

Defending your corporate brands

- ✓ Online branding complicates trademark protection. It offers opportunities for growth but is difficult to police
- ✓ Domain name stealing isn't the only threat and going offline is no solution to regulatory challenges as chatrooms threaten reputation
- ✓ An IP audit can help discern extent of intellectual property, facilitating brand name protection strategy and identifying vulnerabilities
- ✓ Determining the availability of a brand name requires research and should be the kick-off point for any effective monitoring program

COUNTRY CODE TLD GROWTH

Often, country code registrations accelerate in regions that are experiencing rapid growth or regulatory change.

The fastest growing country code top level domain (TLD) registrations during Q1 2007 were .ru (Russian Federation), .fr (France) and .kr (South Korea).

Top ten registries

Top CCTLD Registries by domain base for the first quarter of 2007

Rank	Domain	Country
1	.de	Germany
2	.uk	United Kingdom
3	.eu	European Union
4	.nl	Netherlands
5	.cn	China
6	.it	Italy
7	.ar	Argentina
8	.us	USA
9	.br	Brazil
10	.ch	Switzerland

Source: Zooknic, April 2007

Trading on reputation?

Corporate branding and name recognition are well-established fields and most companies are well versed in the importance of creating customer loyalty based on reputation and identity. Product promotions and advertising campaigns attract millions of dollars and many companies have become household names as a result.

Part of establishing a good reputation is being able to protect it. Legal environments in the US and globally have a long history of allowing companies to safeguard trademarks and corporate identity. Yet any marketing professional will tell you it can take years to develop a reputation but only minutes to lose it.

Protecting trademarks and intellectual property has become a far more challenging problem in the internet age. Areas for infringement are numerous, change quickly and may not be immediately obvious to many companies.

The most obvious form of online brand recognition is the corporate domain name. The number of registered top level domain (TLD) names totaled 128 million at the end of Q1 2007, according to research from VeriSign, the global registrant for .com and .net web addresses. This represents an estimated 31 percent increase over 2006 registrations. In the first quarter of 2007 a total of 10.7 million new domain names were registered.

For companies that operate in a global environment, it is important to be aware of the various country code suffix variations used in domain names. Of the 120 million registered names, the .com prefix is the most popular followed by .de, .net, .org and .uk. There are currently over 240 country code domain extensions available. For a company operating in multiple

jurisdictions, it is common to have a range of country specific sites. For example, a company operating in the US, the UK and Australia will likely register the .com, .co.uk and .com.au country codes.

Even if a company does not have operations in a particular country, it may still be worth registering the name in order to prevent a third party from doing so and benefiting from the name.

High traffic zone

The importance of a robust online branding strategy can be highlighted by the number of unique domain name system queries performed on a daily basis. During Q1 2007 a VeriSign analysis showed that there were, on average, 30 billion queries or attempts to access .com or .net domains per day, resulting in millions of users accessing the web or sending emails. With this level of traffic, online branding becomes vital.

Establishing a domain name is only the first step, however. Once a domain is registered it has to be renewed. Rules vary from country to country but often this must be done on an annual basis. Failure to renew a registered name may result in a third party acquiring the name and using it for his or her own benefit or demanding a significant price to return it. Laws do exist to prevent cybersquatting like this, but the legal environment remains unclear in many countries. The overall renewal rate for registered .com and .net sites during Q1 2007 was 76 percent. The rate for sites that had previously been renewed was 85 percent, indicating that once names are established, renewal is being more closely monitored.

Apart from the significant opportunities the internet affords companies in terms of

marketing and brand development, it also presents a considerable array of dangers. By its nature, the internet is a very difficult environment to police, making it particularly hard to monitor the usage of brand names and other messages that may be distributed by third parties. Any online marketing presence must be supported by a robust and well-designed intellectual property protection procedure.

The first step for creating a process to monitor and protect intellectual property is to understand the types of third parties that are registering domains and the potential uses of those registered names.

Third parties dominate the scene

Research into 86,621 registrations by Corporation Service Company (CSC) shows that 72 percent of registrations belong to third parties, not the brand owners. Of these, 71 percent are generic TLDs. Despite the number of third-party registrants, the distribution is quite concentrated with the top 20 third parties owning 12.9 percent of all third-party registered names.

By far the most common use of third-party registrations is for pay-per-click

sites, with 34 percent of all third-party sites analyzed in the study resolving to a pay-per-click site. Pay-per-click is an advertising model that utilizes websites and search engines where advertisers only pay when a user actually clicks on an ad to visit the advertiser's website. They typically take one of two forms: 'keyword' or 'content match'. Keyword matches are based on purchasing specific words, while content matches are more contextual. Keyword matches are often displayed on search engine results pages, while content match ads appear beside relevant content on site pages.

Advertisers will bid on keywords they believe their target customers would input into a search engine when looking for a particular product or service. The list of advertiser sites that result from such a search are usually ordered in proportion to the amount each advertiser pays for the 'click'.

Certain industries are much more prone to domain infringement than others. The most commonly infringed brands are in the telecoms equipment, computer software, banking/financial and consumer electronics industries.

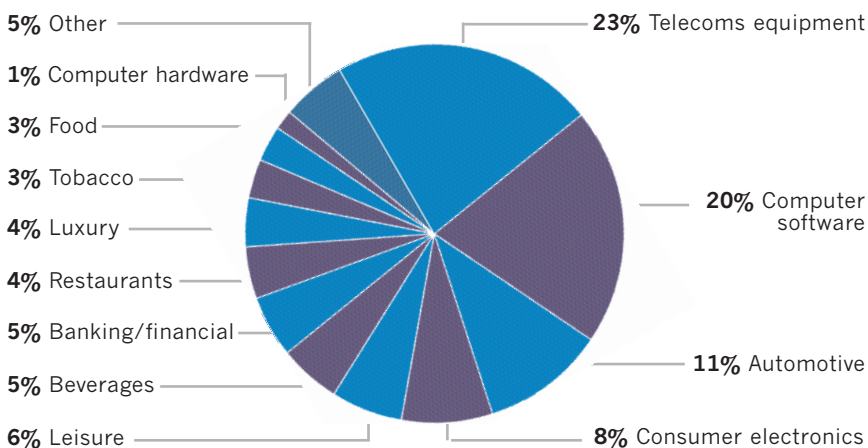
USING NAME VARIATIONS

For a long time the most common – and simplest – form of domain name infringement was the registration of misspellings of company names or corporate websites that are very close to the real name. Up to this point the most common misspellings revolved around variations of vowels or strings of vowels. The use of consonant variants is starting to emerge and is something companies should keep a close eye on.

With new releases of internet browsers, new techniques for registering domain name variants are becoming available. Until recently the vast majority of websites and domain names used ASCII (American standard code for information exchange) characters, which are based on the English alphabet. Examples include `bücher.de` and `egov.go.kr`. It is now possible to use non-ASCII characters, many of which look similar to traditional English letters. This is one of the major areas where companies are not keeping pace with change.

A recent study by CSC finds that 22 percent of the top 100 brands have been infringed by users registering .com variations replacing English characters with foreign characters. Many of these involved multiple infringements for the same brand.

Breakdown of most-favored pay-per-click industries



Note: all figures are rounded to the nearest whole number

Source: CSC

OFFLINE, NOT OFF THE HOOK

Many companies that do not directly conduct business online believe they are insulated from the risks of the internet. But this is not the case.

A study from iCrossing/Harris Interactive finds that 88 percent of people have researched products online which they later purchased offline. A Cyber Dialogue study shows an estimated 10.3 million Americans have changed their mind about financial service brands after reviewing information online.

So what types of issues should corporate legal teams be looking out for in the online world? When assessing the range of potential infringements, it is crucial to remember the internet is made up of more than domain names. Also consider other mechanisms including chatrooms and messages boards, auction sites, email, instant messaging, file sharing networks and hidden web page text.

Elements of risk

The internet is undoubtedly one of the most powerful marketing and communications tools available to corporations. But alongside the potential branding benefits come a wide range of legal and compliance challenges which are of particular importance to governance, legal and IT executives.

Corporate domain names and brands are open to misuse, trademarks can be infringed and customer privacy can be violated through complicated scams. Legal teams need to work in unison with marketing and IT professionals to formulate systems to monitor and police any damaging activity that could be taking place on the internet.

Serious consequences

Left unchecked, online brand infringement can have a significant impact on a company's reputation and its ability to effectively market and sell products. Some of the most common impacts include: lost sales and revenues; diverted customers; tarnished brand equity; weakened or unenforceable trademark rights; limited pricing power; and a loss of brand trust. Legal teams need to ask themselves: What obligations do I have to proactively police the internet for abuse? How are my brands being misused in the online environment? And how can I be proactive about monitoring online abuse without being overwhelmed with data?

The global, anonymous nature of the internet makes understanding and detecting abuse extremely difficult. Criminals, disgruntled employees, upset consumers and even overzealous competitors are free to post almost anything online from anywhere in the world.

The oldest and most well known form of online brand infringement is direct domain name abuse. Many people are aware of this because of the very prominent 'cybersquatting' cases. Most recently, companies like MySpace, the BBC and Victoria's Secret have won battles contesting domain names. Despite the relatively robust legal protections that have been enacted, this form of violation continues to increase every year. As of June 2007 the Internet Corporation for Assigned Names and Numbers (ICANN) reports that it has handled 11,249 cases involving 19,573 domain names since 1999.

The severity of domain name infringement depends largely on the type of content associated with the infringing site. This can range from inactive pages to potentially offensive material such as pornography.

Traffic diversion is another common infringement and is constantly evolving and changing. Though it can take several forms, the basic theme involves leveraging the name recognition of a particular brand so as to drive traffic to a third-party site.

This type of infringement is profitable because unsuspecting users are redirected to a different website that can feature pop-up advertisements from competing companies or, in some cases, users are even redirected right to a competitor's site. Other traffic diversion pages may attempt to capture credit card details or other sensitive information from unsuspecting users who believe that they are accessing a trusted site. In some cases the squatter may also attempt to profit by selling the site back to the brand name owner.

The dirty dozen

12 areas of infringement remain the key methods used in online attacks

- 1 Domain name abuse
- 2 Traffic diversion
- 3 Trademark infringement
- 4 Trademark dilution
- 5 Offensive content
- 6 Brand disparagement/feedback
- 7 Claimed affiliations
- 8 Affiliate/partner compliance
- 9 Unlicensed/unauthorized sales
- 10 Product counterfeiting
- 11 Digital piracy
- 12 Identity theft & fraud

Source: CSC

One form of diversion still little understood by many companies is the practice of linking search results to pay-for-placement banner and pop-up ads, which are often triggered by keywords linked to trademarks. Competitors can apply these tactics to your brand, or protesters can try to dissuade users from purchasing your products.

Apart from diversionary tactics, straightforward trademark theft, where individuals and companies create marks deceptively similar to registered trademarks, is still an extremely prevalent activity on the internet.

Alan Greenspan, a media and IP attorney at Jackson Walker, provided a cautionary warning in a September 2006 interview: 'For some reason, the world is of the opinion that if you can find it on the internet, it's yours to do whatever you want with. People would never imagine a situation where a cus-

tomers would come in and steal things off somebody's desk but that is exactly what is happening on the internet all the time.'

He went on to say that 'many companies do not have a good handle on their intellectual property and some have even failed to properly register trademarks and copyrights.'

Apart from the obvious problems associated with trademark theft, dilution is also a concern that needs to be attended to just as closely. With trademark dilution, abuse can occur even in the absence of consumer confusion. Using easily identifiable trademarks without permission or in a generic manner and altering text or other elements to convey a usually negative message can weaken brand equity and potentially impact brand reputation.

Many of the traffic diversion and infringement techniques that have been described in this chapter were pioneered by the online pornography business. That industry remains one of the foremost perpetrators of online brand infringement. In fact, these practices are so common that every company should automatically assume that its brand names are being used to direct users to pornographic content, and should therefore monitor accordingly.

Monitoring of official third-party relationships is also vital to a company's reputation. When working with affiliates there is a loss of control of information and it is easy for out-of-date pricing or specs to be released. Constant monitoring can help to prevent inadvertent brand damage but there is a larger problem: substandard customer service or illegal behavior by affiliates can cast a pall over a legitimate company's business. As unfair as it may be, many an honest company has fallen afoul through guilt by association, from both a legal viewpoint and a moral one.

BAD CAN BE GOOD

Corporations should also be aware of the reputational dangers caused by brand disparagement and negative feedback or reviews. The internet is riddled with chatrooms and forums in which people exchange ideas and comments. Anyone can choose to launch a campaign against a particular brand or company. These can spread remarkably quickly and the effects can last for years.

Utilizing the same forums can also be beneficial for companies using them as non-biased focus groups. It can be a very effective method to gain real feedback from customers about their thoughts on products.

Some companies may seek to boost their own reputation or attract users to their products by claiming a close relationship or affiliation that does not exist. That said, strategic affiliations can be a powerful tool. But when used by unlicensed companies they can damage corporate reputation and impact revenues.

BEING RIGHT IS NOT ALWAYS ENOUGH

Sometimes doing nothing can be the very best solution. There are occasions where a third party infringes a brand and profits from it but taking action against that group would damage your reputation.

In an August 2007 suit, Johnson & Johnson took action against the American Red Cross, seeking to enjoin it from licensing the 'red cross' emblem on some of its products, as well as to surrender to Johnson & Johnson all licensed products for destruction. The suit is also seeking punitive damages from the Red Cross.

While Johnson & Johnson may lay claim to the legal rights of the emblem, the suit is attracting considerable negative attention from members of the public and media. Red Cross president Mark Everson remarked, 'For a multibillion-dollar drug company to claim that the Red Cross violated a criminal statute that was created to protect the humanitarian mission of the Red Cross, simply so that Johnson & Johnson can make more money, is obscene.'

This is one situation where the potential benefit may be outweighed by the negative impact on reputation.

The solution

As we have seen, there are a vast array of ways a corporate brand, trademark, copyright or reputation can be infringed in the online environment. The internet is constantly evolving and as some internet risks diminish, others supplant them. It may seem like an overwhelming situation but there are many tools available to corporate legal teams working hard to protect intellectual property.

Possibly the single greatest obstacle to effectively monitoring and policing a company brand is not the infringers but a lack of knowledge and understanding by corporations themselves. Very few in-house counsel and corporate secretary teams are aware of the range of possible threats to intellectual property. In fact, many are even unaware of the breadth of their own company's intellectual property assets.

Greenspan recommends that companies conduct an audit to identify their intellectual property assets and then implement a program to protect them: 'Most companies nowadays have security so that people can't wander through their physical site and see what is going on. The same types of precautions must be taken to protect intellectual property assets.' Further to this, he points out that the Sarbanes-Oxley Act's internal control requirements apply to IP assets as well as to 'hard assets'. Thus management has a fiduciary responsibility to take the necessary steps to detect and prevent IP infringement.

So where should the company start in its efforts to police the internet? Frances Zollers, professor of law and public policy at Syracuse University's Whitman School of Management, explains that

detecting online brand infringement doesn't have to be complicated. 'Google your name. Imagine a couple of spelling variations and google those too.'

That type of one-off testing may be a good place to start but it is not a viable long-term strategy. For any large company, such a method would not capture anywhere near all the potential sources of brand or domain infringement.

In order to have any hope of effectively unearthing all potential problems, a company needs a unified strategy. This requires involvement not only by the legal and secretariat teams but also by the IT, marketing, HR, compliance and governance and PR teams.

Malia Horine of NameProtect (now part of CSC), expands on the challenge: 'Even large corporations don't have massive resources to implement policing and ongoing enforcement efforts to protect everything that happens to their brand online.'

She underscores that statement in saying that 'with the internet you are not just talking about the web... you're dealing with things like blogs, auctions sites and chatrooms. There are different aspects of the internet that can affect your brand, so you need to keep a broad picture in mind as well.'

After performing an IP audit, the next step is to identify the most pressing issues and sort those out as part of an overall strategy.

Targeting vulnerabilities

Any monitoring and protection policy must be borne out of an understanding of how potential infringements affect the value of the brand as well as the probability of infringement occurring.

Infringers generally falls into two categories: those who wish to tarnish the reputation of others and those who are looking to profit off the established goodwill of other companies.

The real value of monitoring lies in the ability of brand owners to quickly identify, quantify, prioritize and counter infringements on a case-by-case basis. A methodical way of classifying and handling infringements can also reduce the time spent processing cases internally.

There are a large number of domains a company might seek to register to eliminate threats, especially where the probability or cost is high. By understanding infringing activity through analyzing data sets, a company can begin to predict which variants of brands are most prone to infringements.

There are, however, a vast number of permutations in many countries that would be prohibitively expensive to register. For instance, for a six character brand there are 100 million typo variations across the 750 domain extensions. In this instance a monitoring and action plan is more appropriate.

The complicated part comes when assessing what to do with offenders when they are discovered. When taking legal action it is important to understand the complicated nature of trademark infringement law. John Plumpe, principal at CRA International, explains: 'It can be difficult sometimes for a plaintiff to demonstrate what they have lost, but it can be easy for them to show what the defendant has gained.'

The most important situations are probably those that involve direct fraud, counterfeiting or theft. The law relating to these areas is well-tested and there are a range of protections available. In other areas it is far less clear what avenues are available to the company.

There are some situations where even though there is a clear legal infringement it is better to take no action at all. If there is little to no damage to the brand, then taking legal action against an individual or group that may be perceived publicly as sympathetic could do more harm to a company's reputation than taking no action (see Johnson & Johnson v Red Cross sidebar, page vi).

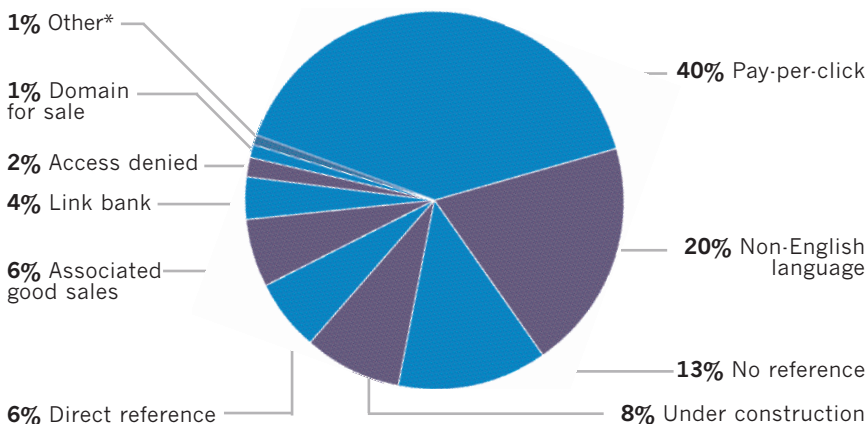
ERASE ERRATA

The starting point of any campaign is the same: detection of the infringement. Currently, one of the most effective tools for detecting potential brand infringement is web crawling. This can take one of two types: targeted crawling, looking for specific names or combinations of names, or random crawls. Random crawls gather information across the internet for further analysis.

Crawling tools should target all areas of the web including domains, auction sites, blogs, news and general web content. A web crawl for even a small number of keywords or phrases is likely to return a huge amount of data. This is where more advanced technology can come into its own. The use of an intelligent analysis filter that sifts through the results of the crawl and sorts the actionable from the non-actionable will save considerable time and money.

Ideally, any technology used in such a fashion will be web-based. This removes the need for expensive software and the IT department does not have to load software or perform expensive maintenance. One other significant advantage to a web-based crawling and analysis system is that it can be accessed and used from almost anywhere at any time.

Third-party registrant web content



* Other includes: Adult content, negative reference

Note: all figures are rounded to the nearest whole number

Source: CSC

By any other name

Once a brand is developed it is important that a plan is formulated to protect that brand all the way through from its creation to its full maturation. And in doing so, a company must evaluate a large number of elements.

Some of the first questions companies should concern themselves with involve identifying the areas in which the company should trademark the brand name and the risks and costs associated with doing so. In some cases, the name may not even be available. Being equipped with this knowledge can prevent a costly legal battle down the road. A thorough trademark clearance process – including researching the proposed name, getting a legal opinion on its availability and applying for a trademark registration – secures the naming rights and the legal benefits accorded by those rights during both the brand monitoring and enforcement process.

Extensive research needs to be conducted and should be considered an integral component of the monitoring process. In today's global economy, it is important to compile information about the various regulatory environments in which the company operates. This will allow the formulation of brand protection strategies across all key markets and countries.

Monitoring pay-per-click sites (the most prevalent form of infringement) will give companies a very good indication of the latest infringement trends and provide at least some insight into which areas monitoring and protection strategies should be focused on.

It is important that output from monitoring activities is presented in a format that allows it to be applied to a broad range of operations and departments. The legal and secretariat teams will need to submit information to various internal teams, which will often

necessitate translations to accommodate for differing formats. By correctly structuring the outputs, identifying the actionable from the non-actionable, deciding what to do becomes a great deal easier.

Being able to automatically format outputs into some of the more commonly used forms will ease policing efforts. For example, there is a standard form to request removal of names or products from auction sites. Many litigation papers and government filings also have standard formats that should be accommodated by a monitoring tool.

The most important aspect of any effective brand monitoring process is to take a unified and strategic approach that includes all major corporate departments and is easily understood and distributed. With this foundation, a company can help to establish its brand and protect it from online abuse.

CORPORATE SECRETARY WOULD LIKE TO THANK OUR RESEARCH PARTNER

FOR MORE INFORMATION



CORPORATION SERVICE COMPANY[®]



Address: 2711 Centerville Road,
Suite 400, Wilmington, DE 19808



Phone: 800-927-9800



Web: www.incspot.com

Corporation Service Company[®] is a leading provider of legal and financial services for large companies, law firms and financial institutions worldwide. Founded in 1899, CSC[®] offers clients integrated services in the areas of compliance and governance, entity management, litigation and matter management, public record document and retrieval, uniform commercial code, trademarks, domain names and brand monitoring, motor vehicle titling and registered agent. CSC is the only trusted partner that combines proprietary technology, intellectual property and internet expertise to offer trademark, domain name and brand monitoring solutions to reduce cost and risk.

CSC is pleased to announce exciting free online learning opportunities for those interested in trademark, domain name and brand issues: CSC Trademarks Web Seminar Series and INTA[®] .ASIA Live Webcast. To register or learn more about these seminars, visit the 'Education at CSC' website at <http://cscinfo.webex.com> and <http://cscevents.webex.com>.