

Do you know where your domain names are?

Managing and monitoring domain names can be a bewildering task, but doing so is vital to guard against trademark infringement and dilution, and to promote the brand worldwide. Having the right policies and procedures in place can make the task a little easier

By **Jeffrey Van Hoosear**, Knobbe Martens Olson & Bear

The Bush Library Foundation may or may not know the location of the domain name www.GeorgeWBushLibrary.com. It paid US\$3,000 to obtain it from an individual who had registered the name first. At the time of purchase, the domain name was set to expire in a few months. Apparently, there was confusion as to who was to renew the domain name and it was allowed to expire. An “enterprising” website development company saw the expiration notice and purchased the domain for less than US\$10. The Bush Library Foundation then bought the domain name again for US\$35,000. The failure to register or properly maintain important domain names can have significant consequences, as the Bush Library learned the hard way.

This article outlines a strategy to assist companies in deciding why, what, where, when and how to register and manage domain names. Currently, there are approximately 250 country-code top-level domains (ccTLDs) and another 50 generic top-level domains (gTLDs). To complicate the process further, the Internet Corporation for Assigned Names and Numbers (ICANN) approved a new programme last year which will allow

companies to reserve their own specific gTLD. For example, Apple could apply for “.apple” or “.mac”, Starbucks for “.starbucks” or “.coffee”, and the city of Seattle for “.Seattle”. The increasingly large number of domain name venues can create a registration and management nightmare for any company.

A company often registers and manages its domain names the same way that it manages its trademarks and service marks. This is often a mistake, since there are different considerations when registering and maintaining domain names. First, the laws and regulations regarding domain names tend to change more often, and more quickly, than trademark laws. Staying on top of these changes requires a higher level of involvement than trademark maintenance and can be time consuming. Second, the time and cost to register a domain name are usually far less than the time and cost required to register a trademark. It is cheap and easy for both a company to register a legitimate domain name and a cyber-squatter to register an infringing domain name. A company will clearly want to consider registering domain names that go beyond its usual trademark filings.

To create and manage a domain name portfolio successfully, a company should:

- Determine the primary domain name objective for registration.
- Establish policies for the selection, registration and maintenance of domains.
- Develop a procedure for domain monitoring.

Determine the company’s objectives

Knowing the company’s primary objectives is essential to setting up an effective domain name management plan. Registering

every possible domain in every country is neither practical nor probably even possible. As a starting point in determining what domain names to register, a company should determine whether its primary objective is to protect or promote itself. Companies primarily concerned about trademark infringement or dilution of their brand by others should consider registering with the primary gTLDs (.com, .net and .org), as well as certain ccTLDs that have no, or minimal, restrictions for registration (.us, .de and .eu), to prevent third parties from doing so.

In the United States, the .com gTLD is by far the most sought-after extension and most global companies seek it as their primary domain address. In much of the world, however, companies use ccTLDs as their primary domain address. As of 2008, the top five gTLDs are .com, .cn, .de, .net and org. Of the approximately 180 million domain names currently registered, over 80 million are ccTLDs, which represents approximately 50% of all domain registrations. Unfortunately, the increased popularity and availability of ccTLDs have also led to an increase in bad-faith registrations of protected trademarks. Because the administrator of each ccTLD establishes its own policy for applying for and managing the addresses within its proprietary domain, trademark owners often have a difficult time enforcing their rights. Accordingly, it is far better to obtain a ccTLD where possible, rather than attempt to acquire it from another later.

Countries are also constantly changing the ccTLD registration rules and a significant number of restrictions to ccTLD registrations have been removed. An additional problem is that out of the approximately 250 ccTLDs available, less than 50% have publicly available registration rules and less than 50% have a Whois service. Consequently, there is a need to monitor continually ccTLD registry changes. Two companies that help to monitor these changes are MarkMonitor and VeriSign. If a company uses a service to help monitor ccTLDs, it may also want to make sure that the service can provide complete ccTLD capabilities, such as local presence services and local contact services. This makes it easier for the company to qualify for registration. For example, the .de registration requires a local postal residence and not just a post-office box address.

After a company has identified the gTLDs and ccTLDs that will protect its brands, it should also register those domain names that are likely infringement targets for its brands. It should consider registering

domain name variations which use a hyphen, and the singular or plural terms. For example, *IP Magazine* may want to consider registering the domain names “www.IP-Magazine.com” and “www.IP-Magazines.com”, even though it would not register those names as trademarks. In addition, a company should consider registering abbreviations or common misspellings (eg, “www.IPZine.com” and “www.IPMagazine.com”) as domain names. Finally, a company should consider registering the names of well-known officers, directors or spokespersons (eg, www.billgates.com), to maintain full control and protection over the brand.

While brand protection is certainly an admirable goal, many companies are also concerned with promotion. A company may decide that greater internet exposure will increase its revenue and thus develop a completely different registration strategy. To maximise its exposure, the company might register domain names in countries with significant actual or potential commerce, or where this would benefit local sales or marketing efforts. The company would register in all the top “traditional” commerce countries (which may be different for different industries, but for this example would be .ar, .au, .br, .ca, .cn, .de, .eu, .jp, .kr, .ru, .tw, .uk and .us), and the top “e-commerce” countries (eg, .br, .ca, .co.mx, .co.uk, .de and .jp — and of course, there is some overlap between these two types of commerce). The domains would not be trademark or brand specific, but would be product (or service) oriented. For example, an apparel company would include its trademark brand plus the terms “apparel”, “swimwear”, “denim” or “footwear”. An insurance company would include words such as “insurance”, “annuity” or “retirement”, along with its company name or trademark.

Whether the strategy is to protect or promote, or a combination of both, a company should also keep a list of domain names to be registered in the event that new gTLDs or ccTLDs become available, as they often do with little notice. In addition, it should keep a list of additional geographical regions (ccTLDs) in which it may want to register a domain name, but cannot due to current restrictions.

Establish domain name policies

The first step in setting up an effective domain name programme is to know all of the domain names owned by a company and consolidate them to a single location for maintenance and monitoring. This is often

difficult, as most companies have many departments, divisions, groups or subsidiaries that have registered domain names at different times. Reverse Whois tools can search for any term within a record, including company, contact name, address, server and email address, and can help a company to locate all of its domain names. A company should also audit key departments and personnel, such as marketing, sales and legal, to check for domain registrations.

A company should review the entire portfolio for accuracy and consistency, and consider consolidating all domains with a single registrar with one primary company contact. If there are any inaccuracies or inconsistencies, changes should be made as soon as possible to meet all ICANN or other registration requirements. It is important to remember that false or inaccurate information is often a legitimate basis to challenge a domain registration. A company should conduct annual audits to review its domain names and to confirm the accuracy of all information. At the same time, the company should review its existing or potential brands, and identify any action that needs to be taken as to the portfolio.

As domain name laws and regulations can change with little or no notice, it is important to have policies and procedures in place regarding who can register domain names and how they will be registered and maintained. It is especially important to determine an appropriate administrative contact. An administrative contact is required in most applications and also appears in the ownership information. This contact is generally the recipient of important notices regarding transfers, renewals and expirations. Problems often arise if an employee is listed as the contact, and then leaves the company, or if his email account is deactivated or not monitored. Setting up a company email such as `admincontact@yourcompany.com` can avoid many problems and ensure that at least one person is always available to review and respond to important messages. In addition to setting up an administrative contact, it is prudent to have a consistent policy as to who will be listed as “registrant”, “technical contact” and “billing contact” in the domain name registrations.

Another critical decision concerns who is allowed to approve or renew new domain names. If more than one person has the ability to make changes or decide maintenance issues, the company should establish a central point of contact to review and approve all such actions for purposes of

consistency and budget. The central contact can be someone in management, in-house or outside legal counsel, or a reputable independent company specialising in domain management.

In every domain name portfolio, some domain names are more important than others. For example, a domain name that serves as a corporate home page or an e-commerce website is probably more important to the company than domain names registered defensively to protect against cybersquatting or misspellings. The most important domain names should always be registered for the maximum allowable terms; for gTLDs, this is 10 years. They should also be set up for automatic renewal and locked at the registry to prevent domain name hijacking or unauthorised transfers.

Develop a procedure to monitor domain names

The easiest way to monitor domain names is to hire a company such as MarkMonitor or VeriSign to conduct regular searches looking for new domain names that contain a particular term, such as prominent or distinctive portions of a company’s name or brand. Important features of any domain name monitoring service include notification of all newly registered or expired domain names that contain the particular terms of interest; and the ability to conduct searches using exclusions (to help filter) as well as “wildcards” (to help search misspellings or variations). The service should also provide a link to each active website, as well as a link to the Whois record for each domain name provided in the search results.

Monitoring domain name registrations allows a company to take swift action against potential infringers. It has several options:

- Continue monitoring the domain name and the corresponding website.
- Send the domain name registrant a cease and desist letter.
- File a complaint with ICANN under its Uniform Dispute Resolution Policy (UDRP).
- File an infringement action in court.

Mistakes can happen in even the best-managed domain name portfolios and a domain name may inadvertently be allowed to lapse. Monitoring should alert you to any such lapse and allow you to take immediate action.

Some domain names may need to be acquired (or re-acquired) as soon as possible. Recently, a well-known technology

company discovered that an important ccTLD was not obtained during the appropriate period. To avoid embarrassing publicity, it decided to reacquire the domain name via an anonymous acquisition, rather than by a public legal proceeding. In using a third party, the domain name was re-acquired quite quickly, for a few thousand dollars and with no publicity.

If time is not of the essence, a company can monitor the domain name's expiration date and subscribe to a back order service, which places an order to register the domain name if it expires or lapses. This approach is useful only if the domain name is not essential, as it could take several years for the term of the domain name to expire.

One of the best traditional approaches for acquiring domain names that are identical or confusingly similar to a company's trademark is to file a UDRP complaint with ICANN. UDRP fees and costs typically range between US\$10,000 and US\$15,000, and a decision is issued in about two months. A large number of respondents default and approximately 80% of the decisions are in favour of the petitioner.

However, UDRP proceedings apply only

to gTLDs and only about 25% of ccTLDs have a similar resolution policy. The only recourse that a company may have in some situations is to file a legal action to recover a domain name. In the United States, the Anti-Cybersquatting Protection Act is designed to prohibit attempts to take financial advantage of another's trademark. It provides for temporary restraining orders, statutory damages of US\$1,000 to US\$100,000 per infringing domain name, and attorneys' fees and costs. Unfortunately, there is not an equivalent law in most of the ccTLD jurisdictions. A trademark owner seeking to recover a domain name will need to rely on local legal authorities as to what, if any, options are available.

Conclusion

Managing domain name portfolios will never be a simple task. However, it is not too difficult to set up the policies and procedures set forth above. Proper domain name management is critical to protect against trademark infringement and dilution, as well as to promote the brand to a global market. **iam**



Jeffrey Van Hoosear is a partner at Knobbe Martens Olson & Bear's Orange County office and specialises in international trademark and unfair competition matters. In 2006 and 2007, based on a survey of his peers, he was nominated as one of the World's Leading Trademark Practitioners by *Who's Who Legal*. Mr Van Hoosear has spoken extensively in the field of trademark and copyright law, and authored numerous articles on trademark issues for different IP-related publications.

Jeffrey Van Hoosear
Partner
jvanhoosear@kmob.com
+1 949 721 5274

Knobbe Martens Olson & Bear
United States
www.kmob.com