This article appeared in the February 2002 edition of *The Metropolitan Corporate Counsel*

Next Generation Domain Name Strategies: .com, .name, .biz, .info . . . Dot What?

By Karol A. Kepchar
Akin, Gump, Strauss, Hauer & Feld, L.L.P.

If many businesses and their legal counselors felt confident about their corporate domain name strategies at the start of 2001, they may feel less so now. Last year brought the launch of several new top-level domains (TLDs), the growth of domain name jurisprudence and the increase of users on alternate roots where generic TLDs unapproved by the Internet Corporation for Assigned Names and Numbers (ICANN) proliferate. Now is a good time for businesses and their counsel to review their domain name strategies in light of the "next generation" Internet landscape.

The Internet's Domain Name System

A basic understanding of trademarks and how the domain name system (DNS) works is essential to the formulation of a sound domain name strategy. The developers of the DNS did not intend domain names to function as trademarks to identify the source of a product or service. The DNS, which permits users to choose a unique alphanumeric designation to correspond to a site's unique IP address, was developed to facilitate navigation over the Internet. Instead of using IP addresses comprising arbitrary number strings, users could use words or combinations of words and numbers that would be memorable and thus would make navigation easier. Users can choose an arbitrary or generic term, or they can choose one of their own trademarks or their trade name as a domain name. Businesses commonly did so, and still do so.

It is only when a domain name corresponds to a designation that has been used either in cyberspace or in the real world as a mark to indicate the source of a product or service that the domain name takes on a source-identifying function. In other words, the "trademark-ness" of a trademark "rubs off" on a domain name incorporating the trademark. For example, once The Coca-Cola Company uses "coca-cola.com" as a domain name, "coca-cola.com" has immediate trademark significance. Users will reasonably assume the site originates with or is sponsored by The Coca-Cola Company. Conversely, if a bicycle business uses "wheels.com" as a domain name but does not use "Wheels.com" in the content of its site or anywhere else to identify its goods or services, the domain name "wheels.com" does not function to indicate source, and thus cannot be protected as a trademark.

The fact that the DNS allows trademarks to be used as domain names has contributed to the problems associated with trademark protection on the Internet. Because domain names must be unique, only one entity can use, for example, "regal," by itself, as a domain name under any single TLD. Yet, in the real world, there are dozens of businesses that own and have registered "Regal" as a trademark for different types of goods or services, *without any infringement of the others' trademark rights.* The DNS and associated domain name policy do not reflect this reality.

Trademark owners should also bear in mind that roots (large computer networks) in addition to the ICANN-sanctioned authoritative root to which the vast majority of Internet browsers point exist on the Internet. These roots are separate networks wherein users can use

domain names under dozens of TLDs (e.g., .shop, .xxx, .sport and .tech) that have not been approved by ICANN. These roots have existed for several years, but for most of that time they have been small "cybercommunities," primarily because a browser modification is required to reach the different root servers. Over time, however, the visibility of the alternate roots—and their importance in domain name policy-making—has increased significantly.[1]

In 2000, ICANN approved seven new TLDs for inclusion in the authoritative root. Some of these new registries, .biz, .info and .name, are accepting registration. In response to trademark owners, all of the registry agreements will contain procedures intended to protect trademark owners' rights in the new domains.[2]

Given the Domain Name Landscape, How Much Protection Is Enough?

Even the most reasonable domain name strategy will likely reach a point of diminishing returns to the trademark owner. How much protection is enough? A "next generation" domain name strategy must answer several questions.

1. Where do I secure defensive domain name registrations for my mark?

There will likely come a day when trademark owners see little added value in having to secure and maintain numerous defensive registrations in 10 or 20 TLDs, or on various computer networks, but that day has not yet arrived. The reaction among trademark owners to the launch of the new TLDs indicates that such owners still see value in defensive registrations in multiple TLDs, and, to be sure, defensive registrations can avoid or minimize conflicts. However, it is not unreasonable, as the TLDs and roots proliferate, for the average business to replace defensive registration activities with periodic monitoring to identify real conflicts.

2. How do I prioritize targets for enforcement action?

For many trademark owners, it is simply not feasible to pursue every objectionable domain name in every TLD. A reasonable way to prioritize targets is: 1) to pursue domain name usage likely to cause confusion as to the source or sponsorship of goods or services; 2) to pursue clear cases of cybersquatting in the "core" TLDs and in countries of strategic business importance; 3) to pursue domain names exactly corresponding to the company's most valued marks, active first, then inactive, in every TLD; and, finally, 4) to pursue conflicting active domain names in alternate roots and less significant TLDs and country code TLDs.

Most domain name auction sites will take down domain names for sale that correspond to a trademark, upon receipt of proof of a trademark owner's rights. In this way, multiple domain names can be removed from the site (but not canceled) in a very efficient manner. Periodic use of the "take down" processes of auction sites is a good supplement to an overall domain name strategy.

---

[1] In May, 2000, a company called New.net launched a DNS existing concurrently with the authoritative DNS. According to New.net, 94.8 million users worldwide have access to New.net domain names.

[2] Most of the new registries offer a "sunrise" period in which owners of certain registered trademarks are able to register the corresponding domain name before name registration is open to the general public. NeuLevel, the registry for .biz, offered an IP Claims Service and STOP dispute resolution procedure akin to ICANN's Uniform Dispute Resolution Procedure (UDRP), instead of "sunrise" registration.

3. Once I identify a target, what is my best theory and forum?

Legal challenges to domain names based on trademark rights fall generally into two categories: trademark infringement claims based on likelihood of purchaser confusion or dilution of a famous mark; or cybersquatting claims (i.e., bad faith use and registration of domain names). A registrant's bad faith need not be demonstrated in trademark infringement or trademark dilution claims, but it is a required element in cybersquatting cases.

A popular weapon in the trademark owner's arsenal has been ICANN's UDRP, a mandatory administrative procedure to resolve cybersquatting disputes. Since the UDRP's launch in 1999, decisions have been overwhelmingly in favor of complainants.[3] As a result, trademark owners often opt for this process even when the available evidence of a domain name registrant's bad faith is less than conclusive.

The U.S. Anti-cybersquatting Consumer Protection Act (ACPA) also remedies cybersquatting, allowing plaintiffs to sue domain names themselves as property (in rem jurisdiction) in federal court when the domain name registrant is not susceptible to U.S. jurisdiction, and offering statutory damages as an alternative to actual damages for cases brought against persons.

Choosing a forum will depend on various circumstances, for example: 1) how strong is the evidence of bad faith? 2) is emergency injunctive relief needed? 3) can the foreign registrant be sued in a U.S. court? 4) is discovery needed to support the claim? and 5) as a budgetary matter, how many cases will be brought and will they likely be contested by the registrant? The decision to pursue a cybersquatting claim in court or under the UDRP may turn on the strength of the evidence of bad faith.

Notwithstanding the significant legislative and policy developments surrounding cybersquatting over the past few years, the vast majority of domain name disputes are not instances of bad faith cybersquatting, but rather instances where the Internet brought previously disparate enterprises together on the same computer screen. For example, formerly geographically remote entities may now collide on the Internet, or entities with formerly distinct pre-Internet trade channels may now appear together on search results lists. These cases typically do not involve bad faith, and are properly the subject of trademark infringement claims or possibly dilution claims when the trademark owner's mark is famous, and not cybersquatting claims.

Conclusion

It is easy for businesses to fall into a "ready, shoot, aim" approach to domain name policy, particularly when changes to the Internet landscape come quickly and often. The changes, however, do not negate the two years of valuable historical perspective under the dispute resolution regimes that should help in the formulation of a thoughtful, cost-benefit-oriented approach to trademark protection on the Internet.

Karol A. Kepchar is a partner in the intellectual property practice group at Akin, Gump, Strauss, Hauer & Feld, L.L.P. Her practice includes litigation, counseling and transactional

[3] According to the ICANN Web site (icann.org) as of December 28, 2001, 80 percent of cases that went to decision were decided in favor of the complainant.

matters in the fields of trademarks, copyright and unfair competition, and includes issues related to the Internet. Ms. Kepchar is resident in Akin Gump’s Northern Virginia office.