New gTLDs – Understanding and mitigating the risks of the 'super six'

The new gTLD programme is creating a much larger world for rights owners to monitor and protect their brands. **Elisa Cooper** discusses the six categories that merit special attention from brand protection professionals

As companies are making new gTLD-related (generic top-level domain) decisions regarding where to register, block and police, having a thorough understanding of the different categories of top-level domains (TLDs) can provide a much needed starting point. Each of the "Super Six" categories of TLDs has special considerations that must be evaluated before taking any course of action. Here is a breakdown of the Super Six categories of TLDs to help you make more informed decisions about your domain portfolio strategy.

The generic TLDs

Let's begin by looking at the first category of TLDs, the generics. These include TLDs such as .app, .blog, .news, .sucks and .web. While this set of TLDs could easily be folded into one of the other five groupings, they are so truly generic in nature that they deserve their own category.

Many of these TLDs are not likely to launch in the near-term, as they are hotly contested with multiple applicants seeking to acquire them. Regardless, these are the TLDs that are expected to generate the largest numbers of registrations, and for that reason alone, brand owners must take note. The real question then becomes whether to block, register or simply police.

For some truly unique brands, blocking might make perfect sense if it is an option offered by the registry. However, if a particular trade mark is a dictionary term, it is possible that the corresponding domain may be deemed as a premium domain, in which case the block will not apply and the domain will be made available for registration at a higher price point. Also, for brands that share the same name as others, but are protected in different parts of the world or in different classes, blocking will work as a defence against cybersquatters but will not prevent other brands with legitimate rights from registering the domain.

Gripe sites TLDs

The second set of TLDs, the gripe site TLDs, presents a much more complicated set of issues. When a company says that it is not going to register even one new gTLD registration – whether because it is planning to utilise the new URS (Uniform Rapid Suspension) or leverage the trusty UDRP (Uniform Dispute Resolution Policy) – I urge them to take a second look at TLDs like .fail, .feedback, .wtf, .reviews and .exposed.

I believe that it is completely reasonable to expect that these TLDs could be legitimately used to direct traffic to websites where unhappy customers of products and/or services could post their experiences. That is the crux of the reason why a successful URS or UDRP may be difficult to obtain. With both the URS and the UDRP, a successful complainant must show that the domain was registered in bad faith. Given this, relying on either of those methods could prove extremely difficult in recovering or suspending these types of registrations.

As is the case with any TLD, registering an exact-match trademark as a domain will not protect against speculators from registering variations, typo-squats and misspellings. However, many companies feel that there is something particularly distasteful about seeing exact-match registrations of their brands in conjunction with .sucks or .wtf, and are willing to register them defensively.

Vice sites TLDs

This category of TLDS which include strings such as .adult, .porn and .poker generally elicits two distinct set of responses from brand owners. Some brand owners have absolutely no interest in registering these adult-oriented TLDs and ask: "Why would I ever need or want these?" Meanwhile, for companies whose brands are particularly

One-minute read

Many brand owners are concerned that the new gTLDs are creating more opportunities for cybersquatting and trade mark infringement. In particular, six of the new top level domains deserve special attention from rights holders. The generic TLDs, such as .app or .blog, may be among the most hotly contested, while the gripe site TLDs, such as .sucks, may prove difficult for brand owners to recover or suspend. The vice site TLDs look to be particularly unique challenges for companies with especially family-friendly brands. The corporate identifier and charity TLDs can potentially prove to be confusing for consumers, and certain industries, such as travel and leisure, may want to pay close attention to registrations in the geographical TLDs.

Is the URS Right for You?

With more than 400 delegated registries and over two million new gTLD registrations, incidents of cybersquatting are becoming commonplace for well-known marks. Many brand owners are now looking to the URS as a possible solution for quickly remediating domain name abuse.

The URS provides an inexpensive, expedited arbitration process for dealing with instances of clearly infringing new gTLD domain name registrations. Domains that are the subject of a successful URS ruling are suspended for the remainder of the registration term, or can be renewed for an additional year at the current registrar.

With a filing fee of just $375 and a formal complaint that can be no longer than 500 words, it is clear why so many are taking a closer look at this option. And if you're looking for a way to get almost immediate gratification, filing a URS complaint might just fit the bill, as decisions can be handed down within a week's time.

However, while you may be able to redirect an infringing domain relatively quickly to a website stating that the domain has been suspended, you will not be able to update Whois contact information. Contact information for the domain will continue to show the original infringing registrant. Moreover, the domain must remain at the registrar where it was initially registered.

The biggest downside of the URS is that there is no transfer mechanism. The domain will become available for registration again at expiration, which means that brand owners are forced to monitor the domain after it becomes available for registration or they must place a snap on the name in order to attempt recovery at expiration. Of course, there is never a guarantee that domains can be recovered when they become available for registration again.

So what should you do if you need the domain transferred? Start by contacting the registrant and informing the owner that the domain is infringing and ask that the name be transferred. Including an offer to cover the registration costs is one approach to consider and can help to speed up the process. If the registrant does not comply, then following-up with a more formal Cease and Desist may be the next step. In the case that the registrant still does not comply, consider a UDRP, which provides for a transfer mechanism. Of course, there may be cases where going straight to a UDRP may be best due to the risk of cyberflight and/or timing requirements.

focused on families and children, there is often a strong response and desire to protect against their brands appearing in conjunction with terms like .porn or .sex.

Unlike with the gripe site TLDs, companies should be able to use the URS or UDRP to suspend or recover sites registered to a vice site TLD, assuming that the domains are used in bad faith and infringing well-known marks.

The decision to defensively register brands as domains in these potentially objectionable extensions is really one about risk tolerance. For some , there is little concern and a willingness to absorb this risk. For others, these registrations would pose a serious problem given their focus on families and children.

Corporate identifiers

Corporate identifier TLDs include strings such as .inc, .ltd and .gmbh. Initially, when the list of applied-for TLDs was posted, this category was identified as posing significant risk to well-known brands as the combination of company names with these TLDs would have given the appearance of legitimate ownership. Last year ICANN's Governmental Advisory Committee (GAC) identified these strings as presenting risks and advised that: "Strings that are linked to regulated or professional sectors should operate in a way that is consistent with applicable laws. These strings are likely to invoke a level of implied trust from consumers, and carry higher levels of risk associated with consumer harm."

The GAC also advised that the following safeguards should be implemented (quoted directly from the GAC advisory):

1) Registry operators will include in their acceptable use policy that registrants comply with all applicable laws, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.
2) Registry operators will require registrars at the time of registration to notify registrants of this requirement.
3) Registry operators will require that registrants who collect and maintain sensitive health and financial data implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law and recognized industry standards.
4) Establish a working relationship with the relevant regulatory or industry self-regulatory bodies, including developing a strategy to mitigate as much as possible the risks of fraudulent, and other illegal, activities.

Additionally, for those TLDs associated with regulated markets an additional set of safeguards were advised:

1) Registrants must be required by the registry operators to notify them of a single point of contact which must be kept up-to-date, for the notification of complaints or reports of registration abuse, as well as the contact details of the relevant regulatory, or industry self-regulatory, bodies in their main place of business.
2) At the time of registration, the registry operator must verify and validate the registrants' authorisations, charters, licenses and/or other related credentials for participation in that sector.
3) In case of doubt with regard to the authenticity of licenses or credentials, Registry Operators should consult with relevant national supervisory authorities, or their equivalents.
4) The registry operator must conduct periodic post-registration checks to ensure registrants' validity and compliance with the above requirements in order to ensure they continue to conform to appropriate regulations and licensing requirements and generally conduct their activities in the interests of the consumers they serve.

In response to the GAC advice, registries are required to adhere to the PIC Spec (Public Interest Commitment Specification) as part of their registry agreement with ICANN to specifically address the GAC Advice. Any registry in violation of the PIC Specification is subject to the Public Interest Commitment Dispute Resolution Policy (PICDRP). The PICDRP allows a complainant to challenge a new gTLD registry that is complying with the Public Interest Commitments made in their application for a new gTLD. Examples may include failure to provide special rights protection mechanisms, or registration restriction policies that were promised as part of their registry agreement.

Does all of this mean that companies no longer need to be concerned with the corporate identifiers?

Probably not.

It is still unknown how strenuous the registration policies will be, or whether they will be proactively monitored for compliance by ICANN. If these namespaces remain as clean as the .edu or .gov TLDs, then there will be nothing to worry about. However, if the registries themselves are not enforcing their registration requirements, putting the onus on the brand owner to monitor for abuse, then companies will still be at risk for impersonation and

fraud. Over time, we will certainly learn more about what the risks really are.

Charitable TLDs

These TLDs includes strings like .charity, .foundation and .gives. And similar to the corporate identifiers, these strings were also identified by the GAC as posing special risks.

Undoubtedly, these TLDs have the potential to be used to commit fraud. In particular, for companies that run large foundations or where philanthropic endeavours are a major part of their culture, there is the risk of impersonation where criminals may use these TLDs seeking donations.

Again, while these TLDs may have promised in their registry agreement with ICANN to mitigate the potential for fraud or other illegal activity, it is unknown at this time whether registries will comply with their PIC Spec, and whether ICANN will monitor for compliance, or whether it will still be on the shoulders of brand owners to proactively monitor for abuse and take appropriate action.

Geographical TLDs

The final category of TLDs is the "Geographical TLDs." These include TLDs such as .NYC, .Tokyo and .London, .Paris, .Berlin and .London already appear to be gaining some traction as both are among the top 10 most popular new gTLDs. Generally speaking, when making registration blocking and policing decisions, a good rule of thumb is to focus only on exact-match registrations where there is a close nexus to the brand. So for these TLDs, companies should ask themselves whether these locations are specifically related to their brands. Travel and leisure, and retail brands should pay especially close attention to these TLDs as they launch.

On managingip.com

ADNDRC releases its first URS decisions, June 2014

The internet can be a ridiculous place, May 2014

Brand owners share their gTLD strategies, April 2014

So, is that it?

You may be saying to yourself by now, "Wow that's great, that's all I have to look at!"

Not so fast.

Depending on the vertical (pharma, financial, media, travel, high-tech or retail), there are dozens of other industry-specific TLDs to be evaluating. However, with over 600 registries launching over the next few years, categorising, identifying and tracking TLDs of concern will be critical when making registration, blocking and policing decisions.

The good news is that the rate at which new gTLD registries have been launching is expected to slow down in 2015. The bad news is that some of the most sought-after and desirable new TLDs will also be launching then, so even greater review and analysis will be necessary to make the right decisions for your brands. Every brand should examine this short list of TLDs carefully to determine whether a registration is necessary. By the time that many of these TLDs become available for registration, we should know much more regarding adoption rates, abuse trends and URS efficacy.

Elisa Cooper