Bloomberg BNA

Electronic Commerce & Law Report™

VOL. 21, NO. 1 JANUARY 6, 2016

NEW TOP-LEVEL DOMAINS

The expansion of the domain name space has amplified the importance of online brand protection. Attorneys from Tucker Ellis discuss how to identify, solve and strategize for the legal and business problems that can arise in this area.

Strategies and Best Practices for Resolving Domain Name Problems

BY DAVID J. STEELE AND MARKUS HOPKINS

In today's global economy, consumers turn to the Internet to find and purchase goods and services, and to interact with companies. In the same way that the Internet has changed how business is transacted, the Internet has changed the ways businesses are taken advantage of and how brands are infringed. Businesses, and their legal counsel, face a myriad of legal and non-legal issues arising from domain names.

David J. Steele (david.steele@tuckerellis.com) is a partner in the Intellectual Property and Brand Protection Group at Tucker Ellis LLP. He specializes in trademark and Internet law, and focuses much of his time protecting famous and well-known trademarks from infringement of all types, especially online infringement. Markus B. Hopkins (markus.hopkins@tuckerellis.com) is an associate in the Intellectual Property and Brand Protection Group at Tucker Ellis LLP.

This article will provide an overview of current domain name related problems, including cybersquatting[1], the recent addition of new top level domain names to the Internet and domain name portfolio management. The article will also discuss available steps that companies can take to assess these issues, and to develop and implement practical and effective domain name strategies to remedy problems.

Overview of Domain Name Issues

Domain names typically represent the largest issue that companies face on the Internet because of the number of new domain name registrations that occur every day (100,000+ domain names) and because of the harm that arises from the unlawful registration and use of domain names.

[1] Cybersquatting is the registration, trafficking in, or using an Internet domain name that is identical or confusingly similar to a trademark with the bad faith intent to profit from the trademark. 15 U.S.C. § 1125(d).

 ISSN 1098-5190

Generally, the most common problem results from cybersquatting. Common cybersquatting cases involve the registration and use of a domain name to sell counterfeit goods, to host advertising (often a ''parking page'' that displays links to goods or services), or to engage in affiliate fraud.

Other times, the domain names are used in phishing[2] scams or to impersonate the company.

Infringing domain names often include a misspelling or mistyping of the trademark (i.e., a letter is omitted from, or added to the mark, or an adjacent letter on the keyboard is substituted e.g., famoussbrand.com, or famosbrand.com). Infringing domain names can also contain a word or phrase that is descriptive of the good or service offered under the brand (e.g., famouscoffeebrand-latte.com, or outlet-clothingbrand.com).

Classic cybersquatting problems typically involve hosting a parking page that displays links and/or advertisements to goods or services. For example, an infringing domain name that is similar to a computer company's trademark may display links and/or ads to the company's own webpage, along with links to other competitive brands.

The cybersquatter's goal is to lure consumers to click one of the links, thereby creating revenue (directly or indirectly) for the cybersquatter. Ultimately, online advertisers shoulder the cost for this type of harm. Sometimes the brand owner agrees to pay online advertising companies to direct consumers searching for their own brand or product to their website.

Some cybersquatters register and use infringing domain names for affiliate fraud. Here, the cybersquatter signs up with the company (or an affiliate network) to direct consumers to a brand owner's page for a referral fee. Then the cybersquatter registers an infringing domain name and simply redirects consumers to the company's actual website and earns revenue from the redirection.[3] In some affiliate fraud cases, the consumers never even noticed the redirection.

Cybersquatting problems, which use a domain name for counterfeiting or to impersonate the company, are significantly more harmful. The hosted websites can look so legitimate it is difficult for consumers to realize the website is not operated by the trademark owner.

When combined with a confusingly similar domain name, counterfeit websites are extremely difficult to detect and are very effective tools for criminals. Consumers who are duped into ordering from a counterfeit website *may* receive counterfeit goods (or may not); more importantly they have disclosed their personal information, including credit card information, to criminals. Even worse for the targeted company is that their customer will directly associate this fraud with the company they thought they were dealing with.

While the above types of problems are the most common, there is a never-ending list of problems. There is a constantly evolving cat-and-mouse game that exists on the Internet. Just when you think you've seen it all, the next new thing rears its ugly head. And that is the perfect transition to the next topic, the rapidly changing landscape of the domain name system and the addition of new top-level domain names.

In 2014, after a lengthy process, The Internet Corporation for Assigned Names and Numbers (''ICANN'') began introducing new top level domain names (''TLD'') to the Internet.[4] As of December 2015, over 700 new TLDs have been added to the Internet, with several hundred more scheduled for addition over the next year or two. Some examples of new TLDs include .berlin, .cars, .company, .deals, .photo, .sucks, .web, .xyz, to list only a very few examples.

These new TLDs present significant risks as well as opportunities for companies. Each time new TLDs have been added to the Internet, nefarious individuals have taken advantage by cybersquatting on trademarks. Accordingly, companies should be concerned about cybersquatting on their trademark in these new TLDs, and should consider preemptively registering, at a minimum, domain names that are identical or confusingly similar to their trademark in TLDs and which are directly related to their field.

In order to help companies protect their marks in these new TLDs, ICANN introduced two new protections for trademark owners in connection with the introduction of new TLDs.

The first protection is the creation of a trademark clearinghouse (''TMCH''), which allows the owners of trademarks verified by the TMCH to register domain names corresponding to the trademark during preregistration periods (aka ''Sunrise Periods''). Trademark holders in the TMCH will also have the option to be notified when someone else registers a domain name that matches their record in the TMCH.

The TMCH is currently accepting submissions and will remain open indefinitely. Because of the benefits provided under the TMCH, it is strongly recommend that companies with registered trademarks consider registering their trademarks in the TMCH as soon as possible.

The second protection is an additional dispute mechanism named the Uniform Rapid Suspension System (''URS''). The URS is intended to provide a faster and less expensive mechanism than the existing Uniform Domain-Name Dispute-Resolution Policy (''UDRP''). Unlike the UDRP, the URS only permits a trademark owner to deactivate an infringing domain name, not to force its transfer or deletion.

[2] Phishing involves the collection of sensitive information (usernames, passwords, credit card details, etc.) by impersonating a trustworthy entity.

[3] Most affiliate advertising agreements prohibit this type of conduct.

[4] *See New Generic Top-Level Domains: New gTLD Basics; New Internet Extensions*, available at http://archive.icann.org/en/topics/new-gtlds/basics-new-extensions-21jul11-en.pdf (last visited Dec. 12, 2015).

  ECLR ISSN 1098-5190

The URS typically only takes a few days from start to finish, thereby providing the ability to have domain names ''turned off'' without having to go to court. Thereafter, the trademark owner could proceed with a UDRP or a court action to recover the domain name.

Also of note is that the URS has a higher standard of proof—clear and convincing evidence—than the UDRP's preponderance of the evidence Also, the URS is only applicable to disputes with any of the new TLDs (not legacy TLDs like .com, .net).

Taken together, these protections provide brand owners tools to prevent and remedy infringement in the new TLDs. However, the number of new TLDs being added each week is proving to be very difficult to handle for even the best prepared trademark owners. Therefore, companies are well advised to develop and implement an appropriate strategy for addressing new TLDs.

Learning About Domain Name Problems

Likely the hardest part of dealing with domain name problems is getting your arms around the landscape. The domain name system, and related legal issues and remedies, are awash in acronyms and technical jargon.

If that wasn't challenging enough, the landscape is rapidly changing. But getting up to speed and keeping abreast of changes will pay dividends over time. The International Trademark Association (''INTA'') offers a number of resources, and attending either its annual meeting or one of the INTA's various educational sessions is worth the effort. Similarly, attending an ICANN meeting, whether in-person or remotely, is also helpful.

The most common source of information about domain name problems that might affect a company is from professional domain name reports. Several commercial companies (e.g., Thompson Compumark, MarkMonitor and Domain Tools), and a few law firms that specialize in domain name matters, offer reporting services. The services offered vary widely.

Some reporting services are limited to legacy TLDs like .com and .net. Other reporting services offer searching of all new TLDs, while some include country code TLDs (''ccTLDs'') like .co.uk. Most standard reporting products are limited to newly registered or newly deleted domain names, while some reporting services offer comprehensive reports, which include all currently registered domain names.

Companies should periodically obtain a comprehensive domain name report that details any and all possible infringement. These comprehensive reports serve as a starting point for locating infringement. Additionally, companies should also subscribe to one or more daily or weekly domain name reporting services to detect any newly registered or newly deleted domain names.

Another source of information about domain name problems will likely come from within the company; either directly from employees or from outside sources such as customers or family members, but which are reported to employees.

It is important that appropriate company policies exist to ensure this information is communicated to the proper domain name administrator or to a member of the legal department. Lastly, periodic Internet searches should also be conducted to detect any domain names that may have slipped by the professional searches.

Solving Enforcement Problems

The first step in resolving a domain name infringement matter is to promptly make a record of any and all relevant facts. Often with Internet-related infringement, the facts change between discovery of the matter and taking action. Servers containing multiple infringing websites are often taken down by service providers when any impacted party complains, and this may result in content affecting other parties being removed.

Additionally, bad actors may lose service for other reasons such as technical difficulty, failure to pay their bills, or a change in strategy. Do not wait until a decision on whether or how to proceed is reached; it is very important to create a record of the facts as soon as possible.

At a minimum, screen captures of every example of problematic content should be created to preserve information, such as the date they were created and where the captured content is located. If the contents of a website can be used as evidence in litigation, the website should also be recorded through a trusted third-party such as archive.org. Ownership information, or ''whois data,'' should also be preserved.

This information is obtainable using a number of third-party sources such as domaintools.com[5], or directly from the registry/registrar for the subject domain name. In addition to whois data, web server hosting information is also useful to determine what activities occur at a given location on the Internet, or to determine what country the website is hosted in, which often impacts the available remedies.

The collected information may include the number or nature of other websites hosted on the same server and what else the server is used for, such as sending e-mail (i.e. for spam or phishing attacks). Much of this information is available through direct querying, or through third-party information sources. Finally, until the matter is finally resolved, periodic monitoring of the domain name for any changes in ownership or use is an important component of preserving all relevant information.

There are a number of available legal and non-legal tools that may be used to remedy cybersquatting. Common tools can include a phone call or simple mail to the registrant, cease and desist letters, takedown notices with website hosting companies, filing administrative actions under the TLDs' respective dispute policies (e.g., the Uniform Dispute Resolution Policy (''UDRP'') for .com, .net, and a number of other TLDs), and even filing lawsuits under the United States Anticybersquatting Consumer Protection Act (''ACPA'').

While each tool has its advantages and disadvantages, such as cost versus speed, effectiveness, etc., the location of the registrant or TLD where a domain name is registered may limit the availability or practicality of a specific tool, or may enhance a tool's effectiveness.

For example, registrants in the United States, who are subject to personal jurisdiction, are more likely to respond to a cease and desist letter than Chinese registrants who are not subject to personal jurisdiction in the

[5] Domaintools.com also offers, for subscribers, a wealth of other useful information, including reverse whois data (used to learn what other domain names a registrant currently owns as well as historic data), detailed information about the hosting server, and other relevant information.

United States. Taking the relevant factors into consideration (i.e., locations, number of domain names owned by the registrant, applicable dispute policies, and which tools are likely to be effective, etc.), it is possible to optimize the domain name's recovery within appropriate budget constraints.

A telephone call or short mail from in-house counsel may be effective with unsophisticated registrants (someone who is unaware that they shouldn't register the domain name). Slightly more impactful are cease and desist letters. Cease and desist letters are often an effective tool when the severity of the infringement or the matter's priority is low, the registrant owns only one or two domain names, and the identity and location of the registrant is known.

Where a cease and desist letter is not feasible, or the severity of the unlawful activity requires a more certain and prompt outcome, one or more administrative proceedings may be a better tool.

As discussed above, each TLD utilizes one or more administrative dispute policies for resolving trademark infringement disputes. By far the most common administrative proceedings are commenced under the UDRP. The UDRP applies to disputes in nearly all of the legacy TLDs (e.g., .com, .net, .org), a number of ccTLDs that have adopted the policy, and all new TLDs.

A UDRP proceeding can be filed against multiple domain names, and at least one dispute provider permits filings against multiple unrelated respondents. The UDRP is consistently applied with more than 15 years of non-binding precedent. However, unlike with litigation, no injunctive relief is available, which means any offending use of the domain name will continue until the conclusion of the proceeding.

While the filing fees depend on the selected arbitration company administrating the proceeding, generally the cost for a proceeding commenced against a single domain name and before a single panelist, is $1,500 USD. UDRP proceedings are typically resolved in 5-7 weeks, and assuming the complainant prevails,[6] the domain name is transferred.

The URS has the same prima facie elements as the UDRP, however, as explained above, the standard of proof is higher. Unlike the UDRP, a URS proceeding is only available for new TLDs and only against a single domain name.

Further, a successful URS proceeding only results in the domain name being suspended and not transferred, meaning the domain name remains in the possession of the original registrant, but may not be used. However, the URS is significantly less expensive to prepare and file, and a decision is typically rendered in just a few days.

Should the complainant desire to have the domain name transferred or canceled, it must file a UDRP, or federal lawsuit for cybersquatting. One effective use of the URS has been to simply deactivate a website at an infringing domain name; thereafter a UDRP or federal suit is filed to obtain the transfer of the domain name, or the registrant (who cannot use the domain name) may allow it to expire.

There are several other useful tools, short of filing litigation, available to remedy infringing domain names. For example, the federal Digital Millennium Copyright Act (''DMCA'') provides effective content takedown procedures, which are followed by many Internet hosting companies. It is common that when an infringer uses an infringing domain name, they also use one or more of the company's copyright protected photographs or logos.

Sending a DMCA takedown notice may result in the entire website being taken down by the hosting company rather than just the complained-of copyright protected works. If successful, this technique can get an offending website taken down while a UDRP proceeding is being pursued.

Another useful tool involves filing a complaint with ICANN regarding a domain name's false whois data (listing false information is common with cybersquatting). Again, this may result in the domain name being disabled. Similarly, filing a complaint with the registry, registrar, hosting company, and/or one or more ''black hole'' websites when a domain name is used for phishing attacks or mail spamming have also proven effective.

Lastly, it is a good idea to place a free ''backorder'' with one or more companies who specialize in registering expiring domain names (e.g., SnapNames and Namejet are two such companies). In the event a domain name expires or is deleted, there is a good chance that one of these companies will register the domain name. The approximately $70 these companies charge for successfully registering a domain name pales in comparison to the potential future legal fees.

Litigation is almost always extremely expensive, especially in comparison to the other alternatives. However, in some circumstances it may provide the best option, due to urgency, severity, or the failure of one or more of the other options above.

The ACPA permits suing either the registrant of the domain name in personam (assuming the court can exercise personal jurisdiction), or suing the domain name itself in rem for injunctive relief (transfer or cancelation[7]) where the court cannot obtain personal jurisdiction.

In the event of an in personam case against the registrant of the domain name, statutory damages of up to $100,000 per domain name are available. ACPA actions provide an excellent tool to recover, in bulk, numerous infringing domain names which are owned by foreign registrants.

Domain Name Asset Management

There are numerous best practices for domain name portfolio management. And while some may not make sense for every organization, many are sound and should be considered.

The first best practice is to consolidate domain names at one registrar. Companies with more than a handful of domain names should strongly consider using a reg-

[6] To prevail, the complainant must prove that the domain name is identical to a trademark or service mark, that the respondent has no legitimate interest in the domain name, and that the domain name was registered and used in bad faith. These prima facie elements are very similar to the federal ACPA.

[7] Always choose to have the domain name transferred!

  ECLR ISSN 1098-5190

istrar specializing in managing corporate domain name portfolios[8].

These specialized registrars offer a higher level of service and numerous related services that corporate clients benefit from (invoices for renewals; local points of presence for ccTLDs, managed DNS servers, etc.). Of course, this higher level of service typically commands a higher price than with typical registrars.

Companies should also use a standardized company name and contact information for all domain names. Using a generic mail address (domains@companyname.com) for management permits important e-mails to be directed to several responsible parties within the company (i.e., the IT department and the legal department). Lastly, all domain names should be renewed for more than one year beyond the current year to ensure adequate time to process renewals.

Many companies should register multiple domain names that are confusingly similar to their brand for defensive purposes (or acquire them through enforcement efforts). These domain names should be put to use directing consumers to the appropriate parts of the company's website.

For example, acmewidgets.com would likely direct consumers to the widget section of Acme's website. These domain names should not be left unused; and they should never resolve to a former cybersquatter's parking page after the domain name has been recovered by the brand owner.

One common management problem that may occur is when an employee registers a domain name they believe the company should own. The problem is that this domain name is then controlled by the employee although it appears to be operated by the company. Moreover, if the employee leaves the company, it is very difficult to recover control over the domain name.

Accordingly, companies should have a policy that all domain names must be registered by the company's domain name administrator. Discovery of these domain names often occurs by monitoring the domain name search reports detailed above.

Developing a Domain Name Strategy

By far, the most important best practice is for the company to develop an effective and appropriate domain name strategy. The development should include key stakeholders from within the company (i.e., legal, sales and marketing, IT).

Not only do these stakeholders have an interest in an effective strategy, they often will contribute to the budget for many of the items at issue. Generally, the strategy should address: what domain names the company should own (both currently and in the future); how, and by whom, the domain names are managed; identifying problem domain names and setting enforcement priorities; and specific goals and tasks to achieve the desired progress within the allocated budget.

A common question regarding enforcement is whether every detected problem must be fixed. (Isn't *not* knowing about these problems better?) Trademark owners have a duty to police their trademarks, including from online infringement, to protect the public from confusion.

Failure to adequately police a mark can be grounds for trademark cancelation, and willful blindness does not excuse the owner's duty to police. However, a mark owner need only take reasonable efforts to police its mark, and courts are flexible where owners employ reasonable enforcement efforts.

Accordingly, a more prudent approach is to set priorities and thresholds that reasonably address domain name problems in view of the mark and the market. If a domain name triggers a threshold, then appropriate action should be taken.

Remember, many infringement cases actually make business sense to fix. If a domain name is intercepting and misdirecting customers directly to competitive goods, that infringement likely harms the company more than the costs to fix the problem, and a prudent business approach is to fix the problem.

Similarly, if an infringing domain name is being used for phishing (collecting customer's data) or for fraud, that use exposes the company to significantly greater risk than the cost to fix the problem. On the other hand, there may be a number of problems that are lower on the priority list, and these can be safely monitored without action.

Often times, lower risk domain names are unlikely to cause consumer confusion and are often not renewed. Accordingly, a prudent strategy could be to wait and see what happens in a year. If new infringing domain names are identified, priorities can be shifted as necessary.

Conclusions

Companies face a myriad of legal and non-legal issues arising from domain names. However, by learning about the legal and technical space, and developing an effective and appropriate domain name strategy, companies can learn about and resolve these issues effectively. Similarly, the diligent management of company owned domain names is an integral part of the company domain name strategy. Lastly, there are a number of available tools, ranging from simple telephone calls to federal litigation ,which can be used to combat cybersquatting and protect the company's brand.

[8] A number of registrars offer this specialization. Popular choices by larger brand owners include MarkMonitor, Safenames, and Corporation Service Company.