

***Still the Wild West:***  
**Hot Issues Facing You on the Internet**  
Paul C. Jorgensen

*The following is a text accompanying a 2006 Powerpoint presentation by Paul Jorgensen.*

**Introduction**

Over the course of the last few years, I have had the opportunity to work on client problems on the Internet. Although the clients ranged from large Internet service providers to political campaigns to famous actors, my conclusion was the same: the Internet is still the Wild West.

Some of us still remember a world without the Internet. This was a time where driving directions were not immediately at our fingertips, where we couldn't answer our child's questions about the color of the sky with an MIT doctoral thesis, and where we could not order our favorite brand of shampoo from South Africa at 2:30 in the morning. Yes, it was a dark time.

But with the speed of the Internet comes new opportunities for business. New opportunities for business mean new ways for your honest clients to get ripped off or damaged.

Yes, the Internet is still the Wild West. Today I hope to give you a flavor of that.

- It is the land of opportunity for commerce and grubstaking to get consumer's attention and money
- Rustlers of all kinds are out there stealing and destroying property. After all, where there is money and an essentially flat playing field where it doesn't matter where you are, you'll have bandits.
- Rules are imposed randomly – there is a lot of self-regulation and law that is rushing into the voids created by new technology and problems on the Internet, but rules are often what you choose.
- Creative justice prevails – like the best lawmakers of the old west, those that succeed on the Internet are creative and don't always take the shoot first or call Marshall Dillon approach.

The thing I want you to carry away from here is a knowledge of some of the major hazards that you may face. You need to know this because you may have:

- Trade names and trademarks that you have invested a lot of money in to get recognized by consumers and engender the goodwill of your goods and services
- Domain names, websites and advertising on the Internet – although perhaps you didn't pay as much for an internet site as brick and mortar stores, your Internet presence must be routinely updated and cared for. This is worth protecting
- You also derive a revenue stream from the Internet – whether directly through sales or indirectly through developing the brand and advertising.
- Because of this investment, there will be disputes that will cost you money and goodwill.

## **Terminology**

Before we start, let's run over some of the terminology that you may encounter and use:

An URL is a Domain Name and File Address.

A domain name is the user-friendly form of an Internet Protocol (IP) address. Each computer that is connected to the Internet has its own unique address. This unique IP address is a string of numbers that can be difficult to remember. The Domain Name System (DNS) allows Internet users around the world to go to a specific website address by entering its corresponding domain name. DNS does this by locating and translating domain names into IP addresses.

A gTLD is a generic top-level domain. The gTLD of an Internet address appears to the right of the "dot" in the address. GTLDs include the familiar .com, .net, and .org as well as seven new gTLDs that were added in 2000. These seven new gTLDs are" .aero (for the aviation community), .biz (for business purposes), .coop (for cooperatives), .info (unrestricted), .museum (for museums), .name (for personal names) and .pro (for professionals).

Search Engine: These are the major computer systems that allow users to enter several simple words and get a list of websites that may answer their search. Google, AltaVista, Lycos and others are major search engines. Since people turn to the top ranking search results of search engines more than 80% of their searches, search engines and results rankings are extremely important.

ICANN was created by members of the Internet community in response to a June 1998 White Paper issued by the U.S. Department of Commerce (DOC) under the National Telecommunications and Information Administration Agency. ICANN facilitates the technical, managerial and policy decisions of the Internet. Although ICANN administers certain DNS functions, it accredits commercial registrars who register domain names for people and companies.

The UDRP is a set of rules adopted by all accredited domain-name registrars. The policy is incorporated into every domain name Registration Agreement, the agreement between the accredited registrar and the registrant. It obligates the domain name holder to submit to a UDRP arbitration procedure in disputes. We'll go into how this works later.

## **What Trouble May Befall You**

There are many things that can go wrong on the Internet. In this presentation, we are not going to cover the privacy or hacking/worm/Trojan horse issues that have proliferated with new technologies. Instead, we are going to cover the major issues that you may face if they sell or advertise or even have a corporate presence on the Internet.

So what can happen?

- Someone could use your trademark or a similar mark in a domain name
- Someone could smear your good name or criticize you on the Internet
- Someone could hide your trademarks or names within their sites
- Someone could use your properties without permission, like your images, names, or logos
- Someone could attempt to divert consumers from your site to their site.
- Someone could connect to your site without permission

Let's look at some details of each of these problems.

## **Cybersquatting**

Cybersquatting happens when someone takes your trademark and uses it as part of a domain name. This action could prevent you from using your mark in conjunction with your website or divert customers searching for you to another, possibly competitive, website.

As you may know, registering a domain name is a first-come, first-served process. Cybersquatters exploit that. They register names of trademarks, famous people or businesses with which they have no connection.

What usually happens is that the cybersquatter gets the domain name, then 1) offers to sell the domain name to you at prices exceeding the cost of registration, 2) sits on it and prevents you from using it; 3) threatens to sell it to a third party; or 4) use the domain to draw traffic and business to their own sites.

In one of my recent cases, we found a website that used a client's name in the domain, along with another word. On the site, the owner used our client's name and sold goods or linked to sites selling goods not authorized by this client. I was able to resolve this issue informally and without suit, getting the cybersquatter to turn over not only the domain name but the website content to our client. Our client now runs the site. More details on informal resolution options later when we discuss attack options.

## **Typosquatting**

Typosquatting is cybersquatting that counts on the fact that most people are poor typists.

Typosquatters pick a domain name that is only one or two letters from your trademark. In cases that I have handled, we had typosquatters registering domain names that used our client's trademark and added a w in one case, and a y in another. Typosquatters are counting on the fact that most people, if they type in the wrong website name, will stay, at least temporarily, at that wrong website. For this reason, typosquatting is most often used by pornographers and poachers looking to draw "hits" to their site from consumers who are attempting to access your website.

Most typosquatters erroneously believe that using a domain name that is one or two letters off a trademark or other domain name somehow shields them from liability. If they use these misspelled words to redirect consumers to websites with competing products and services, you will not be pleased. However, we have been able to use the UDRP procedure to get typosquatted domain names transferred to our client. I will explain that process a bit later.

## **Metatag Abuse**

A metatag is an HTML (hypertext markup language) code embedded on a Web page and used to identify its content. You cannot see metatags when you get to a website. However, if you know where to look, metatags look like complicated streams of words and slashes.

Search engines use metatags to wade through HTML code and text and find search terms, revealing the one with the search terms to the searcher. In short, metatags are one way to help ensure that your customers find you or your goods or services on the Internet.

You can see how you could experience metatag abuse if someone, like a competitor, uses them to divert or confuse consumers. For example, your competitor inserts your trademark into its metatag. A customer using a search engine to find you is diverted to the competitor instead. One judge described the practice as similar to a shop owner posting a sign with another company's trademark in front of her shop.

But this practice was more prevalent in the prehistoric days of the Internet, namely, way back in 1995. Metatags were almost the exclusive tool used by search engines to help them determine how to rank sites in their search results. Now, metatags are only one thing that search engines use, and so its importance is greatly diminished. Only one major search engine, Inktomi, uses metatag priority searches.

Today's more sophisticated search engines like Google don't base its rankings on the easily-doped metatag system. Instead, Google and other search engines base their rankings heavily on the text that

makes up the page, which is much harder to fake or dope. Today's engines use a combination of keywords to prioritize searches. Keywords can appear in 1) the URL, 2) the HTML Title that describes the contents of your web page in one sentence, 3) the metatag/ALT tags, which describe images on the site, and 4) the text of the page.

On this page, the text is littered with keywords. This client has decided to use words that would attract those looking for defense or combat supplies, specifically barriers. The search engine is going to look for keywords and it parses them in terms of prominence, proximity to other keywords, density and frequency.

Improperly used, keywords can infringe your trademarks, trade names, copyrighted materials, and can divert customers from your site.

### **Hyperlinking**

A "link" (or "hyperlink") is a component of a Web page that connects to another Web page. Clicking on highlighted text or a graphic image activates the link. For example, a user could click on the photo of Muhammad Ali and be transported to the page on which a story about him appears.

You are probably going to use linking. It is fundamental to the functioning of the World Wide Web. However, you may not want your valuable content associated with certain sites. For example, a link may defame a person or business if its effect is to create an untrue statement that injures the reputation of a person or business. Your competitor creates a hyperlink titled "Garbage Producers" and links it to a picture of your work site.

A link may violate your reasonable expectation of privacy. For example, a disgruntled employee creates a hyperlink titled "Elephants on Parade" that links to a hidden camera in your corporate board room.

A link may contribute to unauthorized copying of a copyrighted work. For example, someone posts one of your copyrighted books on a website. You order them to remove it. They do, but they provide links to other sites that contain infringing copies of the book. That infringer knew and encouraged the use of the links to obtain unauthorized copies of your book.

A link may imply an endorsement or sponsorship. If a link uses your graphic trademark, like the Nike swoosh, users may believe that the linked user is sponsored or endorsed by Nike.

A "deep link" is a hyperlink that bypasses a website's home page and takes the user directly to an internal page. For example, instead of linking to the home page of Coca-Cola, a deep link might take the user directly to a health page within the site. Deep linking allows users to bypass information and advertisements at your home page and go directly to an internal page. As a result, you can lose income if your Internet revenues are tied to the number of viewers who pass through your home page. Also, your message on a home page can be missed – for example, your home page advocates a point of view, but a deep link to an internal Web page implies that you have a different point of view.

### **Framing**

Framing is the action of visiting a second website while remaining in a previous website. This is similar to the "picture-in-picture" feature offered on some televisions. Consumers will appear to be at your site, but actually traveled to another site. Framing may trigger a dispute under copyright and trademark law theories.

A framer may be violating a copyright for reproducing or creating a derivative work based upon the original work. A "derivative work" is "a work based upon one or more preexisting works, such as a translation,... art reproduction, abridgement, condensation, or any other form in which a work may be recast, transformed, or adapted."

To determine which of your copyright rights were violated in an unauthorized framing situation, courts look to the purpose and function of the frame. At least one court has found that a framer did not unlawfully reproduce copyrighted material by framing, but the framer created an unlawful derivative work.

A framer may imply an association with or sponsorship of the products or services offered by you. As the URL of the framer company still appears on the browser, your identity may be so obscured that the framer appears to be the provider of such goods or services. Customer confusion is inevitable in this situation.

### **Inlining**

Inlining is the process of displaying a graphic file on one website that originates at another. For example, inlining occurs if a user at the site can, without leaving that site, view a "item of the day" featured that comes from another site (a horoscope, a comic strip, calendar, etc.). In legitimate inlining, the user has an agreement with the secondary site to inline to the first website.

Inliners have been stopped, however, on the basis that the process could destroy the integrity of the source material used (if, for example, that source material was displayed at an adult or racist site). If that happens, you can stop the inlining and require an agreement or license to its material. Alternatively, the inliner can stop inlining and, with permission, establish a more traditional link to the source material page.

### **How to Handle the Problems**

Now the good news: the trademark laws – infringement, unfair competition, dilution and cybersquatting appear to be well suited to allow the courts to make hard decisions about your Internet problems. The better news: because of the nature of the Internet, you may never need to go to a court to get the results you want.

Our first step is to carefully research the extent of the problem, including interactions between links, infringing sites, and who is behind the infringement. Information like this is relatively easy to find. However, because of the transitory nature of the Internet, it is important to document information, especially screen shots, that are dated. These will become important if an infringer suddenly changes things that support your argument.

Next, we review the nature and extent of the potential harm, the likelihood of success with various approaches, the costs and the likelihood of repercussions.

Our experience is that when you contact the infringer, many will fold and even pay money to avoid liability. Depending on the facts, you may also be able to contact ISPs, registrars or warehouse sites – they may have policies against the actions of the infringer, and may take action or simply add extra pressure on the infringer to stop. This kind of intuitive approach definitely demonstrates the Wild West nature of the Internet – there are many ways to meet your goals.

### **UDRP Actions**

For domain name infringements, after the initial attempts to get the infringing domain name transferred or cancelled, a cost effective option is a UDRP complaint. Since domain name registrants agree to the mandatory dispute resolution forum for all domain name conflicts, there is little basis for an infringer to challenge the legitimacy of the UDRP. You can use the UDRP if you own or simply use a trademark.

These are the elements of the complaint, which is filed electronically with supporting documents: a) the domain name is identical or confusingly similar to your mark; b) the registrant has no rights or legitimate interest in the domain name; and c) the domain name was registered and used in bad faith. If you are able to support these arguments, the arbitrator may cancel the domain name or require the transfer of the domain name to you. There are no monetary damages.

There are certain advantages of the UDRP process: a) more efficient than using the courts in securing the transfer of a domain name; b) significantly less expensive than a court action, and allowing you to anticipate out of pocket expenses before proceeding; c) many of the UDRP panelists are trademark practitioners familiar with the intricacies of trademark rights and the impact that domain names have on those rights.

## State and Federal Courts

There are numerous state and federal court options available to fight back against Internet problems. These are based on common law and state and federal statutes.

### Trademark infringement

Elements are:

- a) One uses any word, term, name, symbol, device, or combination;
- b) in interstate commerce;
- c) which is likely to cause confusion as to source, sponsorship, or association.

Available for: all of these problems if your trademark is used.

In cases where the trademark is used in a domain name, your best bet is to go informal then UDRP. Alternatively, you, if they are the trademark owner, can use the federal trademark statute. When dealing with domain name issues, courts look to see if:

1. The trademark is used for noncommercial purpose;
2. The website owner is exercising a First Amendment right to free speech (we'll talk more about that in the defenses section in a moment);
3. Whether the site owner tries to divert customers or has a bad faith intent to profit from the mark;
4. Whether the site suggests some sort of sponsorship or affiliation with the trademark owner; and
5. Whether the domain name communicates the protected nature of the content.

### ACPA

The Anti-cybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)) prohibits cybersquatting and provides important remedies to trademark owners, including:

- a) Cancellation of the domain name or the transfer of the domain name to the trademark owner; and
- b) an award of actual damages, or at the trademark owner's option, an award of statutory damages of between \$1000 and \$100,000 per domain name.

Elements are:

- a) a bad faith intent to profit;
- b) the registration, use, or trafficking in (buying or selling) an domain name identical or confusingly to a distinctive trademark, or dilutive of a famous trademark.

Available for: Cybersquatting and typosquatting

### Dilution or Tarnishment

A famous trademark is blurred or tarnished by someone else's commercial use of the mark. Blurring is a "whittling away" or weakening of the mark's distinction, lessening the trademark owner's ability to identify its goods and services via the Internet. For example, if "Versace" was placed in the metatag for various websites selling shoddily made leather goods, over time, that would weaken the Versace trademark.

Tarnishment occurs when a famous trademark is damaged by an unpleasant or unwholesome use of a similar name. Federal Trademark Dilution Act (FTDA) is a statute set up to answer this, but there is great dispute on its application, especially in the definition of "famous" marks.

Elements are:

- a) famous mark;
- b) commercial use of mark; and
- c) action causes loss of the distinctive quality of the mark.

Available for: cybersquatting, typosquatting, metatags, in-lining, linking, framing.

Unfair Competition

Unfair competition refers to a group of state and federal laws that prohibit unethical behavior by businesses. Unfair competition consists of a body of related doctrines that gives rise to several different causes of actions, including (1) actions for *INFRINGEMENT* of *PATENTS*, *TRADEMARKS*, or copyrights; (2) actions for wrongful *APPROPRIATION* of trade names, *TRADE DRESS*, and trade secrets; and (3) actions for publication of defamatory, false, or misleading representations.

Available for: All

There are also related claims that we can use in Internet actions:

False Advertising

False advertising occurs when a misleading statement about a product or service deceives the public.

Elements are:

- a) the advertiser made false statements of fact about its product;
- b) the false advertisements actually deceived or had the capacity to deceive a substantial segment of the target population;
- c) the deception was material;
- d) the falsely advertised product was sold in interstate commerce; and
- e) the party bringing the lawsuit (known as the "plaintiff") was injured as a result of the deception. Actual loss is not required to show an injury, just a reasonable basis for the belief that the plaintiff is likely to be damaged as a result of the advertising.

Available for: linking, framing.

Breach of Contract - A breach of contract may occur if users agree to contractual limitations when using a website, and then create links in violation of those terms.

Elements are: a) contract; b) violation of term of that contract.

Available for: linking, framing, in-lining

Disparagement/Defamation

An action for defamation is to protect the personal reputation of the injured party, whereas the action for injurious falsehood or business disparagement is to protect the economic interest of the injured party against pecuniary loss. Significantly, an injured party may sue for both personal defamation and business disparagement in the same suit so long as he avoids duplication of damages.

### Elements are:

- a) publication by the defendant of the disparaging words;
- b) falsity of the statement;
- c) malice;
- d) lack of privilege; and
- e) special damages.

Available for: linking, framing.

### **Defenses**

There are certain defenses that are available in the situations that I have described so far. These can be intricate, so it is always best to consult with an attorney to determine the risk that these defenses will prevail. Among the frequently used defenses are:

1. No Infringement.
2. Parody
3. Complaint/Gripe Sites
4. Criticism
5. Comparative Advertising.
6. Fair Use.
7. Nominative Fair Use
8. Safe Harbor under the Digital Millennium Copyright Act.
9. Disclaimers.

### **Conclusion**

You need to know that the Internet is IP not IT. You need to be proactive and work with an attorney to forge a comprehensive Internet Policy with the following elements:

1. Proper presentation of corporate identity and brands on the Internet.
2. Website policies, including proper use of marks, permissions and licensing, and privacy (especially if you collect information).
3. Registration and maintenance of domain names – nationally and internationally
4. Routine scanning protocols (websites and auctions)
5. Linking, metatag, framing positions

You should also determine how you will react in situations of trademark abuse, brand dilution, confusion unwanted association, illegal distribution and counterfeit sales. Your attorney should help you determine a cost effective reaction with the goal that you, not anyone else, profits from your use of the Internet.