Cybersquatters, Gripe Sites and Dispute Resolution Procedures: Mitigating Risks to Your Brand Posed by the Web and Social Media

By David R. Street

Lerners LLP

Prepared for

FEI Canada

SME Conference 2011

Driving Growth And Expansion

Concurrent Session IV

Risk Mitigating Strategies for SMEs

Thursday November 10, 2011

Cybersquatters, Gripe Sites and Dispute Resolution Procedures: Mitigating Risks to Your Brand Posed by the Web and Social Media

Table of Contents

Introduction

Companies spend large amounts of time, effort and money in developing and promoting their brands. The Internet has played a key role in expanding the power of brands by providing countless new ways to market a brand. At the same time it has made it much easier for others to profit from another company's brand through infringement and misuse and for others to disparage a brand, tarnish its image and impair its value. In this paper I discuss three areas of risk to your brand posed by the Internet. They are the domain name system, gripe sites which are a special case of a domain name system issue and social media. In each case after identifying the problem and risks I offer some suggestions for mitigating the risks. From the perspective of understanding the risks, it doesn't matter so much what your level of engagement is with the Internet, but rather the overriding importance of continuously monitoring the Internet for anything where your brands or your company are discussed or referred to whether in favourable terms or negative terms. It's not only relevant to the consumers shopping for goods and services on the Internet but also to the very high proportion of consumers who report conducting product research on the Internet before making any purchase from retailers and other businesses.

Brand protection is mainly through the use and application of the law of trade-marks. A brand in the broadest sense of the term will almost always involve at least one trade-mark and often several trade-marks. The expression brand tends to be the term more commonly used in business although lawyers prefer to use the term trade-mark. In this paper I use the terms interchangeably.

Part 1 – Brand Protection by Protecting and Managing Domain Names

The growth of the Internet and its use of domain names pose one of the greatest challenges to the protection of brands and trade-marks. Domain names have become the primary means for consumers to find brand owners. An understanding of domain names is important to understand the threat they pose and how to protect brands and trade-marks from domain name abuse in the form of infringement, dilution and other misuse by third parties.

How the Domain System Works

The internet connects computers by using the Internet Protocol (IP) address system. Each computer is assigned a unique number such as 452.216.784.391. Since humans are not good at remembering strings of numbers domain names are used to associate IP addresses without the need to remember long strings of numbers. It is operated by a non-profit organization known as the Internet Corporation for Assigned Names and Numbers or ICANN.[1]

The Parts of a Domain Name

We all know that a web address looks like this http://www.brand.com. For brand and trade-mark owners it's the parts after the www that are the most important. The ".com" portion or the right most portion after the last period is known as the top-level domain or TLD. The TLD determines the register on which the domain name is listed.

The part to the left of the TLD is the second-level domain. This portion of the domain is where most domain name disputes arise and the allegation is usually that the second-level domain name infringes another party's trade-mark. There can also be third level domains which are alphanumeric strings proceeding the period before the second-level domain.

Top-Level Domains

There are two types of top-level domains; country-code top level domains referred to as ccTLDs and generic top-level domains referred to as gTLDs.

ccTLDs

ccTLDs are two letter extensions that are intended for specific countries or territories. Every one will be familiar with the ccTLD for Canada which is .ca. There are currently 250 ccTLDs.

gTLDs

Generic top-level domains have three or more characters that are not country or territory specific. The most popular of these is .com. gTLDs are further broken down into sponsored and unsponsored TLDs. The current unsponsored TLDs are .biz, .com, .info,

---

[1] www.icann.org

.name, .net, .pro and .org. Sponsored gTLDs are specialized domains sponsored by private agencies or organizations for specific usage and are restricted to specific communities. The current sponsored gTLDs are .aero, .asia, .cat, .coop, .edu, .gov, .int, .jobs, .mil, .mobi, .museum, .tel and .travel.

The organization responsible for the creation and delegation of TLDs is the Internet Assigned Numbers Authority or IANA. IANA is part of ICANN. IANA assigns an operator for the TLD and the operator allocates domain names and maintains a register of all domain names registered under that TLD. If you register a domain you get an exclusive right to use the domain for a fixed period of time but it is not actual ownership. Domain names are issued on a first-come, first-served basis and you have to pay an annual fee to maintain a registration.

There are more than 1,000 independent registrars accredited by ICANN to sell domain names in many different TLDs.

Cybersquatters, Typosquatters and Domain Snipers

Cybersquatting is the practice of acquiring a second-level domain name which includes a well known trade-mark or brand or closely resembles that trade-mark with the hope of benefiting from the goodwill that attaches to the brand or trade-mark. This often occurs when a company focuses on certain TLDs and leaves other valuable TLDs available for registration by others. Sometimes a company inadvertently permits a domain name registration to lapse. There are "domain sniping" programs that notify a third party when a domain name expires and may even carry out a registration for the third party. Typosquatting is really one kind of cybersquatting as it involves acquiring domains that include some kind of often repeated typographical error in spelling of either the trade-mark or the domain. There are different ways a cybersquatter or typosquatter tries to make money. They may sell the rights to the domain to the trade-mark owner. They may use the domain to sell competitive or counterfeit products or to set up a page with advertisements from which revenue is derived on a pay per click basis.

A recent study by the Corporation Services Company reported that the most common prefix registered is 'www' so for example the domain name would be 'wwwbrand.com'.

The most common suffix registered is 'online' so for example the domain would be 'brandonline.com'.[2]

What Can You Do

If you determine that someone has acquired a domain that incorporates one of your trade-marks, there are a number of options that can be taken.

1. The owner of the domain can be approached to see if they will agree to transfer the domain to your company for a modest sum that would include at least the cost of registering and maintaining the domain. You may want to have a third party approach the domain holder if you're a well known company in an effort to keep the price from escalating. This can often be the quickest solution. Once acquired you may simply wish to warehouse the domain if it's a variation on the one you actually intend to use in order to prevent others from acquiring it. It's been reported that the top 50 companies in the Fortune 500 have on average 6,000 domain names registered, most of which are held for blocking purposes.

2. All gTLDs and most ccTLDs have a policy in place to regulate disputes over domain names within a TLD. The Canadian Internet Registration Authority (CIRA) is the registry for the .ca top-level domain. Its dispute resolution policy is known as the CIRA Dispute Resolution Policy or CDRP. It is modeled on the ICANN Uniform Dispute Resolution Policy or UDRP which applies to the .com, .net and .org TLDs. A key requirement of the CDRP is that a complainant must meet a Canadian presence requirement.

If the domain holder refuses to sell or demands an excessive price then the next course of action would be to file a complaint under the applicable dispute resolution procedure for that domain. Disputes are decided based on what is referred to as a resemblance test which looks only at the degree of similarity between the domain name and the trade-

---

[2] "*An Analysis of the Most Infringed Terms within Domain Names*" a White Paper of Corporation Service Company www.cscglobal.com.

mark. Identical domain names are assumed to be confusing. In Canada "complainants have consistently won about 80% of disputes."[3]

Complaints under the CDRP are decided based on documentary evidence and arguments in writing. There are no hearings at which oral testimony or oral arguments can be made. Beginning in 2012 all submissions must be in electronic format. Most decisions are rendered within 60 days. If a complainant is successful, the domain name will be cancelled or transferred to the complainant although a 30 day period is allowed to take the dispute to court. Either party may challenge a decision in court. Costs are approximately $4,000 for a default panel of three members. If the parties agree to a single panellist, the cost is $1,750.

3. A formal court proceeding in Canada alleging infringement under the *Trade-Marks Act* is always an option but takes considerably more time and expense than a voluntary transfer between the parties at a reasonable cost or a complaint under one of the dispute resolution policies discussed above.

New TLDs: New Opportunities and Risks For Brand Owners

In 2010 there were 250 ccTLDs and about 22 gTLDs. As of January 12, 2012 ICANN will accept applications for new gTLDs. Companies will have the opportunity to own and control their own TLD instead of dealing with third party owned and operated TLDs like .ca and .com. There will be countless new opportunities for branding and marketing. For example, an applicant could set registration criteria for the new TLD so that registration would be exclusive to your company only. There could be new TLDs for .dell, .IBM, .rogers, .toyota.

At the same time there will be new opportunities for fraud, counterfeiting, and infringement. There may be a large increase in confusion among online consumers. Policies and programs for domain name registration, brand monitoring and enforcement will need to be changed and updated.

---

[3] "*Dealing with Cybersquatters*" by Michael Erdle prepare for Osgoode Professional Development Centre program Protecting Your Brand on the Web and in Social Media held on September 26, 2011 at page 8.

The new TLCs are not for the faint of heart. In making an application, you're not simply requesting a domain name but you are applying to create and operate a registry. The initial application fee is US $185,000 and the annual fee is US $25,000. The initial window for applications will close on April 12, 2012 although future rounds are to occur once some experience is obtained with the first round of applicants.

Part II - Gripe Sites: What Are They and How To Deal With Them

A gripe site or criticism site is generally a domain that's registered by a dissatisfied consumer that includes along with a well known trade-mark a derogatory term such as "sucks". There is one for example called www.homedepotsucks.com. There's even a site called WebGriper.com that collects links to gripe sites. The issue that arises in these disputes involves balancing the right of free speech and the rights associated with a trade-mark. Where a trade-mark owner comes upon a gripe site the first issue is to determine if either the CDRP or the UDRP applies. If the UDRP applies, the decisions suggest that a genuine cyber griping site about a complainant whose trade-mark forms part of the domain can give rise to a legitimate interest in the domain name sufficient to defeat the complaint of a trade-mark owner. However, if the domain name is not being used as a legitimate gripe site but is left "parked" as a click through revenue generator, or is used to sell products, a complainant will likely succeed.

In the single reported case under the CDRP, the complainant succeeded in obtaining the website where the only difference was that the registrant used the .ca TLC whereas the complainant used .com. There was no derogatory term added to the trade-mark name and there was no commercial use by the registrant. Under the UDRP, there's a greater chance a complaint will be dismissed regardless of whether there's a derogatory term added to the trade-mark, as the registrant will be considered to have a legitimate interest in using the trade-mark as part of the domain name of a criticism site if such use is fair and non-commercial.[4]

---

[4] "*Gripe Sites and Dispute Resolution Proceedings*" by Shane Hardy a paper prepared for Osgoode Professional Development Centre program Protecting Your Brand on the Web and in Social Media held on September 26, 2011.

One of the things you probably shouldn't do if you encounter a gripe site is ask your lawyer to send out a cease and desist letter. Invariably once it's received, the griper will post the letter on the gripe site and the dispute escalates. Consider other alternatives first.

Another reason for monitoring the Web is the early detection of gripe sites. If the site is the work of an individual who was unhappy with a product or service, the first line of defence should be to contact the person involved and see if their complaint can be resolved. If that can be done, the site may be taken down voluntarily before it gains traction with others.

This is another area where registering domain names containing your trade-mark with common derogatory terms as a means of blocking others from getting them is a worthwhile and not all that expensive.

Part III - Brand Protection Problems And Solutions With Social Media

One of the most significant developments in the evolution of the Internet in recent years has been the creation and explosive growth of what is referred to as social media. Everyone will have some knowledge of the big ones which are Facebook, Twitter and LinkedIn but there are many others. They have changed the way people interact. As a measure of their size and potential impact consider the following statistics.

Facebook claims to have more than 800 million active users. Twitter is reported to have more that 175 million users with over 140 million tweets written every day. LinkedIn is reported to have more than 120 million members. With those numbers they can't be ignored and they shouldn't be because they provide enormous new opportunities to market and promote brands. There is a dark side however as there are also many new opportunities to infringe trade-marks and disparage brands.

Some Of The Problems

Usernames and Profiles

As with domain names one of the key problem areas is the adoption of a social media username that is identical or similar to a brand name or trade-mark. There is virtually no control over the adoption of social media usernames. As long as it's unique, in the sense that no one has already been issued that username, a username will be issued to an

applicant on a first come first serve basis. The person obtaining such a username is then free to post content either good or bad about your brand while appearing to be an official or authorized person. Celebrities, athletes and to a lesser extent politicians have all had problems with persons adopting usernames that suggest they are a particular person when they're not.

It's not merely usernames however because registrants may make references to your brand in their profiles and in various postings such as in a tweet posted on Twitter. One of the issues not fully resolved is when does use of a brand name or trade-mark in social media amount to use of a trade-mark in the legal sense that constitutes infringement.

Employees

Problems with social media can and do often arise with your own employees. There are many reasons why every company needs to have a policy on the use of social media by its employees. While not directly related to brand protection a key issue is what sort of access will be permitted by employees during working hours for business use and for personal use. Are employees authorized to post `on social media and if so what are the guidelines for appropriate content? Do you require approval before any pages affiliated with your company are created or content of any kind is posted? If references are to be made about clients or customers there should be a requirement for consent to be obtained. Many companies have some form of confidentiality agreement with their employees. Employees may need to be reminded that nothing they post on social media should be in violation of their confidentiality obligations. Examples should be given about what is acceptable to post and what is not acceptable. One guideline I've heard suggested is not to post anything on social media that you wouldn't also post on a billboard. The policy on social media needs to be brought to the attention of employees by inclusion or referencing it in written employment agreements, posting it on the companies intranet and including it as part of the training for new employees. Social media policies need to be regularly reviewed and updated because this is an area that is constantly evolving.

Licensees and Franchisees

Another area often overlooked is with distributors, sales agents and franchisees all of whom are usually licensed to use your trade-marks in the context of selling your products

and services or for carrying on business as a franchisee. You should address in all those agreements what kind of use these licensed users may make of your trade-marks in their social media which should likely include a requirement that they have a policy on social media for their employees. Another key term would be to require the deletion of any pages referencing your brand once the licence agreement or franchise agreement is terminated.

Solutions

1. If you encounter a username in social medial that incorporates one of your trade-marks one of the first steps to be taken is to review the terms of use posted on the social media site. These companies all have their own intellectual property in the form of trade-marks and copyright and are sensitive to unauthorized use and infringement. Facebook for example has two separate forms for filing a complaint, one for alleging trade-mark infringement and another for alleging copyright infringement. One of the problems however is there is no uniformity in these terms of use and no common dispute resolution process such as there is with the UDRP and CDRP in the context of domain names. Each site's policy must be reviewed and then observed if a complaint is to be prepared and submitted.

2. Communicate directly with the infringer to see if they will voluntarily give up the username.

3. Another solution, more in the nature of a proactive preventative measure, is the registering of usernames on the most prominent of social media sites for trade-marks and some of their variations in order to prevent others from acquiring them.

4. As with domain name issues, you always have the option of commencing a legal action alleging trade-mark infringement. Such actions can be time consuming, expensive, and not very quick to a resolution. There's also uncertainty as to when does use of a trade-mark in social media constitute use that amounts to infringement in the legal sense.

Hackers and Social Media

Hackers love to gain access to social medial accounts because then they can distribute malware from what is a trusted source. In noting that it had recently improved its

security, Facebook reported recently that in one day it had blocked 600,000 attempts to hack into the accounts of Facebook users. Another recent report indicated that 30% of small and medium enterprises have had their social media accounts compromised and malware spread on their systems.

One of the reasons social media is vulnerable to hacking is because of poor password practices. I'm sure we all dislike passwords because we have too many and it's hard to remember them especially when we're expected to change them regularly. Commentators have indicated that a high proportion of social media users use the same password for each of their social media accounts. This is not desirable because it means that a hacker who discovers one password can access all of your social media accounts. It's critical in this area to use strong passwords, consisting of a minimum of eight characters with a combination of letters and numbers and to change them every three to four months. Appropriate password use is another issue that should be part of the social medial policy at your company.

Return on Investment

All businesses will want to minimize their costs of monitoring and protecting their brands online. It's likely that not all infringements need to be pursued, only the most egregious ones and the ones that will have the highest visibility. If you spend time and money on monitoring the internet, register appropriate domain names and social media user names including ones for blocking purposes and take steps to enforce your rights as a trade-mark owner, is there anything out there to help you calculate a return on your investment. There's nothing that I'm aware of. There are a number of programs to help collect and analyze data on web traffic and other activity on the Internet but nothing that purports to measure the ROI for efforts at monitoring and enforcement. It may be however that doing nothing is not a choice. Brands, trade-marks and domain names are valuable assets and if appropriates steps aren't taken to protect those assets their value will be diminished as will the value of the businesses that own them.

Conclusion

In summary, in order to mitigate the risks to your brand, there are four things you should be doing.

First, monitor the Internet for everything about your company and your products and services. Hire one of the companies that perform monitoring services if you don't have in-house expertise.

Second, register and monitor your trade-marks in every country where you're doing business or expect to be doing business in the near future. Generally speaking a registered trade-mark will trump a domain name and a social media username that incorporates the trade-mark.

Third, register and monitor your trade-marks as domain names and social media usernames.

Fourth, establish a social media policy for your company and your employees and require your licensees and franchisees to have one also.

David R. Street
Lerners LLP
130 Adelaide Street West
Suite 2400
Toronto, ON M5H 3P5

Direct Line: 416.601.4141
Direct Fax: 416.601.4142
dstreet@lerners.ca

1884448.2