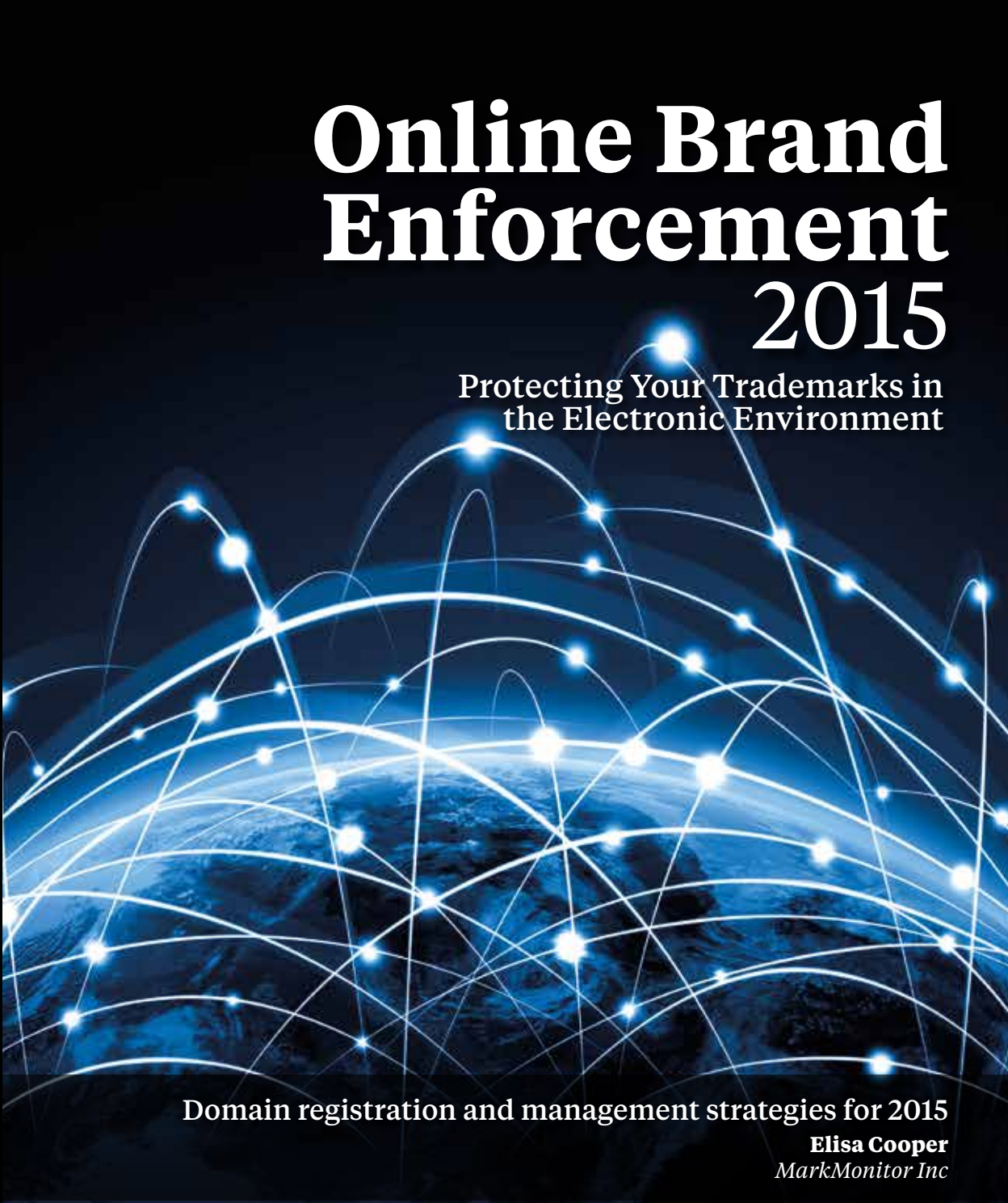
Online Brand Enforcement 2015

Protecting Your Trademarks in the Electronic Environment



Domain registration and management strategies for 2015

Elisa Cooper
MarkMonitor Inc

This article first appeared in Online Brand Enforcement 2015: Protecting Your Trademarks in the Electronic Environment, a supplement to World Trademark Review, published by Globe Business Media Group - IP Division'. To view the guide in full, please go to www.worldtrademarkreview.com.

World Trademark Review™

The IP Media Group™

Smart Brands Protect Their Revenues Online

Strong brands are the foundation for strong corporate reputations, driving Web traffic,fueling revenues and forging customer relationships. As business has moved online, brands face new opportunities and new challenges.

MarkMonitor® is in the business of protecting brands online, helping strong corporate reputations become even stronger in the digital world. We can help you establish your brand online and help you combat the growing threats of brand abuse, stolen Web traffic, unauthorized channels, counterfeit sales and piracy.

More than half of the Fortune 100 trust MarkMonitor to protect their brands online.

See what we can do for you.

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

M

www.markmonitor.com

(800) 745-9229
+44 (0) 203 206 2220

Domain registration and management strategies for 2015

Author
Elisa Cooper

Corporate domain registration and management strategies have evolved over the last 10 years.

It used to be that registering variations, typo squats and misspellings was a viable approach for protecting brands online. It used to be that the domain name system was not a target for cybercriminals and politically motivated hacktivists. And it used to be that there were just a few dozen top-level domains (TLDs) of real importance.

Needless to say, things have changed.

More than ever, companies need to balance the need for promotion with protection by making intelligent domain registration decisions. They also need to ensure that domain assets, once registered, are completely secure. On top of this, companies need to make sure that they are effectively managing the entire domain name lifecycle, which includes directing domains to appropriate content, letting unnecessary names expire and potentially selling unused and valuable names to fund new registrations and policing efforts.

So where to begin?

Make informed decisions

With over 400 new generic TLDs (gTLDs) now delegated, many companies have fallen into a registration rhythm with approaches ranging from minimal registration and blocking strategies for one or two core brands all the way to registrations of multiple brands in every single new gTLD registry.

Generally speaking, many companies are looking to register exact matches for their core trademarks in registries where there is a close correlation between the brand and the TLD. For example, financial institutions are planning to register in TLDs such as '.bank', '.loan' and '.mortgage'. Identifying these kinds of close match is easy, especially given that there are just under 620 open and restricted TLDs.

It is difficult for companies to assess where to register in non-Latin TLDs. When it comes to non-Latin registrations, companies should understand how their brands are marketed internationally. If they are marketed using non-Latin characters, then consider registering in the new internationalised domain name (IDN) TLDs, assuming that there is a nexus between the brand and the TLD. However, mixing character scripts and registering Latin second-level domains with non-Latin TLDs are generally discouraged.

Companies also have to make difficult decisions about whether it makes sense to register in city or geo TLDs. In these situations, companies need to think about whether they are actively marketing or promoting their brands in these cities or regions.

In addition, certain categories of registry pose their own special risks, including gripe ('.wtf' and '.sucks'), vice ('.sex' and '.poker'), corporate identifier ('.inc' and '.gmbh') and

> **Reliance on a hardened domain registrar which is familiar with all potential attack strategies is a must. Most likely, this level of sophistication can be found with a registrar which deals exclusively with corporate clients**

charitable ('.foundation' and '.charity') TLDs. Companies must determine their tolerance for risk when planning their registration and blocking strategies around these.

Finally, there are all of the truly generic new gTLD registries, such as '.web', '.blog' and '.news' – again, there are difficult decisions to be made, as there is no 'one size fits all' when it comes to developing a registration and blocking strategy.

Take advantage of blocking – but beware

When the ICM Registry initially launched '.XXX' back in 2011, the notion of a registration block was a fairly novel idea. Essentially, the ICM Registry allows companies which are not part of the global adult entertainment industry to pay a low-cost fee to seek the permanent removal of names matching their trademarks from the general pool of names available for registration. Many saw this move as a genuine attempt to protect the rights of brand owners; others saw it as yet another mechanism for generating revenue from rights holders under the guise of a sunrise period.

Donuts Inc, which applied for over 300 new gTLDs, and Rightside Registry, which applied for over 30 new gTLDs, are both offering submissions to their respective domain protected marks lists (DPMLs). This service essentially enables brand owners to block a string containing a trademark which has been validated against the Trademark Clearinghouse across every TLD managed by either Donuts or Rightside Registry. Exact matches can be protected, as well as any string containing a validated trademark.

This means that if MarkMonitor successfully submitted MARKMONITOR to the Trademark Clearinghouse, strings such as 'MarkMonitorProducts', 'MarkMonitorServices' and 'MarkMonitorClients' could be blocked across all of the Donuts TLDs and/or Rightside Registry TLDs.

The downside is that fees will be associated with each protected string. Also, any blocked registration can be overridden and registered as a domain by anyone that owns a validated Trademark Clearinghouse submission.

Moreover, any names that are identified as premium are ineligible for blocking. This means that if a trademark is a dictionary term, a first name or surname or a three-letter acronym, there is a distinct possibility that it will be deemed as premium by the registry and therefore will be ineligible for blocking. To complicate matters, premium name lists are distributed only just before the launch of every sunrise period for the Donuts and Rightside Registry TLDs.

For companies that have truly unique trademarks, blocking can be a cost-effective approach; but for others, it may not provide much protection at all.

Employ appropriate levels of security

Every single domain under management should be created, configured and then locked to make it unavailable for transfer.

There is also an elevated locking mechanism – sometimes referred to as a 'registrar lock' or a 'super lock' – which essentially freezes all domain configurations

until the registrar unlocks them upon completion of a customer-specified security protocol. Companies can control the level of complexity associated with their specific protocol, and domains are made available for updating through the portal only when these security protocols are completed accurately. This extra level of security should be applied to mission-critical domains such as transactional sites, email systems, private extranets and site-supporting applications.

Generic domain locking can still be exploited by an attacker who (with compromised log-in credentials) can update nameservers and redirect customers to illegitimate websites without transferring actual control of the domain from one registrar to another. To combat this, another step is to registry lock or premium lock, which makes the domain unavailable for any updates at all. This method of locking is currently available for '.com', '.net' and a number of country-code TLD (ccTLD) registrations.

Reliance on a hardened domain registrar which is familiar with all potential attack strategies is a must. Most likely, this level of sophistication can be found with a registrar which deals exclusively with corporate clients. Such a registrar will also have specialised security features for preventing, detecting and responding to attacks against any domains, including:

- verifying portal account access via two-factor authentication;
- restricting access to a portal via IP address;
- sending notification of any name changes;
- avoiding automated emails as a primary means of communication;
- keeping activity logs to track all domain name updates;
- maintaining strong password management to force password changes; and
- offering multiple levels of access

In addition, it is critical that the registrar being used be well established and experienced. It should also function as part of the security ecosystem, with strong relationships with other registrars, top internet service providers, security organisations, browser partners, major software developers and standards groups, which will keep it well informed as new threats emerge. Speed matters – these relationships will enable the registrar to quickly rectify any security breaches that do occur. Seek out a registrar that offers both guidance and deep experience in security, as well as domain management.

Finally, domains that are vital to ongoing operations should be continually monitored for unauthorised DNS updates, changes to website content and DNS cache poisoning.

While there are near-foolproof methods for locking down '.com' and '.net' and many ccTLD domains at the registry, other domains may still be at risk. Continual monitoring of core sites is recommended, so that any issues can be remedied quickly.

Make the most of defensive registrations

The bulk of corporate domain portfolios largely consist of defensive registrations, which often include common misspellings, product names and abbreviations in countries where the rights holder may not even be doing business. Unfortunately, many companies are not directing traffic from defensive registration to live content.

Why let these valuable assets go unused?

Determine where domain names need to point. For example, if an internet user types in a domain name, where should that user be directed? Should the domain resolve to a main corporate site, an e-commerce site or a HR site? Consider matching foreign-language domain names (IDNs) to language-specific websites, or product domain names to specific URLs.

Redirects can be managed easily through the use of standard web forwarding solutions, which also provide valuable statistics to help you understand the traffic generated from these defensive registrations. Information garnered can also be useful in rationalising portfolios, adding domains where needed or dropping domains with little or no traffic.

Speaking of portfolio rightsizing...

Campaigns that have run their course, products that were never launched and services or promotions that have been

Elisa Cooper
Vice president, domain product marketing
elisa.cooper@markmonitor.com

Elisa Cooper is a vice president of product marketing for MarkMonitor, with 20 years of experience. Over the last 12 years, she has worked closely with Fortune 1000 corporations to define and develop market-leading domain management and brand protection solutions. Ms Cooper also serves as a senior domain name consultant working with corporations on portfolio consolidations, domain name strategy and online brand protection. She has spoken and written extensively on these topics and is the chair of the Internet Corporation for Assigned Names and Numbers' business constituency and an active member of the International Anti-counterfeiting Coalition and the Online Trust Alliance.

discontinued – all contribute to unnecessary domain registrations that exist within many corporate portfolios.

At the least, an annual audit of domains under management is recommended as best practice to identify names that are no longer needed. While it may be a bit cumbersome, it is necessary to ensure that portfolios do not become bloated over time.

A number of methods can be used to rightsize portfolios, including focusing on:

- exact-match registrations in top TLDs;
- ccTLDs where products or services are actively marketed; and
- IDNs where existing non-Latin trademarks are also registered.

Typically, the single most important factor when deciding what to keep or what to drop comes down to traffic. Understanding just how much traffic is being generated by existing registrations is essential to maximise the value of domain portfolios. Bear in mind that domains used for internal applications may be critical, but might not generate much traffic – so internal sign-off is absolutely necessary before letting any name expire.

When conducting such a review, you may come across dictionary terms, three-letter domains or other valuable registrations that are not being utilised and are not particularly associated with your company. The secondary market for these types of domain is still strong, with names going for as much as six or seven figures in some cases. Now may be the time to consider selling these names, as they can assist with funding additional registrations or covering costs associated with policing efforts.

Implement a domain policing programme

Registering selective defensive registrations can alleviate some obvious risks. However, given the rate at which the domain name landscape is increasing, monitoring for abuse is becoming a much more cost-effective approach, when compared to registering defensively across all new gTLD registries. Even pursuing all cases of infringement will not be practical in this new environment. Companies will need to make decisions regarding whether a registration poses a real threat.

Domain name monitoring can be accomplished by searching through zone files for newly added domain names that contain a particular search term. A number of services available can provide this information on a daily basis.

Important features of a domain name monitoring service include:

- notification of newly registered domains and newly dropped domains;
- the ability to create exclusion lists and search zone files using wildcards;
- the status of each reported domain (ie, active, inactive or dropped);
- a live link for each domain; and
- a live link to the Whois record for each domain

By monitoring registrations, companies can proactively anticipate potential domain name abuse and take immediate action. This can include actively monitoring a site, filing a Uniform Domain Name Dispute Resolution Policy or Uniform Rapid Suspension system complaint, or challenging the accuracy of the Whois record if the name falls into the hands of a suspicious individual or entity.

One size does not fit all

When it comes to developing a domain registration strategy, unfortunately, there is no 'one size fits all' approach. Companies should create a decision-making framework upfront so that they have a clear direction in terms of which brands to register and block, the frequency of portfolio review to effectively manage size, identification of where domains should point and appropriate security mechanisms and policing programmes.

Companies should do their best to understand the new internet landscape and appreciate that any strategy should provide general guidelines only – there are likely to be many exceptions, given this rapidly changing environment. **WTR**

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

MarkMonitor Inc
425 Market Street
Fifth Floor
San Francisco, CA 94105
United States
Tel +1 415 278 8400
Fax +1 415 278 8444
Web www.markmonitor.com