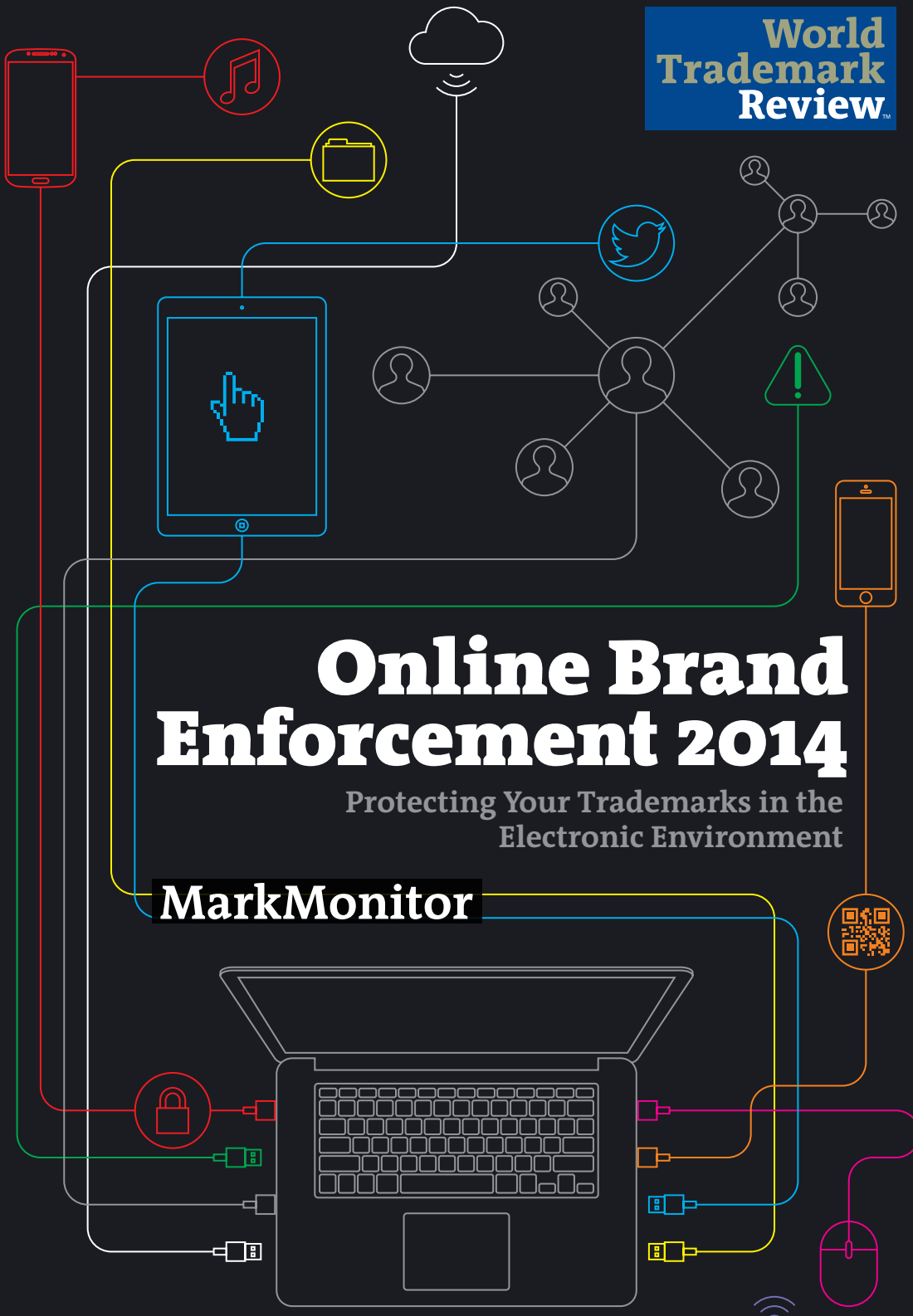
World Trademark Review™

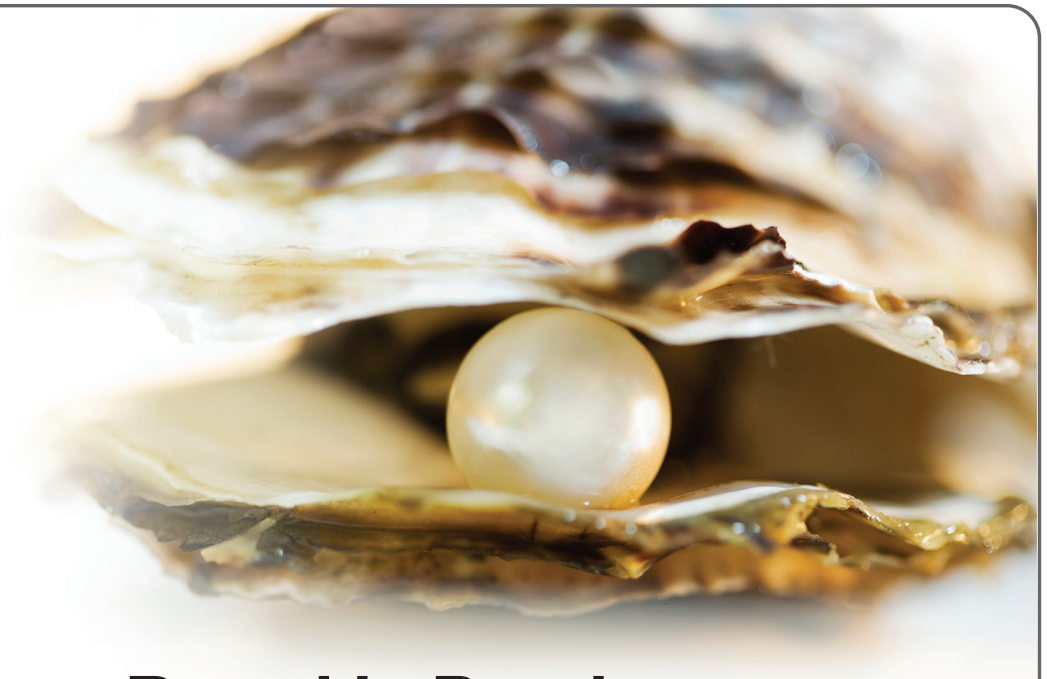


Online Brand Enforcement 2014

Protecting Your Trademarks in the Electronic Environment

MarkMonitor

Part of The IP Media Group



Your Brand is Precious. Protect It.

Counterfeiting. Piracy. Trademark infringement. And whatever comes next. There is no shortage of online threats to an organization's brand, reputation and intellectual property.

MarkMonitor® can help. Our brand protection solutions scour the Internet—auction sites, B2B exchanges, websites, search engines and social media sites—to automatically detect and shut down online brand infringement. Combined with our proven experience and unparalleled customer service, MarkMonitor is the ideal choice when it comes to online brand protection.

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

See what we can do for you.

www.markmonitor.com
(800) 745-9229
+44 (0) 203 206 2220

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

Domain name registration strategies in a new gTLD world

Author
Elisa Cooper

New generic top-level domains (gTLDs) represent the next major milestone in the expansion of the internet name space. The effect that they will have on domain portfolios and brand protection strategies is certain to be profound – and your brand must be ready.

After many years of debate, the Internet Corporation for Assigned Names and Numbers (ICANN) opened the new gTLD application period in January 2012. Although many details regarding the registry operators, launch dates, costs and requirements are not definitive, launches are quickly approaching. Now is the time to ensure that you are prepared by reviewing the applied-for strings – including familiarising yourself with the available rights protection mechanisms, such as the Trademark Clearinghouse – your domain portfolio, domain management policies and brand protection strategies.

Background

Top-level domains (TLDs) are the portion of a domain name located to the right of the dot. There are currently 22, the most well-known of which is '.com'. The new gTLD expansion opens the door for brands, community groups and entrepreneurs to operate their own TLDs, such as '.bbc', '.cpa' and '.fashion'.

In June 2012 ICANN released a list of 1,930 new top-level applications, which represented approximately 1,400 unique new TLDs. Close to 800 brands applied for a TLD in their own names. When awarded their '.brands', these organisations will be responsible for running a domain name registry in which other entities may be able to apply for a domain name, according to the criteria set by the registry.

Entrepreneurs and community groups also see opportunity in the expansion of the internet name space, and more than 600 of the TLDs applied for are generics, such as '.film', '.fashion', '.sports', '.books', '.clothing' and even '.sucks'. These entrepreneurs hope to build businesses around offering the public the ability to register a domain name to the left of the dot, such as 'brand.fashion', 'brand.sports' or 'brand.sucks'.

In general, domain management and brand protection professionals must understand how generics may affect their business category and their brand's digital presence. Do these generics represent an opportunity for the brand to reinforce its digital presence or open new web possibilities? Or do these generics present another potential headache from cybersquatters which take advantage of powerful brand names? What effect will the new gTLDs have on domain portfolios, management policies and budgets?

Reviewing applications and understanding rights protection mechanisms is crucial

Although ICANN's comment and formal objection periods have passed, it is still important to review the TLD applications and prepare yourself for what is coming. Will you be submitting sunrise registrations in any of the generic TLDs? If so, you should be gathering your trademark data and submitting your marks to the Trademark Clearinghouse. Will

you be submitting registrations for geographic TLDs, such as '.africa' or '.berlin'? If so, will any of them be registered using non-Latin character sets? What about defensive registrations? If you choose to go down this route, will you point visitors to new sites or redirect them to existing domains? While there are still many unknowns, you should familiarise yourself with the applications and begin thinking about how these new gTLDs will affect your strategies.

So, what recourse do brand owners have if, after reviewing the applications, they find strings of concern? While they cannot formally object, brand owners can make use of the protection mechanisms that ICANN has put in place to protect them. As part of the new gTLD programme, ICANN has adopted a number of new rights protection mechanisms, including the following.

Trademark Clearinghouse
The Trademark Clearinghouse will serve as a central repository of authenticated trademark information. The information contained within the clearinghouse will be primarily used to support pre-launch trademark claims, sunrise registrations and dispute resolution policies.

Trademark claims
Where a domain submitted for registration in a new gTLD is identical to an authenticated trademark within the Trademark Clearinghouse, the trademark claims service will provide notification (during the first 90 days of general registration only) to the prospective registrant and confirm that:

- the prospective registrant has received notification that the mark is included in the Trademark Clearinghouse;
- the prospective registrant has received and understood the notice; and
- to the best of the prospective registrant's knowledge, the registration and use of the requested domain name will not infringe the rights that are the subject of the notice. If the domain in question is registered, the rights holder will be promptly notified.

Sunrise registrations
Assuming that eligibility requirements are met, sunrise registrations will also be made available to all trademark holders in the Trademark Clearinghouse. Sunrise registration periods provide rights holders with priority registration periods, giving them the ability to register domains before they become generally available to the public. Additionally, notices will be supplied to all trademark holders in the clearinghouse if a party is seeking a sunrise registration. A notice will also be provided to holders of marks in the clearinghouse that are identical to a name registered during sunrise. Conflicts that arise may be subject to a Sunrise Dispute Resolution Policy.

Uniform Rapid Suspension (URS) system
All new gTLDs will be subject to the URS system, which is designed to provide a cost-effective, expedited process to address issues of trademark infringement and abuse. Form complaints are filed electronically and are designed to be as simple and formulaic as possible. Domains are suspended only for the remainder of their registration term, or for an additional year at current market registration rates. However, after suspension ends, domains become available for registration and are likely to be registered again, resulting in a never-ending cycle of watching and suspending.

Post-delegation Dispute Resolution Procedure
The Post-delegation Dispute Resolution Procedure will provide rights holders with the ability to file complaints against registries which have acted in bad faith with the intent to profit from the systematic registration of infringing domains at the second level (to the left of the dot). According to ICANN, an example of infringement is where a registry operator has a pattern or practice of actively and systematically encouraging registrants to register domain names and to take unfair advantage of the trademark to the extent and degree that bad faith is apparent. Another example of infringement is where a registry operator has a pattern or practice of acting as the registrant or beneficial user of infringing registrations to monetise and profit in bad faith.

Registry Restriction Dispute Resolution Procedure
The Registry Restriction Dispute Resolution Procedure is a complaints procedure for community-based gTLDs in which the

complainant asserts that it is "a harmed established institution as a result of the community-based gTLD Registry Operator not complying with the registration restrictions set out in the Registry Agreement". The complainant must prove that the TLD operator violated the terms of the community-based restrictions in its agreement, and that the complainant and the community named by the objector were measurably harmed.

Time for a domain portfolio review

In addition to reviewing the application list, identifying any concerns and understanding available rights protection mechanisms, now is the time to plan for how your domain portfolio will be affected by the expanded name space. Perhaps a particular TLD may open new business possibilities for your brand, especially if it turns out to be popular with consumers.

Unfortunately, due to the real threats of cybersquatters which prey on well-recognised brands to steal traffic, the addition of so many new TLDs will require brands to re-examine the defensive portions of their domain portfolios. Today, the bulk of corporate domain portfolios largely consist of defensive registrations, averaging up to 80% of a portfolio. In the case of large brands, defensive registrations can consume up to 99% of the total portfolio.

With these additional TLDs, registering your brand defensively in each of them is not feasible from an economic point of view, even if all of the new TLDs make perfect sense for your brand. Even if only 50 of the new TLDs prompt a defensive registration, if you have multiple sub-brands, products, promotions or other terms that are used as domain names, registering all of those terms across those 50 new TLDs could impose significant new costs.

Now more than ever is the time to take a long, hard look at defensive holdings, decide which of your existing domain names are no longer necessary and purge them from your portfolio. Criteria for your purge may include:

- domains which were registered, but never used;
- domains for products or services that were never launched;
- domains that are too long or include several hyphens;
- domains in highly restricted TLDs, where costs are high and risk of cybersquatting is low;
- domains in countries where you may not be doing business; and
- domain name variations that receive little or no traffic.

While casting a critical eye on your domain portfolio, ensure that you keep the domain names that would incur high recovery costs if circumstances changed and you found that you needed that name in your portfolio. Also, be sure to keep the domain names with a high likelihood of squatting.

Revisit your domain management policies

With between 40 and 50 TLDs estimated to launch each month and the number of internal registration requests expected to increase, this is also a good time to review domain management policies. Be sure to identify the individuals who are permitted to request, approve and modify registrations. The latter point is especially important, as we have seen cases in the last year of 'hacktivists' targeting familiar domain names and modifying registration details to make a political or social point. If more than one person is granted the ability to make changes, it is still advisable that a central point of contact be tasked with reviewing and approving all changes.

Be sure that you have clear policies that determine when new domains should be registered. These conditions may include product launches and campaigns, the opening of new TLDs or the liberalisation of country-code TLDs. Your policy should also provide guidelines on important variations, common misspellings or even combinations of terms, such as 'brandshop' and 'shopbrand' for domain names. Define any other special circumstances that should be addressed, including policies on WHOIS information that should be recorded and nameserver details, such as how contact information should be specified.

Another policy to be implemented revolves around the 'locking' of domain names. By locking a domain name, unauthorised transfers or changes to the domain name system cannot be made. It is no longer sufficient to secure your website; the domain name itself must be secure from hackers too. If your domain registrar is not providing state-of-the-art domain name

security, including registry locking, you may wish to move your portfolio to one which does.

Finally, determining where you want your domain names to 'point' is a critical decision which should be addressed. Should it resolve to a main corporate site, an e-commerce site or HR site? Do your foreign-language domain names point to language-specific websites? Through the use of standard domain name system solutions, you can easily obtain valuable statistics to help you understand the traffic generated from defensive registrations. Information garnered will be useful in rationalising portfolios, adding domains where needed or dropping domains with little or no traffic.

Reassess your brand protection strategies

This is an ideal time to refresh the strategies that you are using to protect your brand. At the most basic level, it is important to monitor for potential problems in all new gTLD registrations for improper use of brands, trademarks and slogans. Be sure to monitor questionable registrations for 'go-live' dates so that you can begin monitoring site content. By monitoring domain registrations, companies can proactively anticipate potential domain name abuse and take immediate action. This can include:

- actively monitoring a site and associated traffic;
- filing a Uniform Domain Name Dispute Resolution Policy or URS procedure; or
- challenging the accuracy of the WHOIS record if the name falls into the hands of a suspicious individual or entity.

With so many wide-open name spaces, cybersquatters and phishers will likely redirect internet traffic in the new gTLD environment to fraudulent websites by registering domains that are confusingly similar to legitimate sites. If you do not already have established guidelines, your legal, brand protection and risk management teams should work together to put policies in place for detecting and investigating internet-borne fraud sites or abusive and illegal domains that infringe your trademarks.

Incorporate an active defence strategy that identifies administrative, legal and/or technical means to shut down rogue sites that are targeting your brand, so that your customers do not fall victim to scams. Identify the most highly trafficked abusive or illegal sites and prioritise them for enforcement. Have a plan in place for capturing that traffic and redirecting it to the appropriate sections of your brand's website.

Conclusion

Now is the time to prepare for the launch of the new gTLDs. Review your existing domain portfolio, update policies and guidelines and calculate the budget impact of the new TLDs in which you will want to register your brands. Departments responsible for domain registration budgets should anticipate an increase in budget, as close to 620 new gTLDs are expected to launch over the next two to three years. While many of the costs are not fully known, registration fees, Trademark Clearinghouse submission fees and the additional costs of policing and remediating domain name abuse must be included.

While the flood of new gTLDs is expected to occur this year, not all registrars will be offering registration services in every new gTLD. Selecting a registrar that is committed to providing registration services for all new gTLDs (even those with stringent eligibility requirements) will be critical, as the new domain name landscape promises to become significantly more complex over time. Working with a single registrar (as opposed to multiple registrars) will help to ease some of this anticipated complexity. Regardless of whether you find exciting new business opportunities in these new domain names, you will want your customers and prospects to find your sites, rather than those of an impersonator. WTR

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

MarkMonitor
425 Market Street, 5th Floor
San Francisco, CA 94105, United States
Tel +1 415 278 8400
Fax +1 415 278 8444
Web www.markmonitor.com

Elisa Cooper
Director of product marketing
Elisa.cooper@markmonitor.com

With 11 years of domain name industry experience, Elisa Cooper is an expert in the online brand protection and domain name management field. Ms Cooper has worked closely with many Fortune 1000 companies in assisting with domain and brand protection policy development. She has spoken and written extensively on these topics and is the chair of the Internet Corporation for Assigned Names and Numbers' Business Constituency. She is also actively involved with the International Anti-Counterfeiting Coalition and the Online Trust Alliance. Ms Cooper completed undergraduate and graduate studies in communications at San Jose State University, California.