A pre-emptive strike

Brian Winterfeldt, who is a special advisor on INTA’s internet committee, weighs into the cybersquatting debate. IPPro hears what he has to say

MARK DUGDALE REPORTS
Why did cybersquatting cases increase in 2012?

An increasing number of domain names are registered each and every year. By Q3 2012, 246 million domain names were registered across all TLDs. The total number of domain registrations grew by 26.4 million, or 12 percent, year-on-year, ie, Q3 2011 to Q4 2012.

Brand owners and the public at large are more attune to the value of domain names than ever before. To this point, ‘domain name flipping’ is consistently one of the top online search results when querying, ‘how to make money on the internet’. Unfortunately, not everyone who registers a domain name to obtain a quick buck is attune to trademark rights or policies and laws prohibiting cybersquatting.

Finally, trademark counsel following or involved in ongoing developments on trademark rights protection mechanisms (RPMs) in the Internet Corporation for Assigned Names and Numbers’s (ICANN’s) new gTLD programme since at least 2009 know that there may be rewards to reap from active utilisation of the Uniform Domain-Name Dispute-Resolution Policy (UDRP). For example, ICANN is presently examining whether to augment several RPMs to encompass confusingly similar strings that have previously been abusively registered or used.

What are some of the cybersquatting hotspots?

Most cybersquatters that we encounter hail from outside of the US, and are predominantly from the BRIC (Brazil, Russia, India and China) countries. This trend is likely attributable to jurisdictional limitations on enforcement. Unlike the Anti-Cybersquatting Consumer Protection Act in the US, most other nations still do not have the strong legislation needed to pursue cybersquatters and hold them accountable.

How are trademark owners handling this escalating problem?

Brands are responding to increased cybersquatting by prioritising instance of infringement, increasing enforcement activities and participating within ICANN. Notably, some brands have applied to operate their own branded new gTLDs with twin goals of guaranteeing authentic goods and quality services to consumers while making cybersquatting and imposter websites more irrelevant.

Building strong relationships with domain name registries, registrars and other entities in the domain name after-market is also important, as these entities may be willing to discuss potential filtering systems for infringing domain names or other pre-emptive alternatives.

Given the rise in cybersquatting cases, how do they prioritise?

In general terms, we recommend that brand owners identify potentially infringing domain names, investigate the registration information and any website content, and then prioritise the matter based upon the nature of the infringement. For example, although all infringement is a priority, infringement of a primary brand is generally a higher priority than infringement of a mark for an ancillary offering. In addition, the nature of the infringement may be egregious—including domain names that are used in phishing attempts, resolve to child pornography, or compete directly with the goods and services offered under the brand at issue.

How should brands prevent cybersquatting from occurring in the first place?

At present, there are only a handful of preemptive measures a brand owner can take. Defensively registering trademarks and strategic variations such as plurals or common typographical errors as domain names is one method. Sunrise registration periods facilitate this method by providing brand owners with an advance opportunity to register domain names when a new gTLD is launched. However, this method can get expensive and result in very large portfolios of sometime unwanted or unused domain names.

Absent a risk of ‘cyber flight’, contacting the domain name registrant can have positive results. Oftentimes, registrants are unaware of trademark rights. Building strong relationships with domain name registries, registrars and other entities in the domain name after-market is also important, as these entities may be willing to discuss potential filtering systems for infringing domain names or other pre-emptive alternatives.

Once cybersquatting occurs, what avenues exist to help brand owners enforce their rights?

Absent a risk of ‘cyber flight’, contacting the domain name registrant can have positive results. Oftentimes, registrants are unaware of trademark rights. In instances of bad faith conduct, there is the UDRP in the new gTLD space and comparable ccTLD dispute resolution procedures. This is in addition to the US Anti-Cybersquatting Consumer Protection Act for registrants, or domain names registered on name servers, located in the US. Some TLDs, such as .xxx, have a rapid takedown procedure, and the Uniform Rapid Suspension system will apply to all new gTLDs launched through ICANN’s new gTLD programme.

How will new gTLDs contribute to the problem and what measures will be available to deal with it?

The new gTLDs will expand the current name space from 21 gTLDs to around 1400. That could have an exponential impact on the frequency of cybersquatting.

To try to counterbalance this impact, several new RPMs are available in the new gTLD programme. Brand owners can store all of their trademark data for use in a central database called the Trademark Clearinghouse in connection with other RPMs.

Brand owners can use that data to obtain defensive sunrise registrations during mandatory 30-day periods in all new gTLDs. A low-cost uniform sunrise across all TLDs has been requested, and is under consideration by ICANN, although if it is to apply in the new gTLDs, then it will likely be up to individual registry operators.

Brand owners can also use that data to participate in mandatory 60-day trademark claims services, which will provide a notice to potential registrants attempting to register an exact match of a trademark in the clearinghouse, as well as provide a notice to brand owners upon registration of their marks as domain names.

In addition to the enforcement options listed above, brand owners will also be able to use the URS system to quickly suspend infringing domain names at a fraction of the cost to file a UDRP complaint. However, suspended domain names drop back into the pool of registerable names after the expiration date of the domain name. Brand owners should also continue to participate in trade organisations such as the International Trademark Association, in order to influence public policy and make the internet a safer environment for trademarks and consumers.