ASPATORE SPECIAL REPORT

Navigating ICANN's New Rules Regarding Generic Top-Level Domain Names

An Immediate Look at the Opportunities and Challenges That Come with the New gTLD Program

ASPATORE

Understanding the Many Challenges Involved in Registering New gTLDs

Brad Newberg and Judy Harris

Partners

Reed Smith LLP

ASPATORE

Introduction

If current plans are implemented, the number of top-level domains—the characters to the right of the dot in an Internet domain name such as .com or .edu—will expand from a couple of dozen to thousands in the next few years. The opportunities for trademarks to be abused in this new system are endless. It is incumbent upon every brand owner to learn the ins and outs of the planned new system and to strategize regarding the best ways to protect their brands in this new environment. What follows will give you a head start in that endeavor.

Generic Top-Level Domain Names: New Rules

There are approximately two dozen generic top-level domains (gTLDs) currently on the Internet, such as .com and .net, as well as various country codes, such as .uk. Just about all domain names can be found attached to one of these TLDs, with .com being, by far, the most popular. There are also certain special community-sponsored domains (e.g., the new .xxx for adult entertainment).

Recently, the Internet Corporation for Assigned Names and Numbers (ICANN) began implementation of a plan to dramatically expand the number of TLDs. With certain very narrow limitations, under the plan, organizations located anywhere in the world will be able to apply to operate a TLD corresponding to just about any string of letters, English or otherwise; and that means almost any word or phrase, including an organization's name or brand. As an example, Reed Smith operates under a homepage of www.reedsmith.com but could have applied for .ReedSmith and thereby had the ability to establish domain names such as www.lawyers.reedsmith or www.trademark.reedsmith, combining its TLD with second-level domain names.

There are three types of TLDs that will be relevant to most companies in this new world: 1) brand names, such as .ReedSmith; 2) generic terms, such as .lawyer, .shoes or .music, or as we found out once the applications were revealed, terms like .lol or .app; and, 3) "community-based" TLDs, where a "registry" purports to act as the representative of a particular community and has pledged to operate a TLD for the good of that specific group as a

whole. An example is .bank, run by an entity that is known among, and has promised to represent members of, the banking industry.

ICANN states that the expansion program's purpose is to open up the Internet, increase competition and innovation, and facilitate global access by allowing new TLDs to be in non-Latin scripts. ICANN's critics, however, have been skeptical. They believe that these imminent changes to the Internet ecosystem have been driven primarily by those entities that stand to profit from the confusion that will be created by the expansion.

Potential Effects of the New ICANN gTLD Program on Internet Users

In terms of the goals of the program as stated by ICANN, we believe that it is highly unlikely that the new program will be successful. One need look no further than the recently revealed list of applicants to see what percentage of those applicants are either already well-established, enormously powerful entities such as Google and Amazon, or entities, such as Donuts (which has paid over $50 million to apply for more than 300 TLDs), formed solely to take advantage of a perceived opportunity to make money selling second level domain names and/or "flipping" TLDs for short-term profit. An embarrassingly small percentage of the revealed applicants come from developing countries or are applying for TLDs in non-Latin scripts.

That said, it is possible that certain generic TLDs could prove useful, and that certain brands will be able to use their TLDs to market products and services in new and creative ways. For example, the American Bankers Association, which has applied for .bank as a community TLD, contends that it will require, among other things, banks which wish to purchase a second-level domain name on .bank to meet certain high data and cyber security standards and, thus, consumers dealing with an entity whose Internet address ends in .bank, will know that the bank they are dealing with has met those standards. Brands might take advantage of the new system and try to market their TLD as the one place to go for information about that company and can come up with domain names that, when combined with the TLD, create witty and memorable puns, or can offer more personalized second-level domains for consumers.

For the most part, however, the new system is likely to cause mass confusion without any tangible benefits. It will also certainly make the fraud, cybersquatting, and typosquatting (when an entity secures a domain name that is a common typo of a well-known brand, for example gooogle) issues already prevalent on the Internet exponentially worse.

Right now, the majority of Internet users find most of the websites for which they are looking by entering terms into a search engine, such as Google. What the TLD expansion will almost certainly ensure is that those numbers will increase from the majority of, to just about all, Internet users.

The average Internet user is still not aware of this imminent massive change to the Internet environment, even though it is already well underway. Once ICANN's plans are fully implemented, which might happen within calendar year 2013, that average Internet user, at least without a massive publicity campaign that seems highly unlikely to occur, will have no idea which generic TLDs are out there, which brands have adopted their own TLDs, and so on. At least under the current system, if you are looking for a company, you can try to type in a .com url. Soon, an Internet user will not know whether the company still uses .com as its main hub or uses its own .brand or a .industry generic TLD. For example, if I am looking for my favorite rum company—let us call it "BrandX"—once these new TLDs are operational, I will not know whether to go with brandx.com, brandx.brandx, brandx.rum, brandx.alcohol, brandx.liquor, brandx.spirits, and so on. Each of those TLDs might or might not exist under the new system, and the resulting chaos will likely frustrate even the most sophisticated Internet users, causing them to navigate around the system by even heavier reliance on search engines.

Impacts of the New ICANN Rules on Attorneys and Clients

Those clients that have not applied for their own TLDs, as well as those that have, will need to strategize with their attorneys to develop a plan to efficiently and effectively patrol a vastly expanded environment for instances of infringement, piracy, cyberquatting, typosquatting, and the resulting consumer harm and confusion that may adversely affect a client's business interests.

Because of the enormity of the challenge going forward, it will be necessary for attorneys and their clients to (1) identify early on those new TLDs most related to the clients' brands and the industries in which they operate; (2) prioritize which of the identified TLDs will be most likely to cause them harm; (3) develop a plan for ongoing monitoring of the potentially most problematic TLDs, and, (4) be prepared to enforce their rights as necessary, using—as best they can—the minimal protections in the new system, as described below, and existing trademark protections, based on an assessment of the likely marginal benefits of each enforcement effort.

Internal and external counsel, working together, should develop a plan well in advance of the new TLDs becoming operational, so that all instances of cybersquatting, typosquatting and similar behavior can be handled in a uniform fashion, without having to convene meetings and develop new approaches each time a new problem is discovered. Planning ahead will streamline the process and cut down on costs later on.

Ultimately, the companies which will benefit most from this new gTLD program are: those which operate search engines; companies involved in the sale of domain names or the operation of registry functions; cybersquatters and typosquatters; monitoring services offering to spot such cyber and typosquatters; and, any other entities that can find a way to profit from consumer confusion. Attorneys who are proactive in helping their clients operate lawfully in this new environment and in protecting their clients from those companies that do not will also benefit from the critical services they will be providing.

Protecting Trademarks from Potential Consumer Confusion and Infringement

With respect to what business owners can, and should, be doing, with the help of their attorneys, to protect their interests, as described above, the three key answers to this question are: strategize, strategize, strategize. At a minimum, starting right now, brand owners should:

1. Review the list of TLD applications and ask themselves whether any infringe their trademarks. Are there any with respect to which the brand owner would want to file a formal objection?

2. If the brand owner filed any TLD applications, are there other applications to which that brand owner should object because the strings applied for in those applications are confusingly similar to the string for which the brand owner applied or which it already owns? (Consider, for example, the following pairs of names, each of which is the subject of a pending application filed by a different applicant: .Accountant and .Accountants; .Date and .Dating; .Fit and .Fitness; .Game and .Games. While these true examples are all generic terms, specific brand names could also have confusingly similar strings to generic terms such as .kia to .kid or to each other such as .visa to .vista.
3. If there are generic TLDs for the industry in which the brand owner operates being applied for by one of that brand owner's competitors—or by a third party intending to run the TLD for profit—does that make the brand owner uncomfortable? If so, that brand owner should consider its options. Perhaps a trade organization or a significant number of entities in the same industry could join to file a community objection.
4. Many of the TLDs applied for will be irrelevant to the business of any given brand owner (*e.g.*, a law firm likely will not care about .shoes, but might want to follow or monitor .lawyers). Each brand owner must decide which of its trademarks it wishes to register as second-level domains and where (on which TLDs) it wants to register them. These decisions should be made very soon.
5. The brand owner should decide whether it will be monitoring all, or just some, of the TLDs upon launch for infringement of its marks. This strategic decision will be different for every company. Some companies may decide that for their most important brands, they need to monitor and enforce certain TLDs regardless of the TLD's relevance to their industry. Some will want to pick and choose. Some will decide that there are brands for which it is not worth the cost and expense of monitoring and enforcement in this new system.
6. For any and all marks which a brand owner wishes to vigorously enforce in this new system, as well as for those which the brand owner thinks will be likely targets of cybersquatters or typosquatters, it will need to get those marks on the Trademark Clearinghouse list, described below. The Clearinghouse is scheduled to open in October 2012, and the expected cost of a

listing in the Clearinghouse is approximately $150 per trademark. Therefore, companies with thousands of marks may need to make some strategic choices as to their priorities.

7. It is incumbent on brand owners to know the trademark protections—limited as they may be—that are present in the new system, so that they can take advantage of them or make educated choices regarding the marks for which they might use the protections.

In addition to starting to strategize, as suggested above, to protect one's interests, the very first step business owners should take if they have applied for a TLD is to check the list of applications that was published earlier in 2012 to see if another entity or other entities have applied for the same or a confusingly similar name to the one or ones for which they have applied. If another entity has applied for the same name or a similar string, the company needs to evaluate how much it is worth to it to "win" the applied-for TLD, prioritize its goals, and develop a strategy for attaining those goals. This stage of the process is fraught with risk, and it is important that the business' strategy be developed in consultation with an attorney. Guidance provided by ICANN, for example, encourages private discussions between or among those entities that have applied for the same or very similar TLDs. However, there is every reason to believe that the antitrust laws will apply to any such discussions, so companies should exercise extreme caution before sitting down to talk, with actual or potential competitors about, for instance, jointly developing a bidding strategy for any auction that might follow (or to avoid such an auction) or agreeing to any market allocation or to a venture to operate jointly a particular TLD. Such discussions could be fine under certain circumstances and potentially extremely problematic in others.

Raising Objections

The seven-month formal objection period started on June 12, 2012, when the public portions of the applications for new TLDs were posted; that period is currently scheduled to close on January 12, 2013. The filing of an objection starts a dispute resolution process that can cost anywhere from a couple thousand dollars to tens of thousands of dollars per party, depending on the type of objection chosen (since each type of objection goes before a different arbitration organization), the number of arbitrators

requested, and the number of objectors, among other factors. A formal objection opens an arbitration process that must be ruled upon before an application can be approved and a TLD can launch.
There are four grounds on which one can base a formal objection. The first is "string confusion," whereby an existing TLD operator or an applicant for a new TLD (but no one else) can object on grounds that the applied-for string is confusingly similar to the objector's existing TLD or the name sought in its new TLD application. For example, a quick look at the list of applications for existing TLDs reveals such close overlaps as .Accountant and .Accountants; .Date and .Dating; .Fit and .Fitness; .Game and .Games, and scores more as well as many applications for the identical words.

The second type of formal objection is a legal rights objection, which, in most cases, would be filed by a trademark holder claiming that the objected to TLD application, if approved, would violate the objector's rights. This objection would be filed against an applicant who is seeking a TLD that is identical to a mark in which the objector has a protected legal interest. It might also be used in the case of an entity seeking to own a TLD that seems designed to confuse consumers into believing it is associated with a legally protected mark, for example, if an applicant were to file to operate, say, .AmericanAirline (instead of American Airlines).

To prevail with respect to such an objection, the rights-holder objector must show that it has a valid trademark (whether registered or unregistered) and that the potential use of the applied-for TLD by the applicant being challenged would take unfair advantage of the distinctive character or reputation of the objector's mark, would unjustifiably impair the distinctive character or reputation of the objector's mark, or would otherwise create an impermissible likelihood of confusion between the applied-for TLD and the objector's mark. The standard to win a legal rights objection is a hodgepodge of standards from different countries and different types of existing proceedings, and the arbitrators may look at all or just a few of the factors from these standards in coming to a conclusion.

The arbitrators who hear such disputes will be given a list of non-exclusive factors they may review in ruling on the objection, including: whether the applied-for TLD is identical or similar, in appearance, phonetic sound, or meaning to the objector's existing mark; whether the objector's acquisition

and use of rights in the mark has been bona fide; whether the mark is recognized in a sector relevant to the applied-for TLD; the applicant's intent in applying for the TLD; whether and to what extent the applicant has used, or has made demonstrable preparations to use, the TLD in a way that does not interfere with the legitimate exercise by the objector of its mark's rights; whether the applicant has marks or other intellectual property rights corresponding to the applied-for TLD; whether (and to what extent) the applicant has been commonly known by the applied-for TLD, and if so, whether any purported or likely use of the TLD by the applicant is consistent therewith and bona fide; and whether the applicant's intended use of the TLD would create a likelihood of confusion with the objector's mark as to the source, sponsorship, affiliation, or endorsement of the TLD.

The third ground on which one can base an objection is that the TLD application being opposed is strongly against the public interest. It should be understood, however, that this public interest objection is very limited. An entity objecting on this basis must show that the offending string goes against generally accepted norms of morality and public order. For example, multiple applicants are seeking to operate .sucks as a top-level domain name. It is likely that there will be limited public interest objections filed against .sucks. Whether those objections will be successful remains to be seen.

The last type of objection is a community objection, which has a specific standing requirement (like the legal rights objection). To object on this basis, an objector must be an established institution, associated with a clearly defined community, and must be able to demonstrate that there is significant opposition to the TLD application from the defined community to which the offending TLD would be targeted. This objection can be filed against an application regardless of whether the application itself was labeled a community application when it was filed. The community objector must also show that there would be a detriment to the targeted community if the applicant were granted the TLD. For example, the American Bar Association might file a community objection against the TLD .USlawyers, especially if it appeared that the applicant or applicants for these names were associated with a network of cybersquatters or individuals who, in the past, had fraudulently represented themselves to be attorneys barred and qualified to practice law in certain jurisdictions.

All proceedings to resolve disputes created by formal objections are scheduled to take place after the seven-month objection period has closed, regardless of when the objections are filed, as long as they are timely. The objection proceedings will be heard by different dispute resolution panels than those responsible for the general evaluation of TLD applications. It is expected that, even if an application is eventually approved, it is unlikely that an objected-to application would launch before late 2013.

Trademark Protections and Dispute Resolution Procedures at the Second Level

Once TLDs are awarded and names that have been successfully secured are deposited into the Internet root and become available for use, Registries (those entities which will operate the new TLDs) will be free to start offering second level domain names—those letters that will appear to the left of the new TLDs. An example could be WellsFargo in the Internet address "WellsFargo.bank." It is on this second level where most companies and law enforcement entities believe that the preponderance of fraud, cybersquatting, typosquatting and general consumer confusion will occur. There are certain trademark protections (with many gaps, as described below) that have been built into the system by ICANN that will become available to mark holders with respect to second-level domain names, once TLDs are granted.

These second level domain protections include: (1) a Trademark Clearinghouse list on which companies can list their marks and be eligible for some of the protections outlined hereinafter; (2) a sunrise period for the first thirty days after the launch of any TLD, during which time trademark owners can purchase second level domain names corresponding to their registered marks (placed on the Clearinghouse list) before open registration begins for the public; (3) a process whereby during the first sixty days of open registration to the public: (i) registrants (those who purchase second level domain names) will be warned if they try to register as a second-level domain name a mark that is on the Clearinghouse list, and (ii) trademark owners which have listed their marks on the Trademark Clearinghouse list will be notified if such marks do get registered by someone else as second level domains; and, (4) a Uniform Rapid Suspension Process (URS), which is designed to be similar to, but less expensive than, ICANN's Uniform Domain Name Dispute

Resolution Process (UDRP), which is the current method for resolving domain name disputes.. Unlike the UDRP, however, the URS will only allow a complainant to freeze a name, not get it transferred. Finally, there are procedures that can be invoked against registries themselves that are abusing trademarks, not following ICANN policies, violating terms of their Registry Agreement with ICANN, or not adequately protecting the interests of communities they have undertaken to represent.

The problem with the new protections, in general, is that they contain many gaps. Also, not every protection is set in stone: ICANN has been unable, for instance, to find providers for the URS who are willing to offer the rapid take-down service for the low fixed price that ICANN has promised. Therefore, it is possible that the cost of utilizing the URS might have to be raised to a price point that effectively makes it worthless, when compared to the typical Uniform Domain Name Dispute Resolution Process currently in place for all domain names.

The biggest shortcoming in the system is that almost all of the new protections put the burden on the trademark owner (at least after a very brief initial period) to engage in substantial monitoring activities and to take action themselves against fraudsters, cybersquatters and typosquatters. Moreover, the new protections only cover exact trademark copying and, after the first sixty days that a TLD is open for enrollment, a registry is not required to notify a trademark owner—even for trademarks on the Clearinghouse list—when a second level domain name with the identical trademark has been registered. Therefore, enforcement of trademark rights in general, as well as utilization of the new protections, will require a tremendous amount of time and expense on the part of brand owners. As of this writing, many stakeholders and constituency groups are fighting for enhanced protections, but what, if anything, comes of their efforts remains to be seen. The protections and flaws in those protections are discussed in more detail below:

Trademark Clearinghouse

The Trademark Clearinghouse is intended to function as a central warehouse in which information pertaining to the rights of trademark holders will be authenticated, stored, and disseminated. In particular, the

Clearinghouse will be a database of trademarks that supports pre-launch trademark claims and sunrise services by providing information to new TLD registries. Trademarks that can be listed and protected include, for the most part, nationally or regionally registered word marks; word marks that have been validated through a court of law or other judicial proceeding; word marks protected by statute or treaty; and other marks that constitute intellectual property, such as common law marks and design marks that contain word elements. However, for marks not protected through a court, statute, or treaty, mark holders must provide evidence of use in connection with the bona fide offering for sale of goods and services prior to application for inclusion in the Clearinghouse.

The Trademark Clearinghouse database is structured to report to registries and mark holders only when potential registrants are attempting to register a second level domain name that is considered an "identical match," which is limited to domain names that consist of complete and identical textual elements of a trademark. Thus, the new gTLD rights protection mechanisms will not provide mark holders with notice of, nor significant protection against, typosquatting or uses of any confusingly similar strings.

Sunrise Services

New gTLD registry operators, for a minimum of thirty days before second-level domain registrations are open to the public for that gTLD, must allow trademark holders the exclusive right to register second-level domain names corresponding to their marks. This is referred to as a "sunrise" period. Of course, the trademark holder will have to pay for the domain name registration like any other registrant. In addition, whether or not trademark holders register the domain names, for the same period—again, known as a "sunrise" period, registries must notify trademark holders with marks on the Clearinghouse list if someone seeks to register a second-level domain name using the trademark holders' mark, so that the trademark holder can move to object to the registration.

During the sunrise period, the registry only has to honor those registered marks for which "use" has been demonstrated, meaning that it does not have to give a company the right to register a domain name during the sunrise period if the mark sought to be obtained as a domain name is not

currently being used. The intent of this requirement is to help ensure that those who have the power to exclude others from using a domain name with a trademarked term are not abusing that power. However, a consequence of this requirement is that some companies will be precluded from filing Uniform Rapid Suspension complaints or defensively registering their brands during a sunrise period. For example, companies who have filed "intent to use" applications with the United States Patent and Trademark Office (USPTO), but who have yet to use such marks, are left in the position of having to challenge bad faith registrations in UDRP proceedings after such registrations have issued.

Trademark Claims Services

For the first sixty days that domain name registration in a new TLD is open to the public, new TLD registry operators must provide to potential second-level domain registrants clear notice if those potential registrants try to register for domain names corresponding to exact trademarks in the Trademark Clearinghouse. Registries may choose to offer this protection for longer than sixty days, but only sixty days are required. Moreover, even the briefly required notice does not stop the potential registrant from registering the domain name; it merely alerts the potential registrant that it may be in for a fight if it chooses to go forward. If the potential registrant then goes through with the registration, the trademark holder will be provided with notice that this has occurred, in case the trademark holder wants to take action.

Since TLD registry operators are only required to offer trademark claims services during the initial launch period, it will be difficult, long-term, for trademark holders to protect against bad faith registration of domain names. Infringement of rights will inevitably occur not just in the launch phase, but also for as long as a TLD is active. Since there are no built-in mechanisms whatsoever to help trademark owners monitor the registration of identical or confusingly similar domain names after the sixty-day period expires, the cost and burden of identifying and challenging bad faith registrations will be much greater than if the notices of possible infringement were required for as long as second level registrations were open. Furthermore, since the limited rights protection mechanisms only address "identical match" infringements, trademark owners need to have a monitoring team (or outsourced monitoring company) working seamlessly

with their legal teams to best police against the domain name registrations of cybersquatters and typosquatters. Finally, even for the brief period when notices are required, both the burden of moving forward and the financial burden will be on the trademark holder to take action to freeze or transfer the registration. The cost, however, of ignoring infringements could, potentially, be a lot greater.

Uniform Rapid Suspension

Uniform Rapid Suspension (URS) is a method by which trademark owners can "freeze" infringing domain names where there is no genuine contestable issue as to the infringement and abuse that is taking place. It was expected when ICANN announced this system, that for a fee of $300, trademark owners would be able to submit a complaint and have notice sent to the domain name registry so that it could immediately "freeze" the infringing domain name. However, ICANN has made it clear since the announcement of this remedy that there is almost no chance it will be able to find a dispute resolution provider that can come close to a $300 price point. It is possible that by the time this chapter is published, ICANN will have to charge much more for use of the URS system. ICANN has affirmed that it will not abandon the idea altogether.

The URS procedure will be very similar to a UDRP proceeding. In the URS proceeding, trademark owners will have to establish by clear and convincing evidence that (1) the domain name is identical or confusingly similar to a valid mark, (2) the registrant has no legitimate rights or interests in the domain name, and (3) the domain was registered in bad faith. If they are able to do so, the infringing domain name will remain "frozen" for the remainder of the registration term. However, unlike UDRP proceedings, prevailing in a URS proceeding will not result in the cancellation of the domain name or the transfer of the domain name to the trademark owner. Brand owners who want additional remedies will still have to file a UDRP proceeding or a lawsuit against the registrant.

Procedures Against Registries Who Are Not Acting Appropriately

In addition to second-level domain protections, there will be processes to handle disputes with respect to TLDs after they have launched. These

include the Post-Delegation Dispute Resolution Procedure (PDDRP) and the Registry Restrictions Dispute Resolution Procedure (RRDRP). The PDDRP allows a trademark holder to contest the way the registry is operating, if it owns a TLD close to a trademark and is abusing that proximity, or if the registry is actively encouraging infringing second-level domain registrations. The PDDRP will not involve damages or the transfer or freezing of domain names. It may, however, force registries to change policies or, in drastic cases, lose the TLD. The RRDRP is a similar mechanism for community TLDs, where the registry is not acting in the best interests of that community.

The PDDRP and RRDRP processes have very little teeth. It will likely take repeated violations by a registry before the registry owner is significantly punished. Even then, there is no possibility for damages, and the already issued domain names will have to be attacked individually.

The Impact of the April 2012 Security Glitch

The security glitch in April 2012 delayed the start of the gTLD evaluation process, as well as the comment, objection, and eventual launch process, by approximately two to three months. In addition, a separate glitch involved with ICANN's "digital archery" system—pursuant to which ICANN was going to break the applications down into batches and process them 500 at a time—led to the scrapping of that system and to ICANN's new plan to handle all of the 1,930 applications at the same time.

Both of these glitches have further weakened stakeholders' confidence in ICANN's ability to manage an unprecedented expansion of top level domain names and have made more apparent than ever the need for every company, whether or not it has applied for its own TLD, to have a well-developed plan to protect its intellectual property in the Internet ecosystem and sufficiently budget for the inevitable associated costs. Only constant vigilance and active involvement will protect trademark holders going forward. If they do not act to protect the value inherent in their marks, it is clear that no one else will act for them.

Future Outlook on the New ICANN TLD Rules

Most of the focus so far, both by the private sector and by concerned law enforcement agencies around the world (Interpol, the FCC, the FBI), has been on the enormous potential ICANN's TLD program creates for consumer confusion, cybercrime and cybersquatting/typosquatting. Virtually overlooked to date has been how the creation of more than 1,000 new TLDs might impact competition, and how the antitrust and competition laws will inevitably be implicated. Recently, in a decision in California, a federal judge denied defendants' motions to dismiss an antitrust action against ICANN and the operator of a new TLD, ruling that the Sherman Act applies to ICANN because the transactions involving the creation of new TLDs are commercial in nature, even nonprofit or charitable organizations, if they engage in commercial activity, are subject to the federal antitrust laws, and ICANN and Registries can be subject to suit for conspiring to violate the antitrust laws.[1]

It is already apparent that the potential opportunities to run afoul of the antitrust laws in this expansion of TLDs are numerous. For example, ICANN has encouraged applicants who find they are competing with others for a particular string to enter into private negotiations to resolve the conflict themselves and obviate the need for an auction, which is ICANN's plan of last resort to "choose" between or among overlapping applications, for all applicants which are deemed qualified to operate registries. In many instances, these applicants will be competitors in the market and all of them will be potential bidders at an auction, so extreme caution and consultation with an attorney is advised. Also, as another example, those entities which are ultimately successful in their bids to run registries for a defined community or for TLDs containing words associated with, for instance, a particular industry (say, .auto), would be well advised to seek counsel on how to manage their new TLDs without running afoul of competition laws around the world. Here too, the waters that must be navigated are filled with rough rapids. As a related matter, it will likely be challenging to define a relevant market or measure market power in this new environment, or to determine the market power that may be developed by virtue of controlling a particular TLD. The issues in this area are

[1] *Manwin Licensing Int'l S.A.R.L.v. ICM Registry, LLC*, 2012 WL 3962566 (C.D. Cal. Aug. 14, 2010).

numerous, and are only starting to penetrate the consciousness of attorneys and their clients and of the relevant enforcement agencies.

Conclusion

The jury is very much out, and so far the experts and scholars are skeptical about whether ICANN's imminent, unlimited expansion of the number of TLDs will have any benefits for competition, for innovation, for the fabled entrepreneur working in his or her garage, or for the consumer trying to save time and money searching for information, goods and services online.

Starting right now, businesses and attorneys should be conferring to develop strategies regarding how best to navigate in this new environment. Those businesses that have applied to operate TLDs should be taking steps to protect their business models and their names from encroachment and, if their applications are objected to or contested by other applicants seeking the same name, they should be developing and implementing a plan to rebut objections and to prevail in their quest to become a registry. Those businesses that have decided not to apply for new TLDs in this round should be reviewing the list of applicants and the names for which those applicants have applied to determine whether they wish to comment or file objections regarding any of the applications. At the same time, they should start studying how their competitors and others plan to use their new TLDs to decide whether this is something they might want to consider for themselves if and when ICANN opens another application window.

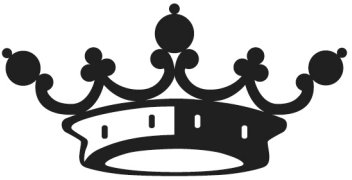
And *all* companies should be developing a strategy for monitoring new TLDs once they become operational to detect instances of cybersquatting, typosquatting and outright fraud in violation of their marks. Since the universe of new TLDs will be so vast, and monitoring and enforcement funds will undoubtedly be limited, businesses would do well to set priorities early on to implement their goals and protect the value of their brands in the most efficient and effective manner possible. Finally, whether a business is running a TLD, applying for a second level domain name on someone else's TLD, or operates in an industry where a TLD that is run by a competitor or by a community representative might be of concern, all entities must avoid violating the antitrust laws and be vigilant for such violations by others that might adversely impact their businesses.

***Brad Newberg**, partner with Reed Smith LLP, has extensive experience in all areas of intellectual property litigation, with a particular focus on copyright, trademark, and domain name matters. He has been practicing in the intellectual property field since the first day of his career and has been lead counsel on numerous cases, in addition to acting as a testifying expert in both copyright and trademark litigations. Mr. Newberg also regularly speaks and writes on all issues related to the Internet. He counsels his clients so that they may navigate through the waters of the different laws that affect social media and he is one of the firm's leading experts on ICANN's new system to expand top-level domain names. He works extensively with his clients to make sure their brands are protected in this new environment.*

***Judy Harris** is a long-time partner at Reed Smith LLP, resident in the firm's Washington DC office. She focuses her practice on Internet and telecommunications matters, as well as antitrust, competition and consumer protection issues before the Federal Communications Commission, the Antitrust Division of the Department of Justice, the Federal Trade Commission, in the courts and on Capitol Hill. In addition to her many years in private practice, Ms. Harris served as a senior trial counsel in the Antitrust Division and headed the Legislative Office at the FCC during debate and enactment of the Telecommunications Act of 1996. She has been deeply involved with ICANN's planned expansion of domain names and speaks and writes regularly on the topic.*

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.



ASPATORE