

## Protect Your Cyber Reputation

Beware those evil domain tasters and search engine manipulators.

BY TED CLAYPOOLE AND ADAM PALMER

For business, the Internet age means sales without borders and a worldwide market of billions of customers. The same aspects of the Internet that are so attractive to business, however, can also be a source of sleepless nights and deep concern for legal counsel charged with corporate brand protection.

Brand protection online is now crucial for all businesses. A poorly policed cyber reputation may cost your company dearly in lost profits, customer goodwill, and corporate image. In cyberspace, your reputation is your most valuable commodity—it determines your visibility and it can dramatically affect consumer confidence in your company.

### IN-HOUSE COUNSEL

Fortunately, protecting your brand in cyberspace is not impossible. It starts with a basic understanding of the major online threats to your company. Although far from a comprehensive list, the following are some of the most common concerns for brand protection in cyberspace:

#### CYBERSQUATTING

Imagine that you have a storefront on Main Street, but that shops, billboards, and bordellos all over town started using your store's name, confusing prospective customers. Cyberspace is like a town, and this troubling effect is called "cybersquatting." Every Web site on the Internet has a domain name.

Consider the address: [www.yourcompany.com](http://www.yourcompany.com). This would be your company's domain name. The .com ending is also referred to as a "generic" storefront or top-level domain name. Other variations may be .biz, .net, .org or even a country code such as .usa or .de for Germany. A cybersquatter may choose a domain name that includes your trademark or perhaps even your company name with a different top level domain ending. Using the above example, the cybersquatting site might be called [www.yourcompany.biz](http://www.yourcompany.biz). The cybersquatter is seeking to profit from the strength of your mark and confusion of your customers—to siphon your customers into places they were not choosing to visit.

Cybersquatting includes many creative variations, where a clever business tries to ride on the strength of your mark to garner attention for its own Web site. Some of these brand brigands are your competitors and some are completely unrelated. Some are scam artists overseas who can vanish as quickly as they appeared.

For example, typosquatters prey on the likelihood that people will misspell a word when typing in a domain name or that people will not notice a minor change, maybe a one letter difference, in a domain name. Your company registers the domain name, [www.trademark.com](http://www.trademark.com), and then the typosquatter registers [www.trademark.com](http://www.trademark.com). Some typosquatters simply place the letter "l" at the end of a famous domain mark, knowing that many people drag a lazy right ring finger over the "l" when typing the period.

*What to do:* Active monitoring of the Internet can lead to the discovery of potential cybersquatter domain names. Internet monitoring services may find substantially more infringing sites than basic commercial search engines. Common commercial search engines do not find sites that may attempt to conceal themselves from detection.

As in most trademark cases, sending a cease-and-desist letter to the offender is likely the first volley in the battle for favorable resolution, but many Internet offenders are hidden or noncompliant. You may file a complaint under the Uniform Dispute Resolution Procedures of ICANN (Internet Corporation for Assigned Names and Numbers, the international Internet governance authority) to force recovery of the domain name.

This is an entirely paper-based process and can be a relatively quick and low-cost solution. UDRP rules require only that a complaining markholder show that the respondent's domain name is confusingly similar, that the respondent has no legitimate rights in the mark being used, and that the domain name was registered in bad faith. The vast majority of UDRP complaints are decided in favor of the complaining party. The UDRP process allows a markholder to proceed against the name itself—a cyberspace "in rem" action, where the offending site's operator is too slippery to be identified and served.

Another option may be to file a complaint in a U.S. court under the Anti-Cybersquatting Protection Act, which can also be brought against the domain holder or against the domain itself. Proceeding either way will allow the trademark owner, if successful, to recover the domain name at issue. In addition, ACPA actions brought directly against the registrant provide for the possibility of further relief, including the recovery of the registrant's profits, damages, and attorney's fees.

### **SEARCH ENGINE MANIPULATION**

Trademark pirates may write your company's mark multiple times in the hidden code of their Web site, may create a web of "dummy" sites that associate their primary site with your mark, or may mirror your entire Web site on their servers to fool search engines into displaying their site first when a customer searches for your mark. They can even pay some search engines to direct your customers to their online storefronts.

*What to do:* If you can prove blatant manipulation, you can either work with a search engine's fraud department, or sue the infringer on traditional trademark claims. However, some courts have allowed a company to purchase its competitor's mark to secure a valuable search engine placement.

### **GRIPE SITES**

Have you found [www.yourcompanystinks.com](http://www.yourcompanystinks.com) yet? Maybe you need to look harder because chances are it, or perhaps some worse variant, exists in cyberspace. Gripe sites are not trying to be confused with your company's Web site, yet they are still using your trademark. In the Internet age, gripe sites are a low-cost way for your company's critics (maybe even dissatisfied employees) to express and disseminate their complaints.

*What to do:* Generally, your company may have to learn to live with these complaint sites. Courts have been loath to hold that the gripe site is confusingly similar to your trademark, and U.S. case law is increasingly offering protection to gripe sites as they often serve as forums of speech of or about a company. In addition, attempts to bring these sites down frequently give the complainer attention and credibility that he craves.

### **DOMAIN TASTING**

Domain tasting is a vicious bite out of your company's IP rights. Official domain name registration rules allow "a buyer's remorse policy" where users could register domain names and return them at no cost within five days. This was called the "add grace period" or AGP. Now that an entire domain name industry exists, a huge number of domain names are regularly registered and returned without the registrant ever intending to pay for, or keep, the domain name past the five-day AGP period.

This is commonly referred to as "domain tasting." Domain tasters may buy your trademarks or buy up names

you want to use, and hold them long enough to test the customer interest. This can cause confusion within your domain system, and infringement on your marks. The domain taster may abuse your brand for five days and then, after the AGP, leave like a bandit in the night without ever paying a cent.

*What to do:* This is more a policy matter that must be resolved at the Internet governance level rather than a specific response for you as in-house counsel. ICANN is considering multiple proposals that may close the AGP loophole. Until then, broad registration of valuable domains, careful Internet monitoring policy, and swift notice to a domain-name registrar of an infringing site may be the only response.

### **PHISHING**

Phishing for passwords, money, or customer data, these criminals cast an electronic net using your marks or copies of pages from your Web site. Phishers may send e-mails appearing to be from your company and directing your customers to a "harvesting" Web site. Phishing attacks can be more highly complex attacks coordinated by organized groups that roam the Internet for prey. Examples may include hacking into a system and placing a phishing page within the legitimate Web site. Some recent attacks have involved e-mails requesting information updates to employment application information for mass employers. The phisher exploits the knowledge that a large percentage of the population in any community has worked for, or applied for a job, with certain companies known for having large numbers of employees.

*What to do:* Unlike most of the other offenders listed above, phishing sites are not only a trademark violation but a crime with serious liability implications. Once detected, in-house counsel or an Internet monitoring service will provide notice to the domain name registry and ISP that a specific domain name is a phishing site and should be deactivated.

The procedures for doing this are commonly posted on major registry Web sites like Verisign. Notice should also be given to U.S. CERT (Computer Emergency Response Team) that a site is a suspected criminal phishing attack. This will engage law enforcement in the response to the site. Finally, the company itself may want to talk with specific customers that are suspected of having been victims of the attack to ensure the integrity of their personal data.

The Internet is a perilous place for your trademarks, but careful observation and vigilant enforcement can be your best weapons for protection.

---

*Ted Claypoole is a member of Womble Carlyle Sandridge & Rice, resident in the Charlotte, N.C., office, and part of the firm's intellectual property team. Adam Palmer is the general counsel of the cyber-intelligence company Cyveillance in Washington, D.C.*