December 29, 2000

American Civil Liberties Union Comments on WIPO Second Domain Name Process

Commentators' note: The responses that come under the "Tradenames" section of the questionnaire are meant to apply with equal force to the other segments regarding personal names, geographical indications and so forth.

Tradenames

24. Interested parties are invited to comment on whether any protection against abusive registration as a domain name in the gTLDs should be accorded to tradenames and, if so, in what circumstances and how.

A "tradename" is a name adopted, whether registered or not, by a business enterprise to distinguish itself, as a commercial entity, from other enterprises. Unlike trademarks and service marks, tradenames operate to distinguish a business on the basis of its character, independently of the goods or services that the business offers. Tradenames receive protection under the Paris Convention (Article 8), without the obligation of a filing or registration. In formulating their comments, interested parties may wish to consider the following illustrative list of issues:

1. Should tradenames be protected against bad faith, abusive, misleading or unfair registration and use in the DNS?

The use of otherwise trademarked names should be allowed unless (a) the use being contested is commercial in nature and (b) the trademark holder can show there is a reasonable likelihood of confusion. Trademark rules should not be used as a pretext to stifle criticism, parody or legitimate competition.

2. How do you define which tradenames would be eligible for any such protection?

Trademarks have already been extensively defined. For example:

"A trademark is a word, name, symbol, device, or other designation, or a combination of such designations, that is distinctive of a person's goods or services and that is used in a manner that identifies those goods or services and distinguishes them from the goods or services of others. A service mark is a trademark that is used in connection with services." (See Restatement (Third) of Unfair Competition § 9 (1995).)

There is, as yet, no apparent need for WIPO to change these definitions, whether for DNS purposes or otherwise.

3. Provide information on the types and extent of any problems or abuses within the DNS related to tradenames.

There is significant evidence that current domain name policies are being used in an abusive manner to silence free speech. A large portion of these activities have occurred in the United States, where a disproportionately large number of intellectual property holders (ranging from high-technology firms to entertainment conglomerates) are based and where a plurality of computer users still reside. American telecommunications giant Verizon, for example, paid nearly US $50 000 to register domain names like "VerizonSucks.com" in an apparent attempt to silence its critics. When one of Verizon's detractors tried to register "VerizonReallySucks.com," the company threatened an intellectual property lawsuit, even though there did not seem to be any likelihood of confusion. Other companies (such as major retailer Walmart) have also taken advantage of the current legal climate to freeze out or shut down protest websites (e.g. walmartcanadasucks.com).

There is increasing statistical evidence that WIPO-related procedures have created a bias towards large intellectual property holders. One such study indicated that this partly due to varying interpretations of domain-name dispute guidelines and clauses that allow trademark owners to pick and choose forums that lean towards their points of view. See Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy* (Nov. 2000) at http://dcc.syr.edu/report.htm

On the other hand, it is unclear whether the purported problems of DNS abuse (in the realm of so-called cybersquatting against large trademark holders) are truly serious enough to justify further regulation in this area. This much was shown in various hearings on the issue held in several countries, including one that was held before the United States Congress, where there was little hard statistical evidence to show that DNS abuse posed a significant problem. Indeed, one witness tacitly admitted to this problem, but nevertheless claimed that "[a]lthough 50 lawsuits out of 5,000,000 domain names is approximately one one-thousandth of one percent, it all depends upon one's frame of reference." See *Internet Domain Names and Intellectual Property Rights: Hearings Before the Subcomm. on Courts & Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (1999) (statement of Michael A. Daniels).

4. How do you define bad faith, abusive, misleading or unfair registration and use in respect of tradenames?

See answer to question #1 above. In these cases, a court should focus on whether there is a true likelihood of confusion. The court should consider a number of factors, including the strength of plaintiff's mark, the degree of similarity between plaintiff's and defendant's marks, the proximity of the products or services, evidence of actual confusion and so forth.

Note that the likelihood of confusion may be lessened or even eliminated in many cases by use of different Top-Level Domains (e.g. McDonalds.com versus McDonalds.farm).

In addition, traditional intellectual property based defenses and bars should be recognized (such as genericism, abandonment, parody and so forth).

5. What provision, if any, should be made for dispute resolution with respect to disputes concerning tradenames registered as domain names?

National courts should decide this issue. The current rules have encouraged forum shopping, where trademark holders pick arbitration arenas that they feel are most inclined to rule in their favor. This apparent bias has been documented and statistically analyzed; see the *Rough Justice* study mentioned earlier. While question of which National Court should control raises difficult question of venue and jurisdiction, in most cases we would favor a rule that gave precedence to the law and courts of the nation of the party alleged to have infringed on a trademark. Citizens should be able to avail themselves of the rights accorded under their own national laws.

6. If a dispute resolution procedure were implemented, who should have standing to challenge the registration of a trade name as a domain name?

The holder of the trademark in question should have standing to challenge the registration of that mark as a domain name.

7. Should any suggested measures of protection for tradenames be considered only in relation to the nature and type of domain name space established by a particular gTLD in question?

Yes, there should be domains, which are established for a specific purpose and where presence in the domain will convey relevant information about the name. For example, "fiatworkers.union would clearly signify that the domain belongs to Fiat employees, rather than the company.

8. Consider whether and how any new measures of protection for tradenames might affect the interests of existing domain name registrants.

See answer to question #7 above.

9. Would directory, listing or similar other services aimed at avoiding domain name conflicts concerning tradenames be useful, and, if so, please describe such services?

No. Such services may not only invade the privacy of ordinary Internet users, but may chill free speech. See below.

10. Consider what would be optimal policy from the perspective of the development of the Internet as a medium for communication and electronic commerce.

The Internet should developed as a medium for all people, not optimized solely for the benefit of commercial or large intellectual property interests.

Technical Solutions for Domain Name Collision Control

25. Interested parties are invited to present information on the development and availability of any technical solutions to reduce the tension between rightholders and domain name registrants, and to comment on whether such technical solutions may offer realistic options for the DNS. In the first WIPO Process, comments were sought, in the context of the prevention of domain names disputes, on the following aspects:

"The requirements of any domain name databases (including the type of information to be stored therein) that may be developed to allow domain name applicants, holders of intellectual property rights, and other interested parties to search for and obtain information for purposes of evaluating and protecting any potentially related intellectual property rights. These requirements may include, in particular, the need to make the information accessible through a common interface and to interlink databases that may be maintained by various registries and/or registrars in order to permit single comprehensive searches.

The possible use of directory and listing services, gateway pages or other methods aimed at avoiding trademark and domain name conflicts by allowing identical names to co-exist, thus overcoming the technical requirement that each domain name be unique."

In the intervening period, new technical solutions may have developed that could serve to reduce the tension and prevent conflicts between competing interests in each unique domain name, principally where the competition is between persons or entities with good faith interests in the name.

In formulating their comments, interested parties may wish to consider, in particular, whether technical means are available for enhancing the DNS WHOIS look-up services (which provide contact data for domain name registrants), including the availability of a searchable database that would operate on a variety of platforms and be compatible with all relevant DNS registration authorities.

At this point, WIPO should not support the expansion of Whois database functionality nor efforts to standardize Whois database operations. These services constitute a serious threat to the privacy of ordinary Internet users. The collection and free dissemination of personal data may become a boon to stalkers, fraud artists and other types of criminals. Some of this illicit behavior is already happening through current whois systems, and should give WIPO pause.

Moreover, the expansion of Whois databases may also chill free speech. This is particularly true in the realm of anonymous speakers, such as pro-democracy activists, whistleblowers, and other dissident groups. By destroying anonymity, these large databases may deter expression online, as potential voices may stay silent for fear of being hunted down via DNS Whois information.

Already Whois database information is being used for purposes other than those for which it was originally created. In New Zealand, government agents have already acquired personal information from the country's Internet registry, in order "to ascertain …activities that carried on mainly in the business area for Internet trading," according to one spokesperson. A number of observers, including Peter Dengate-Thrush (chairman of the Internet Society of New Zealand), worry that "there are no rules for this. And it comes at the same time as we are concerned about e-mail surveillance, and the development of techniques by authorities to monitor traffic and do all sorts of things." (See Kim Griggs, "Kiwi Tax Unit Grabs Domain Info," Wired News, Dec. 1, 2000.)

Similarly, corporations have started using Whois data for telemarketing purposes. In a recent case, a judge in the United States granted a preliminary injunction against Verio Inc., preventing the company from using domain name registrant information to compile massive consumer lists and bombard those people with advertisements via phone calls, email messages and regular mail. (See Joanna Glasner, "Judge Blocks Whois Spam," Wired News, Dec. 11, 2000.)

For these public policy reasons, WIPO should not support attempts to create massive standardized Whois databases at this time.

Submitted by Barry Steinhardt
Associate Director
American Civil Liberties Union
125 Broad Street
New York, NY 10004
USA
Barrys@aclu.org