Intellectual Property Magazine

Picture: Junede / Shutterstock

Cybersquatting ain't what it used to be

The Muscovitch Law Firm's **Zak Muscovitch** discusses how cybersquatting has changed over the years and warns trademark owners to prepare themselves for the future

The nature and complexity of cybersquatting has changed over the years. This summer will mark the 13th anniversary of the adoption of the Uniform Domain Name Dispute Resolution Policy (the "UDRP" or the "Policy"). The UDRP was adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN") on 24 August 1999[1]. ICANN, the not-for-profit corporation which oversees and manages the global domain name system, established the UDRP as a streamlined and inexpensive dispute-resolution procedure to deal with "abusive domain name registrations[2]", or what has become known as, "cybersquatting".

The establishment of the UDRP in 1999 marked a novel and effective way to deal with the new phenomena of cybersquatting. It provided a global jurisdictional framework for adjudication of domain name disputes. Moreover, it provided a procedure that was conducted nearly entirely online. The World Intellectual Property Organization ("WIPO") was the first ICANN-approved dispute resolution provider and it received its first domain name dispute case on 9 December 1999[3]: *World Wrestling Federation Entertainment, Inc v Michael Bosman* (D1999-001). Since then, the Geneva-based WIPO, and the similarly ICANN-mandated dispute resolution provider, the Minnesota-based National Arbitration Forum, have collectively adjudicated well over 37,000 UDRP domain name dispute cases[4].

In the aforementioned first-ever UDRP case, the disputed domain name, worldwrestlingfederation.com, had been registered by a cybersquatter who beat the complainant trademark-owner to the registration of the subject domain name. The domain name was nearly identical to the complainant's trademark and the cybersquatter then tried to sell the domain name to the complainant. This case was typical of the common form of a cybersquatter, namely a "creative extortionist", who takes advantage of a trademark owner who is slow to adapt to the realities of the internet. Many cases involving longstanding trademarks have already wound their way through the UDRP.

Yet cybersquatting persists, both for new trademark owners and for older trademark owners who have still not fully adapted to the ever-changing realities of the internet. New forms of cybersquatting have emerged which do not fit the original pattern of the "creative extortionist", and as a result, many companies continue to be victims of cybersquatting without even realising it. Fortunately, the UDRP has proven versatile enough to satisfactorily address even these newer forms of cybersquatting.

At the core of the UDRP is a three-part test to establish cybersquatting. In order to succeed in the online arbitration, a complainant has to prove that a) it has common or registered trademark rights, b) that the registrant has no legitimate interest in the domain name and c) that the registrant registered and used the disputed domain name in bad faith. Except in the case of these "bad faith" registrations made with the intent to profit commercially from others' pre-existing trademark rights, the minimalist policy relegates all other "legitimate" disputes, such as those wherein both disputants assert trademark rights, to the courts. This was expressly touted by ICANN to be "a feature, of the policy, not a flaw[5]".

Cybersquatting has increased in sophistication over the years and the resulting issues are more serious than ever. No longer are cybersquatters content to merely register domains in bad faith to sell to a pre-existing trademark owner. Now, cybersquatters are registering domain names to actually use themselves for illicit purposes. Trademark owners and their counsel would be well

advised to become familiar with the various newer forms of cybersquatting and to develop an ongoing approach to identifying and resolving cybersquatting issues as they arise. The first step in developing such an approach, is to become aware of these newer forms of cybersquatting which have arisen since the advent of the original "creative extortionist" model of cybersquatting.

The "typosquatter"

The typosquatter is a variety of cybersquatter who usually does not want to extort the trademark owner. Rather, the typosquatter is perfectly satisfied quietly enjoying the rewards of his illicit domain name registration. A typosquatter will find a variation of a trademarked term and then register a corresponding domain name. These variations often include plurals (such as cocacolas.com, for example), keyboard errors due to the proximity of keys (such as xocacola.com, and common misspellings (such as cokacola.com)[6]. Once registered, the typosquatter will harness the typosquatted domain name with "pay-per-click" advertising supplied by one of numerous companies which provide domain name owners with online advertisements. Then, the typosquatter waits for visitors who incorrectly type in the domain name of the trademark owner, and thereby unwittingly arrive at the illicit website of the typosquatter.

This kind of errant internet traffic can often be in the thousands of visits per day or per month, depending on the popularity of the trademark owner's genuine website. Often, the typosquatter's advertisements are of a general nature and are not necessarily related to the trademark owner's goods or services. At other times however, the advertising is specifically targeted to the nature of the trademark owner's business. The typosquatter receives a monthly cheque from the company which supplies him with the advertising, which is usually based upon the number of "clicks" which the advertisements receive. The trademark owner is thereby deprived of potential revenue and the trademark owner's brand is tarnished by confusion. Since the typosquatter usually wants to hold on to the domain name for as long as possible, the trademark owner will usually never hear from him, and as a result, the trademark owner may not even be alerted to the existence of the cybersquatting problem. A surprising number of companies, even large and sophisticated ones, are victims of typosquatting and do not even realise it or are not aware of the full extent of the problem.

A letter from a lawyer will not usually result in any transfer of the domain name by the typosquatter, as he will be hanging on to the very end, hoping to squeeze the brand out of every last penny until he is forced to give up the domain name. Accordingly, a UDRP is often the most effective approach to dealing with a typosquatter. However, where there is potentially a lot of lost revenue and the particular cybersquatter is identifiable, a lawsuit may be more appropriate. A trademark owner would, however, usually be satisfied with just gaining control of the cybersquatted domain name, through the UDRP.

The robber baron

The robber baron is a variety of cybersquatter who conducts cybersquatting on an industrial scale. Not content to stumble upon and register only a handful of cybersquatted names like most creative extortionists, the robber baron has accumulated a massive portfolio of cybersquatted names, often in the thousands or tens of thousands, and often through computer-assisted selection and registration.

"Cybersquatting persists, both for new trademark owners and for older trademark owners who have still not fully adapted to the ever-changing realities of the internet."

Sometimes, the robber baron will use an algorithm to identify domain names which are available for registration and which correspond to a common misspelling or variation of a trademark. At other times, the robber baron will monitor expiring domain name registrations which may have been inadvertently permitted to lapse by the trademark owner and scoop these up en masse, often with the assistance of a friendly domain name registrar. The robber baron will also regularly come up with additional new and innovative methods of cybersquatting and monetisation of cybersquatted names.

A UDRP may be useful in dealing with a robber baron, but sometimes the circumstances are best met with a lawsuit, particularly under the US Anticybersquatting Consumer Protection Act[7], which was enacted in 1999 and provides for damages of up to US $100,000.00 per domain name, plus legal fees. This is the approach that Verizon has often taken with robber baron-type cybersquatters[8].

Robber barons should, however, not be mistaken for large-scale domain name speculators who deal in generic or descriptive domain names, rather than intentionally trafficking in trademark-infringing domain names. There are many sophisticated companies, including even public companies, which have accumulated vast portfolios of domain names which correspond to common descriptive and generic terms and which from time to time also inadvertently correspond with a trademark. These speculators are well counselled in defending their domain names against attacks by trademark owners and will vigorously oppose legal proceedings, often even commencing their own counter legal proceedings for declaratory relief. For example, Marchex Inc is a publically traded company that owns 200,000 domain names[9], and will vigorously defend them on the basis of having registered them in good faith for their value as descriptive or generic[10]. Also, Tucows Inc, another publically-traded company that has reported owning hundreds of thousands of domain names[11], has made it known that they will go to court every time they are attacked with a UDRP over one of their descriptive or generic domain names, notwithstanding that it may also be someone's trademark[12]. Accordingly, in such cases, it is crucial for a trademark owner to identify exactly who they are dealing with prior to launching legal proceedings, in order to avoid an unexpected, costly, and uncertain battle.

The "email hijacker"

The dangers of cybersquatting can go far beyond "mere" trademark enforcement issues. Trademark owners need to also pay particular attention to security issues which arise from cybersquatting. For example, perhaps the most dangerous kind of cybersquatter is the one who uses a cybersquatted name as a means to an end, such as in the case of diverting confidential email communications intended for company employees.

Crucial and highly confidential emails from customers and clients of a trademark owner could be received and read by a particularly unscrupulous cybersquatter who has registered variations of a corporate domain name which is used for corporate email. The domain name, emiratesairlines.com, is not owned by the well-known Emirates airline, and neither is emirites.com (a misspelling). One can imagine what can potentially occur if highly confidential emails were to be inadvertently sent to someone with an email address @emirites.com instead of the proper and accurate, @emirates.com email address. Particularly for publically traded

companies, release of unauthorised and confidential information could be financially devastating.

The "affiliate fraudster"

Another type of serious fraud can occur when a trademark owner unwittingly pays commissions to a cybersquatter who is using a cybersquatted domain name to earn those very commissions. It is very common for many online companies to offer what is referred to as an "affiliate programme", wherein anyone can sign-up as an "affiliate" of the company and as a result, will be paid an agreed commission for every sale that the affiliate makes through his website. These commissions are tracked through "affiliate codes" and the affiliate receives compensation often directly from the company. It is usually prohibited for such an affiliate to make commissions through a cybersquatted domain name that is confusingly similar to the company's own trademark, but nonetheless, countless companies are regularly paying out substantial commissions to such cybersquatters. Accordingly, it is crucial for companies that offer such affiliate programmes, to audit all affiliates for proper use of domain names, as otherwise affiliates will be paid for cybersquatting by the trademark owner. This would of course not only be terribly unjust, but also very embarrassing.

The "ignoramus"

The ignoramus does not intend to harm the trademark owner. Rather, the ignoramus just does not know any better. The ignoramus tends to be someone who erroneously believes that any domain name which is 'available' for registration from a registrar, can be lawfully registered and has little or no idea that cybersquatting is unlawful. He has read about domain names and 'decided to get into the business'. More and more ignoramuses have cropped up as the internet has become more popular and speculation in domain names has become a more widely known business.

Typically, the ignoramus will not have the professional acumen of the typosquatter and as a result, will register domain names which are indeed confusingly similar to a trademark, but which result in no financial reward to the ignoramus. For example, CocaColaSite.Info may have been registered by an ignoramus. It would likely never receive any "type-in" traffic, and as an unused domain name without a website, poses little risk to the trademark owner who would likely never really want this domain name for itself anyway. Often, an ignoramus registers such a domain name because they mistakenly believe that the marketing department for a trademark owner would really like the domain name, and would be more than happy to compensate the ignoramus for his creativity and foresight.

Ignoramuses usually tend to respond well to a demand letter, once they get over the shock of having engaged in unlawful conduct, and after realising that there is absolutely no way the trademark owner would pay a penny for the cybersquatted domain name. The problem for the domain owner, however, is whether it is really worth the expense and effort in recovering this kind of domain name, particularly through a UDRP since so many of them likely exist and because it poses no immediate and direct threat. Furthermore, for many trademark owners, there is virtually no end to the number of such relatively innocuous but wrongful domain name registrations.

Tackling cybersquatting

Companies and often their counsel, have no idea of the extent and the degree to which trademarks are being misused by cybersquatters, let alone the damage and loss of revenues being caused. It is crucial that in conjunction with expert domain name law advice, trademark owners assess the extent of their cybersquatting problem and develop a range of appropriate responses depending on the nature of the circumstances. Cybersquatting should not be treated as an issue which can be satisfactorily dealt with through one-time action. It is a problem which companies must continually monitor and respond to.

Accordingly, trademark owners should consider the following proactive steps which are integral to competent prevention and management of cybersquatting issues:

- Comprehensive searching for current and possible future cybersquats with the assistance of an expert consultant or domain name lawyer.
- Establish a triage system whereby the degree of severity of each particular cybersquat is resolved through the appropriate measure, ranging from a demand letter, to a UDRP, to a lawsuit.
- Ensure that marketing departments coordinate the adoption of new trademarks and the enforcement of all existing ones, with legal counsel.
- Audit all "online affiliate" arrangements in order to ensure that affiliates are not using cybersquatted domain names to earn commissions.
- Review email security in order to assess vulnerability to diversion of email through cybersquatting.

Footnotes

1. ICANN's Timeline for the Formulation and Implementation of the Uniform Domain Name Dispute-Resolution Policy (http://www.icann.org/en/help/dndr/udrp/schedule).
2. ICANN's Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy (25 October 1999), at Paragraph 4.1(c) (http://archive.icann.org/en/udrp/udrp-second-staff-report-24oct99.htm).
3. ICANN's Timeline for the Formulation and Implementation of the Uniform Domain Name Dispute-Resolution Policy, id.
4. WIPO Prepares for Launch of New gTLDs while Cybersquatting Cases Continued to Rise (6 March 2012) (http://www.wipo.int/pressroom/en/articles/2012/article_0002.html) and National Arbitration Forum Launches Dispute Program for .XXX Domain Names (5 December 2011) (http://www.adrforum.com/newsroom.aspx?&itemID=1703&news=3).
5. ICANN's Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy (25 October 1999), id at Paragraph 4.1(c).
6. Each of these misspelled domain names is currently registered to a person other than The Coca-Cola Company as of 30 March 2012.
7. 15 USC § 1125(d).
8. See for example, *Verizon California, Inc v Navigation Catalyst Sys, Inc*, 568 F Supp 2d 1088 (C D Cal 2008).
9. See Marchex Inc's SEC Quarterly Report (Form 10-Q), dated, 4 November 2011.
10. See for example, *Havanna SA v Brendhan Hight, Mdnh Inc* (WIPO Case No D2010-1652).
11. See Tucows Reveals Key Domain Name Portfolio Assets, 20 February 2008 (Tucows News Release).
12. See for example, *The Brickman Group Ltd LLC v Tucows.com Co* (NAF Claim Number: FA1201001425812), and also see *Tucows.Com Co v Lojas Renner SA*, 2011 ONCA 548 (CanLII).

Author

Zak Muscovitch is the principal of The Muscovitch Law Firm and www.DNattorney.com. Since 1999, he has handled hundreds of domain name disputes for trademark owners and domain name registrants from all over the world, including many precedent-setting cases. Zak also assists corporations with domain name and website transactions.