client's business is an essential piece of the available steps to secure desired domain names and to reclaim misappropriated domain names – an essential piece of the intellectual property puzzle.

The explosive growth and mass appeal of the Internet has been fueled in large part by the introduction of domain names, easily recognizable alpha-numeric strings that correspond to unique numeric Internet Protocol addresses assigned to an individual computer. For example, the State Bar of Michigan's domain name, www.miichiganbar.org, corresponds to a unique numerical sequence that identifies the computer server hosting the website. ".org" is the top level domain. "miichiganbar" is the second level domain. Additional levels under a second level domain name allow a domain name owner to further expand the address hierarchy among individuals or sub-organizations. For example, www.harris.miichiganbar.org, would be a third-level domain name associated with the author of this article. Unfortunately, the fundamental appeal of domain names also is their Achilles' heel: their inability to assign the identical domain name to multiple users. This critical limitation has led to the intersection of Internet law and classic trademark principles with, at times, challenging results.

At its essence, trademark law protects a word, symbol, or slogan used by a person or entity in connection with specific services or goods. Through actual use of a mark, whether it be a servicemark or a trademark, and federal registration, one can acquire nationwide exclusivity of use of the mark in connection with the goods and services for which it is used. (Under the Lanham Act, 15 USC 1051, et seq., nationwide exclusivity can be acquired without actual nationwide use. In contrast, in the absence of a federal trademark registration, the scope of common law trademark rights is tied directly to the geographic area of use and extent of use of the mark. (Michigan trademark registration alone only provides exclusivity of use within Michigan.) Because trademark rights do not equate to ownership of a word, different entities can use and have rights in the same exact mark provided the goods and/or services are sufficiently dissimilar and there is no likelihood of confusion between the two uses.

This dichotomy has led to the enactment of new laws to try to alleviate egregious domain name cybersquatting, and to the development and planned implementation of additional top level domains to allow businesses with similar marks to stake out their respective territory on the Internet.

Current and Future Domains

Today, as the Internet community considers and begins implementing new top level domains, the availability of domain names, and continues to see an expansion in the availability of alternative domains, the most common question "what domain name should my company register?" can cause the most sophisticated marketing departments to struggle.

There is no question that the .com top level domain remains the most sought after, universally recognized domain.

it also is far and away the most used and, as a result, the least available. This has led, during the past few years, to a number of developments designed to broaden the availability of top level domains. Perhaps the most creative of these is the recent partnering between certain countries and entrepreneurs to market country code top level domain alternatives

to the available top level domains. As a result, domain names can now be registered under the country code top level domains .tv, .ws, and .md, representing Tavula, Western Samoa, and the Republic of Moldova, respectively. There are presently more than 250 country code top level domains. The regulation of country code top level domains varies from country to country. Because of this disparity, the United Nations and its World Intellectual Property Organization have called for an international set of rules to govern country code top level domains.

The Internet community also has pushed for the adoption of additional top level domains to supplement .org, and .net. In November 2000, the Internet Corporation for Assigned Names and Numbers (ICANN) announced the approval of seven new top level domains: .biz, .info, .name, .pro, .aero, .coop, and .museum, which are for unrestricted use; individuals; accountants, lawyers, and physicians; the air transport industry; cooperatives; and museums; respectively. ICANN, a non-profit corporation among others with responsibility for top level domain management, has not yet reached agreement with all of the proposed new domain name administrators. Not all of the new top level domains are not all expected to be available to the public until sometime in the second half of 2001.

The Intellectual Property Constituency, an ICANN subgroup, has proposed a reserved "sunrise" period during which trademark owners would have a first opportunity to register marks under the new domains. Other groups have made similar proposals. ICANN has not yet announced how the allocation of the new domains will be handled. Notably, the Federal Trade Commission has issued warnings cautioning the public to refrain from purchasing domain names "preregistration" for one of the new top level domains, since no entity can promise availability of the name at that point.^[1]

Most recently, ICANN requested public comment on the introduction of internationalized domain names (IDNs). The IDNs would consist of non-Roman characters, such as Chinese, Arabic, and other East Asian characters. Entities, such as VeriSign, already have begun test beds of internationalized domain names using non-Roman characters. Third parties unaffiliated with ICANN, such as New.Net, also have begun offering system level domains, which operate under the third level domains through special software patches and arrangements with specific Internet Service Providers.

Choosing Which Names and Marks to Register as Domain Names

In light of the above, the decision as to which of a company's names/marks to register as a domain name is becoming increasingly confounded. There is no easy answer. Instead, the decision must flow from a company's legal and business needs tied to the specific needs and aspirations of the company. This article focuses on domain name issues for existing trademarks, however, it is important to not equate a domain name alone with a trademark. The registration of a domain name alone does not give the registrant rights in a trademark that is the same as the domain name.

For a company with few marks, the decision is decidedly easier. Given the relative inexperience with renewing a domain name, a company with limited marks should attempt to register each of its marks, variations, in at least the .com top level domain (if available), and perhaps other depending on its current and future marketing plans, and risk aversion. A company with a famous mark or any mark that it decidedly does not want to appear as a domain name in any top level domain – permutations such as ihate[mark].com – should not register the name. Registration by others of this latter type of domain names, without other indicia, may be protected by the First Amendment. Thus, while the permutations are many, a company with these now common sites, may want to consider registering some of these variations.

For companies with a large number of marks, the decision becomes a balancing act, but similar principles generally should apply. A company with several marks may choose to widely register each of them or selectively choose the combination of marks and available top level domains to adequately protect its domain name portfolio may not require the level of administration of a trademark or patent portfolio, but should be implemented to ensure that a company's registrations are maintained.

The following steps may be a useful guide:

- Identify the company's marks (current and planned) and assess the possible business need for a corresponding domain name or other business justification for acquiring the domain name.
- Are the company's marks federally registered? If not, should they be?
- Are the marks available as domain names and, if so, under which top level domain?
- If not available as a .com domain name, are there other top level domains available that are needed? If the .com domain name is taken, by whom and under what justification?
- Are there variations, permutations, or other derivations of the mark that the company should register for business or other defensive purposes?
- Does the company have a mechanism in place for monitoring use of its marks, including its domain names?
- Has the company implemented a system for maintaining its domain name registrations?

Reclaiming a Domain Name

The Lanham Act's trademark and antidilution provisions, along with state law principles of unfair competition and other common law avenues, provide legal bases to attack cybersquatting, otherwise known as domain name hijacking. However, these laws were not designed for the rapid paced world of the Internet and did not provide the level of comfort needed to fully address the domain name issue.

As a result, today there are two principal legal vehicles to combat cybersquatting: The 1999 Anticybersquatting Consumer Protection Act, 15 USC 1125(d) and the ICANN Uniform Domain Name Dispute Resolution Policy. In the past year, the federal courts have rendered more than 700 decisions in domain name disputes. In the same period of time, there have been hundreds of decisions issued by arbitral panels under the UDRP. The procedures and available remedies vary, both the federal act and the UDRP can provide an efficient mechanism for reclaiming a valuable piece of a client's intellectual property. The decisions, particularly under the UDRP, are decidedly favored trademark owners. Nonetheless, in the absence of a showing of bad faith, WIPO panels have generally been more sympathetic to complainants. It is important to be engaging in an attempt to reverse domain name hijacking where, for example, the mark was merely descriptive and the parties were not competitors. See *Goldline International, Inc. v Gold Line*, WIPO Case No. D2000/1000.

The 1999 Anticybersquatting Consumer Protection Act^[2]

The act, which became law in November 1999, put the needed teeth into the Lanham Act to deal with the growing cybersquatting dilemma. It provides for civil liability where, without regard to the goods or services of the parties,

a person, with bad faith intent: (i) registers, (ii) traffics in, or (iii) uses a domain name that (a) is identical or confusingly similar to a *distinctive* mark at the time of registration of the domain name, or (b) is identical, confusing or a *famous* mark at the time of registration of the domain.

Personal names protected as marks under Section 1125 are specifically included in the prohibition. A later, separate enactment, Congress added 15 USC 1129, which provides individuals more specific domain names registered after November 29, 1999. This section provides for civil liability where, with person registers a domain name "that consists of the name of another living person, or a name confusingly similar thereto, *with the specific intent to profit from such name by selling the domain name for financial gain to any third party.*" (Emphasis added.) The remedies under this section include injunctive relief, forfeiture of the domain name, and costs and attorneys' fees.

The act sets forth a list of factors a court may consider in determining whether the requisite bad faith exists, including: (i) the trademark, or other intellectual property rights of the defendant; (ii) whether or not the domain name consists of the legal name of the defendant; (iii) the defendant's prior use of the domain in connection with the offering of goods or services; (iv) the defendant's bona fide noncommercial or otherwise fair use of the domain name in connection with an accessible website; (v) the defendant's intent to divert traffic from the mark owner's website; (vi) the defendant's offer to transfer, sell, or otherwise dispose of the domain name for financial gain; and (vii) the defendant's registration or acquisition of multiple domain names that are identical or confusingly similar to distinctive or famous marks of others at the time of registration. Notably, the act provides that bad faith is not found where the court finds that the defendant had reasonable grounds to believe that the use of the domain name was a fair or otherwise lawful use. The remedies under this provision include damages, injunctive relief, costs, or forfeiture, or transfer of the domain name.

To help combat the transparent nature of many cybersquatters, the act specifically provides a new in rem action against the domain name if the domain name violates the rights of an owner of a trademark or service mark protected under § 1125(a) (unfair competition) or 1125(c) (dilution) and if the court is unable to exercise jurisdiction over a person who could otherwise be a defendant. As to this last factor, the inability to find a defendant can be established through providing notice of intent to proceed through the act's in rem provision and publishing notice of the action as set by the court. Remedies under the act's in rem provisions include a court ordered forfeiture or cancellation, or transfer of the domain name and do not include monetary damages. The act's in personam and in rem provisions are mutually exclusive and cannot be pursued simultaneously.

The ICANN Domain Name Dispute Policy

The UDRP is a mechanism for resolving domain name disputes that has been adopted by all accredited domain name registrars of .com, .net, and .org top level domains, as well as some managers of country code top level domain names.

Under the UDRP, all domain name registrants who register domain names through a registrar are required to submit to a mandatory administrative proceeding if a third party alleges that the domain name is identical or confusingly similar to the complainant's trademark or servicemark; the registrant has no legitimate interests in the domain name; and the domain name was registered and is being used by the registrant in a manner that is inconsistent with the complainant's trademark or servicemark. A successful complainant must establish each of these three elements. Like the act, the UDRP sets forth a list of factors that may be indicative of bad faith.

Complaints under the UDRP are submitted to any one of four approved dispute resolution providers, each of whom is required to follow the ICANN Rules of Uniform Domain Name Dispute Resolution. A dispute resolution provider submitting a complaint requesting that the complaint be determined in accordance with the UDRP and the ICANN Rules of Uniform Domain Name Dispute Resolution is subject to the ICANN Rules of Uniform Domain Name Dispute Resolution.

identifying the complainant and the registrant, identifying the domain name and the registrar, specifying the trademark on which the complaint is based, and describing the grounds on which the complaint is based. At the request of the parties, complaints may be resolved by a single-member panel or by a three-member panel. If a respondent's request for a three-member panel, all administrative fees must be paid by the complainant. These fees vary depending on the service provider chosen, the number of domain names at issue, and the panel size. An action can be taken for as little as \$750.

Unlike court proceedings, and without a request by the panel for further statements or documents, the UDRP are resolved on the pleadings alone, without an in-person hearing or argument. A hearing is held at the panel's sole discretion, only in an exceptional matter. Like the act's in rem provisions, the sole remedy is transfer or cancellation of the disputed domain name.

Importantly, the filing of a UDRP proceeding does not prevent either the registrant or a complainant from submitting the dispute to a court of competent jurisdiction for independent resolution, and courts are not bound by UDRP decisions.

[1] See www.ftc.gov/bcp/online/pubs/alerts/domainart.htm.

[2] 15 USC 1125(d).