Domain Name Disputes:
How to Get the Bad Guys Off Your Domain

By Karen McDaniel and Rebecca Bishop

Introduction

In times of great exploration, there always seem to be those who wish to share in the bounty through less legitimate means, such as the pirates who once roamed the open seas, simply taking whatever treasures for which others worked so diligently. While early explorers had to contend with pirates of the Captain Hook variety, today's high tech leaders are faced with interlopers of the cyberspace world who attempt to inappropriately profit from the bounty of the newest frontier – the Internet. Today's "cyberpirates" scavenge for profit by simply taking the trademark and goodwill of businesses and individuals, and registering them as domain names, either to pull potential consumers away from the legitimate sites or to attempt to sell the registrations for huge profits.

So how can a legitimate trademark or domain name owner avoid being held up for ransom?

When the Internet and the unfortunately inevitable cyberpirates – more commonly called cybersquatters – first entered the scene, the answer was unclear. Cybersquatters registered hundreds of famous trademarks as domain names and were successful in obtaining large payoffs in return for their relinquishment because traditional trademark law was not designed to prevent such actions. Panasonic, Fry's

Electronics, Hertz and Avon were among the "victims" of cybersquatters during that time. Recently, however, new remedies have been created which are specifically designed to combat cybersquatting. This paper will discuss the various remedies available and the factors one should consider in choosing which remedy to pursue.

The Anticybersquatting Consumer Protection Act

In 1999, in response to the growing problem of cybersquatting, Congress passed the Anticybersquatting Consumer Protection Act (ACPA). In short, this legislation makes it easier for trademark owners to prevent someone who has no legitimate purpose from using a domain name that is the same as, or confusingly similar to, a challenger's mark. The law applies to domain names that are identical or confusingly similar to a distinctive mark, or identical to, confusingly similar to, or dilutive of a famous mark. The law is embodied in section 43(d)(1)(A) of the Lanham Act, 15 U.S.C. §1125, and to win, a challenger must prove:

1) the registrant had a bad-faith intent to profit from the challenger's mark (see below),
2) the mark was distinctive at the time the domain name was first registered,
3) the domain name is identical or confusingly similar to the challenger's mark, and
4) the challenger's mark qualifies for protection under federal trademark laws.

It is important to note that a challenger does **not** have to prove that customers are likely to be confused by the registrant's domain name, as in a trademark infringement claim. This means a challenger can sue the domain name registrant even if the web site sells products or services that are completely unrelated to those used in connection with the mark.

Proof of Bad Faith Required

The key to the ACPA is that the "pirate" must have registered / used the mark in bad faith. When a trademark owner challenges a registrant's rights in a domain name comprised of that mark, the Act sets forth the following factors to determine whether the registrant obtained / used the name in bad faith:

1) What trademark or intellectual property rights, if any, the registrant has in the domain name.
2) Whether the domain name consists of the legal name of the registrant.
3) Whether the registrant has previously used the domain name in connection with the bona fide offering of goods or services.
4) Whether the registrant has made a bona fide non-commercial or fair use (such as parody or comparative advertising) of the mark in a site accessible under the domain name.

5) The registrant's attempts, if any, to divert consumers away from the challenger's on-line location to a site accessible under the domain name where harm to the goodwill of the mark could occur because:

   (a) the registrant has intent of commercial gain; or

   (b) the registrant intends to tarnish or disparage the mark.

6) Whether the registrant seeks to sell the domain name for financial gain and has not previously used and has no intention to use the name in connection with a bona fide offering of goods or services (or the registrant has a past pattern of seeking financial gain through selling domain names).

7) Whether the registrant provides false contact information when applying for registration of the domain name (or has a past pattern of such conduct).

8) Whether the registrant has multiple domain names and the registrant knows that they are identical to or confusingly similar to the distinctive marks of others or dilutive of the famous marks of others.

9) Whether the registrant seeks to register a distinctive or famous name.

Proving a bad faith intent (which requires evidence of the state of mind of the wrongdoer) is oftentimes quite a difficult endeavor. Many of the above factors, however, permit consideration of circumstantial evidence that might imply bad faith intent on the part of the cybersquatter (such as evidence of no prior use or evidence of a past pattern of conduct). As a result of the ability of a mark owner to rely on

circumstantial evidence, the burden of proof of wrongdoing is somewhat lessened and relief may be secured even in the absence of testimony admitting to a bad faith intent.

Remedies of the ACPA

Remedies under new Section 43(d) include an injunction and damages. Actual damages are available under 15 U.S.C. §1117, and may include the defendant's profits, the plaintiff's damages and costs. Exceptional cases may also carry the award of attorney's fees.

In addition, a special damages provision, found in 15 U.S.C. §1117(d), has been incorporated that relates specifically and solely to actions for cybersquatting under Section 43(d). This provision provides that a plaintiff may elect, at any time before final judgment is awarded by the trial court, to recover an award of statutory damages instead of actual damages or profits. These statutory damages range in the amount of not less than $1,000 and not more than $100,000 for each domain name involved, as the court deems just. Because actual damages are very difficult to prove, the vast majority of challengers under the ACPA opt for an award of statutory damages.

Other Nuances

In additional to the special statutory damages available, the ACPA allows trademark owners to bring an *in rem* action against the domain name itself. Cybersquatters often go to great lengths to hide their true identities and regularly

provide false information when registering a domain name. Therefore, the ability to bring an action against a domain name rather than the registrant (provided the challenger has exercised due diligence in attempting to contact the registrant) is especially important. The challenger in an *in rem* action, however, may only obtain a transfer or cancellation of the disputed domain name and not money damages.

The ACPA also codifies the past practice of exempting domain name Registrars from liability for the act of registering a domain name to someone other than the owner of the relevant trademark. Domain name Registrars are typically only liable under the ACPA if their actions are taken in bad faith.

Finally, the jurisdiction of the ACPA is currently in a state of flux. While courts are increasingly open to finding personal jurisdiction in ACPA suits over foreign registrants using standard purposeful availment tests for minimum contacts, court decisions range across the board. Generally, if the foreign registrant is selling goods that can be purchased by customers in the United States or displaying the advertising of United States companies, personal jurisdiction will typically be established. Alternatively, challengers may be able to file an *in rem* action against the domain name itself when personal jurisdiction may be impossible. *In rem* actions may be brought in the federal district court where the Registrar or other domain name registration authority for the disputed domain is located.

ICANN's Uniform Domain Name Dispute Resolution Policy

Until 1999, the only authorized Registrar of top-level domain names (such as .com, .net and .org) was Network Solutions, Inc. Network Solutions had developed its own dispute resolution policy for challenging another's registration as an alternative to filing a formal lawsuit, but this remedy proved to be quite limited in terms of effectiveness. Criticism of the policy was directed towards the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit corporation responsible for IP address space allocation, protocol parameter assignment, domain name system management and root server system management. In response to this criticism, ICANN adopted a Uniform Domain Name Dispute Resolution Policy (UDRP) in August of 1999 that serves as the only available administrative remedy for domains registered by any Registrar serving the top-level domain names. Since April of 1999, ICANN has accredited 157 such Registrars in addition to Network Solutions, Inc. (although a small portion of these are not yet active). Accordingly, the UDRP is quite expansive in terms of the domain name registrations subject to its terms.

The UDRP creates administrative procedures designed to provide streamlined and economical resolutions of disputes stemming from "abusive registrations." The average length of an UDRP proceeding is only 45 days and the costs are significantly less than federal litigation. For example, an action brought before the World Intellectual Property Organization Arbitration and Mediation Center (one of the four dispute resolution providers approved by ICANN) concerning between one and five domain

names costs between $1,000 and $2,500 depending on the number of panelists chosen. Additional costs include only the expense of drafting the Complaint or Response.

To give the procedures teeth, registrants **must** submit to the administrative proceeding if a challenger files a Complaint with the Registrar of the domain name. To succeed, a challenger must assert and show that a given domain name:

1) is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
2) that the domain name holder has no rights or legitimate interests in the domain name; **and**
3) that the domain name has been registered and is being used in bad faith.

The full rules governing the form and content of pleadings are contained in the Rules for Uniform Dispute Resolution Policy (found at www.icann.org), which was adopted by ICANN contemporaneously with the UDRP. The general process, however, is relatively simple. A challenger submits a Complaint, which encompasses the sum of the evidence the challenger is allowed to present. The registrant then submits a Response, which encompasses the sum of the evidence the registrant is allowed to present. This is the entirety of the pleadings. In other words, there is no discovery, additional motions, etc. before a decision is rendered. Both the Complaint and the Response are submitted electronically.

A panel, composed generally of law professors and attorneys, then decides the merits of the case. Either a one- or a three-member panel may be selected. The domain name Registrar chooses the neutral panel members from a list of ICANN-approved panelists. In the case of the election of a three-member panel, both the challenger and the registrant have input into the selection of one of the three panelists.

Similar to the ACPA, the substantive work of the panel is to determine whether the given domain name was registered and used in bad faith. In making the bad faith determination, the panel looks to the following factors:

1) Circumstances indicating that the registrant registered the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the challenger who is the owner of the trademark or service mark, or to a competitor of that challenger, for valuable consideration in excess of the documented out-of-pocket costs directly related to registering the domain name; OR
2) Registration of the domain name to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the registrant of the domain name has engaged in a pattern of conduct of that type; OR
3) Registration of the domain name primarily for the purpose of disrupting the business of a competitor; OR

4) Use of the domain name as an intentional attempt to attract, for commercial gain, Internet users to a particular web site or other on-line location, by creating a likelihood of confusion with the challenger's mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product or service on a web site or location.

In addition, the panel will consider the following factors indicating a legitimate interest in a domain name:

1) Actual use of, or preparations to use, the domain name or a name corresponding to a domain name in connection with a bona fide offering of goods and services; OR
2) Evidence that the registrant has been commonly known by the domain name (either as an individual, a business or another organization), even if the registrant of the domain name has not acquired any trademark or service mark rights in the name; OR
3) Evidence that the domain name registrant is making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

Note that the factors examined by the panel under the UDRP are very similar to those that a court is directed to consider in examining the merits of an action brought

under the ACPA. The panel decides a complaint based on (1) the statements and documents submitted, (2) ICANN's rules and (3) principles of law that it deems applicable. Although not specifically required to do so, panelists often find that the third category includes decisions issued by other domain name dispute panels in determining how to apply the Policy and the Uniform Rules. Several decisions have also cited federal district court case law in support of the decision, but this is less common.

If a three-member panel is used, a final decision need not be unanimous. Simply a majority of the panel may render the final decision and dissenting panelists may offer dissenting opinions. Since the adoption of the UPRP, dissenting opinions have not been uncommon.

Remedies of the UDRP

If the panel determines that the domain name was registered in bad faith, the panel may either cancel the domain name registration or transfer the registration to the challenger. Note that this is quite different than the ACPA, which allows for monetary damages.

Effect of UDRP Proceeding

The final decision of the panel is not appealable, but use of the administrative remedy does not preclude a party form later bringing an action in court. While neither the ACPA or the UDRP addresses what impact a decision arrived at during the

administrative proceeding might have on a subsequent case in court, the decision of the panel undoubtedly will carry weight in court, particularly since the factors indicating bad faith so closely parallel one another under both types of remedies.

Jurisdiction

As noted above, use of the UDRP must be made by all ICANN accredited Registrars of top-level domains. Of the 157 ICANN-accredited domain name Registrars, roughly half are located outside of the United States. Thus, the impact of the ICANN-mandated administrative remedy is felt worldwide.

So How Do I Choose?

Okay, so you have discovered that someone has obtained a registration for www.yourtrademarkhere.com and, after investigation, you feel confident that the registrant has obtained a registration for the domain name in bad faith. Should you rush to court and file suit under the ACPA or should you start drafting your UDRP complaint?

Time and Money

There are several factors that come into play when deciding whether to pursue a remedy under the ACPA or the UDRP, the two biggest factors oftentimes being time and money. As all attorneys understand, filing, maintaining and completing an action in federal court can be a long and expensive process. In fact, the average district court

action lasts roughly two years, exclusive of appeals, which means challengers will end up paying thousands of dollars in attorney's fees and court costs, all while the registrant sits on a domain name that may rightfully belong to the challenger.

As mentioned above, however, the UDRP is drastically less expensive and concludes relatively quickly. The table below outlines the fees for the administrative proceeding, depending upon the number of domain names at issue and whether a one- or three-member panel is deciding the merits:

Number of Disputed Domain Names	**Single-Member Panel**	**Three-Member Panel**
1	$950	$2,500
2	$1,100	$2,500
3	$1,250	$2,500
4 – 5	$1,400	$2,500
6 – 10	$1,750	$3,500
11 – 15	$2,000	$4,000
16 or more	To be determined in consultation with the Forum	To be determined in consultation with the Forum

Further, once a complaint is filed, final resolution must occur within 49 days (although the average length is 45 days). If a quick, fairly inexpensive resolution is desired, the UDRP may be the obvious choice.

Other Important Factors

Other factors, however, may prove to be equally important. For example, the UDRP provides relief for challengers with trademark rights in any country, while the ACPA requires rights to a mark in the United States specifically. Moreover, the only remedy under the UDRP is to have the domain name registration cancelled or transferred to the challenger. If money damages are desired, particularly if the registrant is selling infringing products and pulling potentially large amounts of revenue away from the challenger, filing suit under the ACPA may be preferable. In addition, as discussed above, jurisdictional issues may actually force the decision based on the domicile of the registrant.

Practically speaking, an overwhelming majority of UDRP cases result in the domain name being transferred to the Complainant. In fact, of the 4,756 cases decided as of the time this paper was written, only 764 resulted in a decision for the registrant. Accordingly, there seems to be better odds in filing a UDRP Complaint, especially if the facts of the case are particularly clear and do not require fact gathering under a discovery schedule.

It is also important to keep in mind that a decision under the UDRP does not preclude an action under the ACPA. In light of the limited costs and duration of the administrative proceeding, the challenger may well choose to file a UDRP Complaint first. If an adverse decision is rendered, the challenger can always take the further step of going to court. The only risk here would be the effect of the adverse UDRP decision

in federal court, which may be balanced by the ability to submit additional evidence of bad faith in the ACPA action.

One final factor worth pointing out is the challenger's overall objectives in pursuing the alleged cybersquatter. If the trademark owner wishes to send a strong message to potential pirates and the public, then the ACPA should be favored due to the expansive remedies. If, however, all that the challenger really wants is the domain name registrations cancelled or transferred, the UDRP is the obvious choice.

Conclusion

Practically speaking, a domain name provides an individual or business unparalleled power to reach an entire world of consumers with relatively little effort. No other means of advertising or direct marketing can achieve such vast coverage at comparable speeds. And although Internet surfers often use search engines to find products or services, accessing a web site by typing in a domain name composed of the trademark or brand name is oftentimes the quickest and certainly most convenient way to access information. A domain name address is, therefore, the core of the Internet identity of a business or individual. A fancy web site will never be fully effective if the domain name address does not correspond.

Cybersquatting takes advantage of this power by usurping the hard work and good will of a business on the Internet. In essence, these cyberpirates steal the very identity of even the most powerful companies by registering their names and marks in

domain names with no intention of using them for a legitimate purpose. Fortunately, the law of the Internet has evolved such that the mechanisms are now in place to attempt to protect the rights secured in trademarks from abuse by cybersquatters.