Domain Name Disputes: Technology Outpaces the Legal System

Sam Ramanujan, University of Central Missouri, ramanujan@ucmo.edu
Someswar Kesh, University of Central Missouri, kesh@ucmo.edu
Steve Ewens, University of Central Missouri, sge2000@att.net

ABSTRACT

The history of the human race is replete with instances in which the implementation of a new technology renders obsolete one or more facets of a society, such as human beliefs, the infrastructure of an industry, or the method of organization of labor. One such case is the rapid growth of the Internet and the World Wide Web (the Web), and the resulting inadequacy of legal systems to provide needed structures for the new realities. In particular, this paper deals with the legal inadequacy dealing with domain name disputes (DNDs). This paper discusses the evolution of the legal framework to address DNDs and based on the analysis of this evolution it provides recommendations to form strategies for preventing, detecting and pursuing cyber-squatters in order to prevent DNDs.

Keywords: Domain Name Dispute, Legal issues in Information Technology (IT), Internet Protocol

INTRODUCTION

The history of the human race is replete with instances in which the implementation of a new technology renders obsolete one or more facets of a society, such as human beliefs, the infrastructure of an industry, or the method of organization of labor. One such case is the rapid growth of the Internet and the World Wide Web (the Web), and the resulting inadequacy of legal systems to provide needed structures for the new realities. A prime example of this inadequacy has to do with domain name disputes (DNDs). Domain names are vital to the efficiency and orderly operation of the Internet and the Web. When two or more individuals or entities compete for the use of the same domain name, the result is a DND. DNDs arose in the first place because of technology outpacing the legal system, particularly trademark law.

The trading of domain names has become a viable business by itself and has a significant impact on eCommerce. In 2007, the domain name "Business.com" was sold for US$345 million by eCompanies who originally paid US$7.5 million for this domain name in 1999 from a seller who bought this domain name for US$150,000. This sale along with the high priced sale of other popular domains such as diamond.com, casino.com highlights the strength of domain name business. Such a growth of domain name business has led to the emergence of cyber squatters and DNDs. Cyber squatters generally either offer to sell the name back to the trademark owner for an exorbitant price, or make money from Internet traffic accidentally landing on their page due to mistyping the URL. In 2006, MarkMonitor found more than 286,000 instances of cyber squatting for the 25 brands it studied [5].

The impact of DNDs is highlighted by the fact that in 2007 alone Microsoft recovered 1100 domain names from cyber squatters. In addition, the World Intellectual Property Organization reports a 25 per cent rise last year in the number of disputes it handled over Internet domain names [9]. Such growth of DNDs in the past few years along with the significant financial impact it has on eCommerce motivates us to examine this issue in greater detail. Both practitioners and researchers will find such a study useful since it will provide a basis for finding ways to prevent or at least reduce DNDs in future.

This study first provides background information on the evolution of domain names and domain name disputes (DND). This is followed by a section that highlights the legal framework for resolution of DNDs in early and mid 90's. Next, we discuss the first attempt by congress to create laws to resolve DNDs namely Federal Trademark Dilution Act of 1995. This is followed a discussion of the extension of the 1995 legal framework for this domain in the form of Anti-Cyber squatting Consumer Protection Act of 1999 (ACPA). An international framework for resolving DNDs, Uniform Domain Name Dispute Resolution Policy (UDRP), and its disadvantages are highlighted in next two sections. Finally, in the concluding remarks section we discuss strategies for preventing, detecting and pursuing cyber squatters.

BACKGROUND AND DISCUSSION

In the mid-1980s, the use of domain names began. Before domain names, the location of a computer on the Internet were specified solely using an Internet

Protocol (IP) address. An IP address is a long numerical string, such as "98.37.241.20" [1]. Such a designation is unwieldy, and is not mnemonic in nature. A domain name, which can contain alphabetic characters, is easier to remember and can be recognizable as related to a trademark, company, organization or other entity. Both IP addresses and domain names must be unique, as both identify a specific computer on the Internet [1].

In 1992, as commercial entities began to appear on the Internet, they competed for domain names under the generic top-level domains (gTLDs) <.com>, <.net>, and <.org>. This became a problem quickly, given that each unique domain name can have only one owner. Under trademark law, which of course existed before the Internet, companies in different industries sometimes had similar trademarks [1]. Each company wanted a domain name that closely resembled its trademark; for example, a number of companies might want to own the domain name "United.com".

In addition to competition among trademark owners for domain names, entities that did not own trademarks sought to acquire domain names for a variety of reasons. Some, who saw the commercial potential of the Internet more quickly than did many trademark owners, were engaging in "cyber speculation" by registering domain names in which they had no trademark rights, in order to sell the domain names at a profit. Others registered domain names in order to receive revenues for misdirecting Internet users to sites which would pay for the traffic. Some individuals and organizations registered domain names for private, non-commercial purposes. Others acquired domain names identical or similar to trademarks in order to publicly express negative opinions about the trademark holder (For example, microsoftsucks.com is a website that is critical of Microsoft). In many cases, these activities were not a violation of existing law [1].

Society quickly developed colorful terms to describe these activities and their practitioners. Two terms are based upon the centuries-old concept of a "squatter", defined as "one that settles on property without right or title or payment of rent" [6]. The first term is "cybersquatting", which a report of the United States Senate years later described as "the deliberate, bad-faith, and abusive registration of domain names in violation of the rights of trade mark owners" [11]. Another descriptive term is "typosquatting", which refers to a type of cybersquatting using a misspelling of the trademark which the cybersquatter hopes will be a common mistake [2]. For instance, one might use "Microsof.com" hoping to attract Internet users who are actually looking for "Microsoft.com".
The third term is "cybergriper"; this is someone who uses a domain name to disparage the trademark owner. A cybergriper is often a dissatisfied former customer of the trademark owner [12].

Some of the effects of cybersquatting and related activities upon the holders of trademarks included (Robinson, 2003):

- Being denied the opportunity to benefit from using the trademark as the domain name.
- Having to choose between purchasing a domain name at an inflated price or being unable to use it.
- Suffering the diversion of Internet traffic, often to sites selling products or services offered by competitors.
- Having the trademark used in connection with parody, protest, and hate sites.

DND Status in the Early and Mid-1990s

The evolution of the Internet outpaced the United States legal system in the early and mid-1990s in two distinct ways. First, the legal system had no statutes that were adequate to settle DNDs. The most relevant law was the Lanham Act, relating to trademark infringement. Up to 1995, almost all DND lawsuits were brought under the Lanham Act. This was not very effective, for several reasons. Trademark law did not give trademark holders unlimited rights to every use of a trademark. Many DND cases did not clearly involve trademark infringement, and the defendant often did not engage in the sale of a product or service similar to that of the plaintiff. In fact, often the defendant was not using the domain name in any commercial activity. These issues made difficult a finding that use of the disputed domain name would cause confusion regarding the trademark or dilute its value [1].

In addition to the lack of clarity regarding the relationships between trademarks and domain names, the legal system was not prepared to deal with DND issues because of geography. Internet activity, of course, is not specific to a particular state, nor even to one country. Legal systems are based upon political subdivisions (city, county or parish, state, and federal, in the United States). How can geography-specific laws regulate geography-independent activity?

This is illustrated by the case of Joe Toeppen, a cybersquatter who became notorious early. In the mid-1990s Toeppen registered hundreds of generic words and trademarks as domain names. (For example, he registered "water.com" and "eddiebauer.com".) Some of his victims sued in federal district court in California, a state of which Toeppen was not a resident. Before deciding the DND issues, the court had to decide if he was subject to jurisdiction in California. The court decided that the Internet activities of Toeppen were enough to establish jurisdiction [3].

John Zuccarini was a well-known typosquatter of the 1990s. He reportedly owned more than 3,000 domain names and earned up to $1 million per year. Eventually he was successfully sued and ordered to pay hundreds of thousands of dollars in damages. He was sentenced to prison for misdirecting children in search of Disney sites to pornography websites [10].

The attitude and methods of a typical cybersquatter can be seen in this quotation from a website operated by a cyber squatter [10]:

> "It is very simple. Purchase ONLY dot.com domains. Purchase them via an offshore trust. Thus legally avoiding any tax liability, and also preventing any damages being awarded to anyone who may feel that they have a right to ownership. It would cost anyone at least $3,000 to legally obtain a domain name from another, and without any possibility of damages or costs, most entities would pay up to $5,000 without a blink of an eye (or lawyer)."

The Federal Trademark Dilution Act of 1995

The Federal Trademark Dilution Act of 1995 (FTDA) was an initial attempt of the Congress of the United States to adapt the legal structure to the Internet age. The intent was to provide a basis for legal action that was more suitable for cybersquatting cases than were the criteria for trademark infringement cases.

Under the FTDA, a trademark holder could bring a lawsuit against an alleged cybersquatter for lessening the capacity of the trademark to distinguish the goods or services that were marketed under the trademark. It was no longer necessary to prove that the action of the defendant produced confusion or that the defendant was engaging in commercial competition with the plaintiff.

As the FTDA became the basis for lawsuits and courts began interpreting its meaning, results varied. Often courts ruled that cyber speculation was a commercial use. Courts also sometimes accepted the argument that the inability of a trademark holder to use the trademark as a domain name diluted the value of the trademark and limited its ability to distinguish the goods or services of the trademark holder on the Internet. Lawsuits under the FTDA were still risky for the plaintiff, though, as some defendants were able to convince the courts that their actions did not violate any laws [1].

The Anti-Cybersquatting Consumer Protection Act of 1999

The Anti-Cybersquatting Consumer Protection Act of 1999 (ACPA) was a continuation of the efforts of the Congress of the United States to provide trademark holders with remedies for cybersquatting. The ACPA was incorporated into the existing Lanham Act, which governs unfair competition and trademark law. Although the ACPA improved the ability of the Lanham Act to regulate DNDs, bringing suit under the ACPA was often expensive and slow. The ACPA was inadequate in dealing with geographic issues, as it was still difficult or impossible in many cases to sue foreign defendants [3].

The intent of Congress was to exclude legitimate criticism and parody from the sanctions of the ACPA [12]. This intent was not always successful; in some cases the decisions of courts were overzealous in punishing the actions of cybergripers whose actions should not have been actionable under ACPA [12]. Court decisions in ACPA cases in 2004 mitigated this overzealousness somewhat by providing a safe harbor for genuine criticism sites. In order to maintain this security, criticism sites should avoid several activities: linking to sites that offer goods or services for sale or otherwise promote economic activity; making offers to sell the domain name or to settle the lawsuit; posting offensive content; registering multiple sites that provoke DNDs; and giving incomplete and/or misleading information while registering the domain name [12].

Under the ACPA, the plaintiff must prove three elements in order to prevail. First, the domain name registered by the defendant must be identical or confusingly similar to the trademark of the plaintiff. Second, the defendant must be shown to have no legitimate interest in the domain name. Third, the defendant must have registered or used the domain name in bad faith [3].

The third element, bad faith, is perhaps the most ambiguous of the three elements, and probably the most difficult to prove. Courts use nine factors to evaluate the bad-faith element [12]:

- The presence or absence of trademark rights or other intellectual property rights of the defendant in the domain name
- The relationship of the name of the defendant to the domain name
- Any prior use of the domain name by the defendant in selling goods or services
- Whether the use of the domain name by the defendant constitutes non-commercial or fair use
- Evidence of intent of the defendant to divert customers of the owner of the trademark
- Offers by the defendant to sell the domain name
- Use of a false name or other misleading information by the defendant while registering the domain name
- Any history of cybersquatting by the defendant
- The degree to which the trademark is distinctive and famous

The Uniform Domain Name Dispute Resolution Policy

The Internet Corporation for Assigned Names and Numbers (ICANN), an organization affiliated with the United Nations, implemented the Uniform Domain Name Dispute Resolution Policy (UDRP) in October 1999 [1]. The UDRP became effective on December 1, 1999. It is neither a law nor a treaty. The UDRP derives its force from domain name registration agreements between domain name registrants and domain name registrar organizations. These registration agreements contain a provision mandating that DNDs will be subject to arbitration [10].

As the UDRP is not a law or treaty, it is able to somewhat effectively address one factor in the failure of previous attempts to regulate DNDs, that of geography. Because the UDRP does not gain its force from the legal code of one particular nation, it can be applied by a complainant in one country against a respondent in another country [10]. However, the UDRP does not completely eliminate the issue of geography. Disputes are resolved using the laws of the country specified in the registration contract of the disputed domain name. That country is usually the home of the registrar and the respondent; this can put the complainant at a considerable disadvantage [3].

In implementing the UDRP, ICANN had three main goals: to establish uniform worldwide rules for DND resolution; to reduce the cost of DND resolution; and to speed up the process of DND resolution [1]. The UDRP has been successful in providing an inexpensive and quick solution [3].

Under the UDRP, a DND has three possible outcomes. First, the arbitration panel can order the registrar to cancel the domain name. A second possibility is the panel directing the registrar to transfer the domain name to the complainant. The third possible outcome is to deny the complaint [3]. Unlike the possible outcome of a lawsuit, the UDRP does not allow the complainant to recover damages or attorney fees [3].

Approximately 85% of UDRP proceedings involve DNDs in the gTLD <.com> [7]. More than 80% of all cases filed are resolved in favor of the trademark owner [10]. Complainants who repeatedly file complaints and do not prevail can become known as reverse domain name hijackers [10].

Weaknesses of the Uniform Domain Name Dispute Resolution: The UDRP is the most common venue for the resolution of DNDs. However, it is not without imperfections. As under the ACPA, noncommercial free speech issues continue to be problematic. The two issues that cause the most divergence of opinion among UDRP panelists are cybergriping or “suck” sites (for example, walmartsucks.com) and fan sites [7].

Ambiguity is a considerable problem with the UDRP. It leaves somewhat ambiguous the definitions of such terms as: “identical”, “confusingly similar”, “good faith”, and “bad faith” [1]. In a context such as the legal system of the United States or most nations, ambiguity such as is found in the UDRP would be reduced over time by the establishment of precedents. Unfortunately, the UDRP procedural framework does not provide a mechanism to identify which decisions should be treated as precedents [1].

The ambiguity in the UDRP produces several counterproductive results, some of which are opposites [1]:

- In the absence of a framework to establish precedents, both under- and over-reliance on preceding UDRP decisions.
- Under-reliance on principles of law.
- Under-reliance on the UDRP itself as policy, which can produce the feeling of

possessing license to simply "do justice" in each case.

In addition to the previously-mentioned issue that DNDs under UDRP will be resolved using the laws of the country specified in the domain name registration agreement, another geographic issue can be a weakness. Article 11 of the UDRP states that the language of the administrative proceeding will be the language of the registration agreement, unless all parties to the DND agree otherwise. This can put one party (usually the complainant) at a considerable disadvantage in conducting the procedure [13].

Two other weaknesses of the UDRP have to do with the failure to apply negative incentives to undesirable behavior. First, UDRP rules permit the panel to find that a complaint was brought in order to attempt reverse domain name hijacking. Unfortunately, the only negative outcome to the complainant is loss of the dispute; no penalty is specified in the UDRP. This removes most of the risk and cost to those who abuse the UDRP process in this way [1].

A more serious weakness related to absence of negative incentives has to do with the range of possible outcomes to a respondent who loses a dispute. The UDRP does not allow for the awarding of damages or legal costs to a complainant who prevails in the dispute. Hence, the only negative outcome a cybersquatter faces under the UDRP is the possible loss of a domain name. Given the modest cost of registering domain names, a cybersquatter can lose most of his domain names in UDRP proceedings and still profit from the very few domain names he does not lose. If not for the availability of the UDRP, many more cases would go to court under the ACPA, with cybersquatters facing the potential for large adverse judgments. By offering an alternative to such litigation, the UDRP may actually be increasing the incidence of cyber squatting [1].

A review of past URDP dispute resolution [4] shows that in 70% of the cases involving trademark owners and the owners of domain names similar to the trademark, the UDRP has ordered the handover of such sites to their respective trademark owners, but a US court recently declined to do this. It argued the site, as registered, was not a commercial one and so could not be said to be infringing the trademark owner's rights. This differing viewpoint from that under the UDRP can lead to confusion

CONCLUDING REMARKS

Based on the discussion presented in this paper we can suggest ways for Preventing, Detecting, and Pursuing Cyber squatters. A number of strategies exist that will enable a trademark owner to systematically protect intellectual property rights. Registration strategies include [2]:

- Register domain names in as many gTLDs as is practical (<.com>, <.net>, etc.)
- Register the trademark name by itself (Ford.com, for example) and also register alternative domain names which combine the trademark and a description of the product or service (Fordautomobiles.com, Fordcars.com, for example).
- Register domain names with predictable typographical errors, such as Microsof.com.

Domain information management stratégies includes [11]:

- Use a domain management services provider to identify all domain names you own.
- Use the provider to conduct a comprehensive domain name audit to identify and fully document domain names that are similar to your domain name or trademark.
- Develop a policy to standardize all your domain name registration information with one company contact listed, so you do not fail to receive communications addressed to former employees who were listed as contacts.
- Consolidate all domain name information into a database managed by a provider who will maintain the database systematically.

Dispute resolution strategies include [13]:

- Use dispute resolution proceedings:
  - In cases in which the cybersquatting is clearly evident.
  - Or in cases in which no legal alternative is available.
- Prioritize potential cases:
  - Cases in which not only the domain name but also the content infringes – highest priority
  - Popular websites with high traffic volume – high priority
  - Site owners with significant assets – high priority

- Repeat offenders – fairly high priority
- Inactive websites – low priority

- In overseas cases, involve local counsel in case evaluation.
- File one combined complaint against a registrant with multiple disputed domain names.
- Check the registration expiration date:
  - If the expiration date of an inactive site is imminent, the cybersquatter may let it expire.
  - Even in the case of an active site close to the expiration date, if you file a complaint the cybersquatter may let the registration expire, leaving you with significant expenses and no case to resolve.

Complaint and response formulation strategies include [10]:

- The complaint or response should be a legal brief; this is usually your one chance to argue your position.
- The complaint or response should be brief.
- The complaint or response should be organized around the three elements of the UDRP policy.
- The complaint or response should supply proof of assertions it makes.
- The complaint or response should cite and briefly explain relevant UDRP decisions.

In addition to the abovementioned strategies suggested in literature, our analysis of DND cases leads us to suggest some additional recommendations to avoid DNDs. They include:

- Register domain names with all possible Acronyms of the company/organization. In particular, if the Acronym is more than 3 characters. For example, America Online won a dispute over the <baol.us> ***domain name*** despite the respondent's contention that it operated a business called Blackamerica Online, Inc. in America Online, Inc. v. Ragland. Most cases with acronyms of 3 or less characters have been decided in favor of the domain name or trademark holders.
- While literature suggests that organizations owning trademarks similar to the domain names have upper hand in retaining the domain names. *The organizations should also register their trademarks and domain names as keywords in major search engines.* The Lanham act does not provide any relief from someone using the trademark/domain name as a keyword since the courts do not consider this to be actionable use of trademark.
- One should also consider registering country specific TLD (e.g. .oz, .nl etc.) in addition to the gTLDs. In particular, buy the country specific TLDs in any county where you may conduct business or sell your product/services. This will allow the local laws to provide added protection for the domain name.
- Check for copyrighted Acronyms and concepts before creating trademarks and domain names for your organization. As mentioned earlier in this paper, registering acronyms, keywords and trademarks can help in preventing cyber squatting and DNDs.

In conclusion, this paper emphasized the fact that Internet community and governments have not yet fully resolved all the issues that are raised as the result of Internet technology outpacing the legal system. In fact, a consensus does not yet exist on which ones of such issues are problems requiring a solution, and which issues are already properly resolved by existing law. Such problems are not confined simply to DNDS, but also to many other emerging technologies. For example, serious privacy and security concerns are issues with RFIDs and patent disputes in Bioinformatics are far from over.

We have certainly made progress toward identifying and resolving problems related to domain name disputes. The ACPA and the UDRP create a better dispute resolution environment than previously existed. Much remains to be decided regarding both what the proper outcomes are and how to best reach them. In particular, geographic issues remain as the geography-independent Internet creates conflicts that must be resolved by so-far geography-dependent legal systems. Under such circumstances, it is best for corporations to adopt a defensive posture and seriously consider some of the recommendations made in this paper. Risk avoidance, it seems, may be the most prudent strategy.

REFERENCES

1. Armon, O. (2003). Is this as good as it gets? An appraisal of ICANN’s Uniform Domain Name Dispute Resolution Policy (UDRP) three years

after implementation. *Review of Litigation*, 22(1).

2. Ash, K. A., & Danow, B. J. (2006). Defensive ownership of domain names. *Managing Intellectual Property*, 156.
3. DuBoff, L. D., & King, C. O. (2005). Domain name dispute resolution for educators. *TechTrends: Linking Research & Practice to Improve Learning*, 49(3).
4. Dorrain, Kristine F. & Ottaviani, John E. (2007). Survey of the Law of Cyberspace: Intellectual Property Cases 2006. *Business Lawyer*, Vol. 63 Issue 1, p271-300.
5. Hesseldahl, Arik (2007). Brandjacking' on the Web. *Business Week Online*. 5/2/2007, p13.
6. *Merriam-Webster online dictionary*. (2006). Retrieved December 7, 2006, from http://www.merriamwebster.com/cgi-bin/dictionary/squatter.
7. Nurton, J. (2006). Domain name disputes on the rise. *Managing Intellectual Property*, 160.
8. Nurton, J. (2005/2006). Europe goes dotty over .eu. *Managing Intellectual Property*, 155.
9. Palmer, M. (2007). Microsoft suing to evict "cybersquatters" Financial Times, March 14, 2007.
10. Partridge, M. (2005). How to win domain name cases. *Managing Intellectual Property*, 146.
11. Robinson, J., (2003). How to prevent cybersquatters. *Managing Intellectual Property*, 127.
12. Ryan Gilfoil, J. (2005). A judicial safe harbor under the Anti-Cybersquatting Consumer Protection Act. *Berkeley Technology Law Journal; Annual Review 2005*, 20(1).
13. Seo, I. H. (2005). Taking back domain names in Korea. *Managing Intellectual Property*, 153.