Lanham Act “False Advertising” Claims: What Is a Plaintiff to Do?
Vincent N. Palladino

Defensive Aesthetic Functionality: Deconstructing the Zombie
Anthony L. Fletcher

Anti-Dilution/Anti-Free-Riding Laws in the United States, Canada, and the EU: Bridges Too Far?
Daniel R. Bereskin, Q.C.

The New Generic Top-Level Domain Program: A New Era of Risk for Trademark Owners and the Internet
Dennis S. Prahl and Eric Null

A Century of Trademark Law—Looking Back and Looking Forward
Moderator: J. Thomas McCarthy
Speakers: Miles J. Alexander, Eric Goldman, and The Rt. Hon. Professor Sir Robin Jacob

Amicus Brief of the International Trademark Association in International Hair Cosmetics Ltd v. International Hair Cosmetics Group Pty

Amicus Brief of the International Trademark Association in PT Bintang Pesona Jagat v. PT Karya Tajinan Prima

THE NEW GENERIC TOP-LEVEL DOMAIN PROGRAM: A NEW ERA OF RISK FOR TRADEMARK OWNERS AND THE INTERNET

By Dennis S. Prahl∗ and Eric Null∗∗

I. INTRODUCTION

Trademarks and domain names have become inextricably intertwined over the years. Domain names can be registered as trademarks,1 they consist of or contain trademarks,2 and many brands and their owners are recognized primarily by their domain names.3 The Internet Corporation for Assigned Names and Numbers (ICANN)4 has recently approved a new way for entities to use, customize, and take commercial advantage of domains as a more significant part of their branding and business strategies. With the introduction of ICANN’s New Generic Top-Level Domain Program (“New gTLD Program” or “the program”), the interaction between domain names and trademark rights is about to take on even greater significance.

For the past several years, ICANN has been embroiled in a debate about whether gTLDs should be expanded beyond the twenty-two gTLDs already delegated.5 That debate resulted in the approval of the New gTLD Program on June 20, 2011.6

∗ Partner, Ladas & Parry LLP; President, Ladas Domains LLC, an ICANN-accredited domain name register; Associate Member, International Trademark Association.

∗∗ J.D. Candidate, Benjamin N. Cardozo School of Law, June 2012; Student Member, International Trademark Association.

1. TMEP (7th ed. Oct. 2010), § 1209.03(m); see STREETCARSHOPS.COM, Registration No. 4,008,318.


3. For instance, Google, Amazon.com, or eBay.com are businesses that do not have brick-and-mortar stores, yet are widely known.

4. ICANN coordinates the domain name system: “To reach another person on the Internet you have to type an address into your computer—a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn’t have one global Internet.” About, ICANN, http://www.icann.org/en/about (last modified Aug. 12, 2011).

5. The most common gTLDs are .com, .net, and .org, though there are nineteen more, see Top-Level Domains, ICANN, http://www.icann.org/en/tlds (last modified Aug. 13, 2011), and that number stands to increase substantially if ICANN’s New gTLD Program is successful and attracts many applicants.

6. Note that there are two broad types of top-level domains (TLDs)—generic (gTLDs) and country-code (ccTLDs). The new program is not an expansion of ccTLDs, which are two-character codes representing a country, such as .uk (United Kingdom) or .ca. (Canada). See
The New gTLD Program presents an opportunity for brand owners to utilize a new domain space for branding, marketing, and reaching foreign markets that were previously not readily accessible. The program gives corporate entities more choices regarding online presence, as they can now own a gTLD as well as a more traditional domain name under, for example, .com or .org. A corporation will be able to own a domain such as www.google.com and also the .google gTLD. The entity will have a good measure of control over how it wants to run the new gTLD. An entity may wish only to allow affiliated or authorized entities to be able to secure domain names under its gTLD, and then promote that fact to consumers, giving a measure of added trust to those domains. Alternatively, an entity may simply use the new structure as another means to steer Internet traffic to its primary address at www.google.com, which may increase market share. Companies also have the option to apply for an industry keyword, such as .toys or .fashion, instead of for a brand, such as .[brand]. With the potential for numerous new TLDs to be delegated, the program likely will fundamentally change the Internet as it is known today.

The efficacy of this program in actually changing how consumers interact with the Internet remains to be seen. The application period starts in January 2012, and new gTLDs will not be delegated for, on average, nine months to a year after the close of the application period in April 2012. However, a number of

generally J. Thomas McCarthy, Trademarks, Cybersquatters, and Domain Names, 10 DePaul-LCA J. Art. & Ent. L. 231, 240 (2000). The new program is an expansion of gTLDs only, which are (typically) three-characters long, such as .com, though the program allows for longer strings.

7. The existing gTLD system posed challenges to reaching foreign markets that use non-Latin character alphabets (such as Russian or Mandarin), because until recently, all existing gTLDs consisted of Latin characters only. Domain names in non-Latin characters are referred to as Internationalized Domain Names (IDNs), and ICANN has already launched some programs for IDNs. For example, there is a Russian-language gTLD, and .asia accepts domain name registrations in Chinese, Japanese, and Korean characters. In addition, ICANN has allowed gTLD applicants to include with their application an exact IDN. gTLD Applicant Guidebook, ICANN, § 1.3, at 34 (Sept. 19, 2011), http://www.icann.org/en/topics/new-gtlds/rfp-clean-19sep11-en.pdf [hereinafter Guidebook]. This article will not discuss the international aspect of the program in detail.

8. Note that only corporations may apply for a gTLD, no individuals or sole proprietorships allowed. Id. § 1.2.1, at 23.

9. It should be noted that the use of the term “generic” in the program should not be confused with “generic” in the trademark sense. The program uses the term to indicate that the TLD string is not a country-code TLD, such as .uk.

10. This could potentially decrease counterfeit and gray-goods markets if these corporations claim “only authorized retailers can use our .brand gTLD.”

11. Applications without significant delays may take only nine months from application to delegation, though applications subject to numerous objections, extended evaluations, and string contention resolution, may take up to twenty months. Id. § 1.1.3, at 18-19.
entities (including places such as Chicago and California, and companies such as Motorola and Canon) have announced their intention to apply for a new gTLD.\textsuperscript{12} ICANN predicts 400 or more applications following the first round.\textsuperscript{13} On the other hand brand-owners such as Hewlett-Packard and Procter & Gamble have announced that they are not participating.\textsuperscript{14}

Still other organizations have started campaigns aimed at stopping the program altogether. The Association of National Advertisers (ANA), for example, corresponded with ICANN in an effort to stop the program launch, claiming there are no material benefits from the program, and even if there were benefits, they are too attenuated, and the program needlessly forces brand owners to spend precious resources to prevent brand dilution.\textsuperscript{15} The movement is gaining momentum; the ANA and eighty-seven other major associations and businesses have formed the Coalition for Responsible Internet Domain Oversight to oppose ICANN's gTLD Program.\textsuperscript{16} The ANA is threatening legal action against ICANN if it follows through with the rollout of the New gTLD Program.\textsuperscript{17} ICANN responded that ANA had its moment to speak during the ICANN comments periods, it did speak, and its concerns have been addressed through that process.\textsuperscript{18} The ANA has not indicated the legal theory or theories on which it will rely if ANA proceeds to file suit. However, a potential roadblock to successful litigation may be satisfying the standing requirements of injury in fact, causation, and redressability.\textsuperscript{19} The ANA may find

\textsuperscript{12} Applicants for new gTLDs, .Nxt, http://dot-nxt.com/applicants (last visited Nov. 5, 2011).


\textsuperscript{14} \textit{P&G and HP Reject New gTLDS}, Managing Intell. Prop. (Nov. 8, 2011), http://www.managingip.com/Article/2931447/P-G-and-HF-reject-new-gTLDs.html. Neither Hewlett-Packard nor Proctor & Gamble would have been able to apply for their abbreviation HP and P&G, as ICANN has required strings to be at least three characters long and ampersands are not allowed. \textit{Id.}; see also infra note 96.

\textsuperscript{15} Letter from Robert Liodice, President and CEO of ANA, to Rod Beckstrom, President of ICANN, http://www.ana.net/getfile/16602.

\textsuperscript{16} \textit{87 Major Assns. and Businesses Join with ANA to Form Coalition to Oppose ICANN's TLD Expansion Program}, ANA (Nov. 10, 2011), http://www.ana.net/content/show/id/22351.


\textsuperscript{18} \textit{Id.}

\textsuperscript{19} Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992) (standing requires the following: (1) an injury in fact that is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical; (2) a causal connection between the injury and the conduct complained of, i.e. the injury must be fairly traceable to the challenged action of the defendant; and (3) it must be likely, as opposed to speculative, that the injury will be
similar trouble securing a preliminary injunction, which requires a showing of likely future harm.\textsuperscript{20} These determinations depend substantially on the characterization of the harm asserted (who is actually harmed, what the harm looks like), and whether the court views that harm as imminent and likely.

The program will affect not only those who choose to participate in the program, but also entities not planning to apply. Specifically, trademark owners who decide not to apply will feel the effects of the program in the form of increased monitoring to determine whether new gTLDs, or domain names registered under new gTLDs, conflict with their rights. Some trademark owners may also feel the need to apply to try to secure their .[brand] so as to prevent others who may have equal rights to the same .[brand] (such as owners of the same mark in other markets or fields of use) from securing the gTLD. Anheuser-Busch, for instance, may wish to apply for .bud to ensure that Budejovicky Budvar NP cannot, since both parties have longstanding disputes and competing claims to the BUD and BUDWEISER marks. Entities will also wish to monitor the filings in the New gTLD Program and timely object to the applications filed by others that may conflict with their trademark rights. Mark owners should also be aware of the increased opportunities for typosquatting and cybersquatting: as each new gTLD is delegated, it represents a new domain landscape potentially available for bad faith registration of infringing domain names. This kind of infringement is already a significant problem for many entities;\textsuperscript{21} the program will only exacerbate the problem of cybersquatting while simultaneously requiring increased monitoring to ensure protection of legal rights and necessitating more time, money, and effort in enforcement.

redressed by a favorable decision). The court may view the ANA’s injury as a generalized injury of the kind rejected in \textit{Lujan}, and thus dismiss the case on that ground. However, the court may think that the damage caused to the ANA and its constituents constitutes injury to a property right (a common law-type right), and as such would be regarded as injurious. Tenn. Elec. Power Co. v. Tenn. Valley Auth., 306 U.S. 118, 137-38 (1939) (in denying plaintiffs’ standing, the Court said standing is unavailable “unless the right invaded is a legal right, one of property, one arising out of contract, one protected against tortious invasion, or one founded on a statute which confers a privilege”) (emphasis added). Whether property means real property, specifically, or any type of property, would be left to the court. The court would also have to decide if the injury were imminent enough to warrant standing.

\textsuperscript{20} City of L.A. v. Lyons, 461 U.S. 95 (1983) (“absent a sufficient likelihood that [plaintiff] will again be wronged in a similar way, [plaintiff] is no more entitled to an injunction than any other citizen of Los Angeles. . . .”). Again, the attenuation could be a problem for the ANA, but since the program involves somewhat concrete delegation dates, the ANA could succeed.

This article will briefly explain domain names and how the Internet functions. It will then explain the New gTLD Program in detail. It will analyze the problems an increased number of gTLDs and the concomitant increase in new domain names will present to trademark owners, and will explain and critique the measures available for entities to protect themselves from infringement. It will then discuss the effectiveness of alternative remedies for trademark infringement post-delegation, and lastly will provide Best Practices for trademark owners, including those planning and not planning to apply for a gTLD.

II. OVERVIEW OF THE INTERNET AND DOMAIN NAMES

In order to understand the program, one must first understand the basics of domain names. TLDs are that portion of a domain name that appears after the last period. For example, .com, .net, and .org are TLDs; however, these are only three of many, including .biz, .info, and recently, .xxx. In the Uniform Resource Locator (URL) www.infa.org, “.org” is the TLD. Second-level domains (SLDs) comprise the name immediately to the left of the TLD—“inta” in the above example. The SLD is generally the portion of the string that identifies the brand or entity, though as more companies seek individualized gTLDs through the program, that could change. Third-level domains comprise the string immediately to the left of the SLD. The most common third-level domain is “www,” although the mobile website indicator “m” is gaining popularity as mobile phones become ubiquitous (for instance, m.yahoo.com is the mobile version of Yahoo’s website).

The Internet functions as it does because of URLs, Internet Protocol addresses (IP addresses), and the Domain Name System (DNS). Each computer on the Internet, including servers hosting web sites as well as machines of individual end-users, is assigned a numeric IP address. IP addresses are controlled and assigned by

---

22. See Kremer v. Cohen, 325 F.3d 1035, 1038 (9th Cir. 2003).
24. See Kremer, 325 F.3d at 1038.
25. Id.
26. It is worth noting that third-level domains are controlled by the owner of the second-level domain, and therefore are not delegated by ICANN or a registry. E.g., Yahoo controls m.yahoo.com.
27. Id.
the Internet Assigned Numbers Authority.\(^{28}\) That address looks like a series of numbers, such as 172.16.254.1,\(^{29}\) which is unique to that server or machine. However, people do not want (nor do they generally have the capacity) to memorize a series of numbers associated with each website they access. For that reason, the DNS exists to translate these numeric IP addresses into readable and memorable URL addresses.\(^{30}\) When one types “www.yahoo.com” into an Internet browser, the computer, with the help of the DNS, retrieves the website based on the IP address connected to the readable URL.\(^{31}\) The DNS must be very accurate to ensure users are brought to the requested websites rather than to no website or an unrelated website. The increase in gTLDs presented by the New gTLD Program could affect the security and stability of the DNS because of the potential for substantial unwanted traffic getting sent to unrelated websites.\(^{32}\)

Three primary entities play a role in the DNS. The first is the registry. The registry is the manager of the TLD.\(^{33}\) It ensures stability and accuracy of the DNS, namely, to correctly connect the domain name (the readable address) to the relevant IP address, and to make sure that connection is stable.\(^{34}\) The registry provides a master, or zone, file, which aggregates all SLDs under the registry’s TLD, and must be updated daily.\(^{35}\) The registry also provides a WHOIS service to enable the public to connect registrars to domain names within the registry’s TLD.\(^{36}\) Registrars are in charge of selling the SLDs and registering those SLDs with

\(^{28}\) Cf. Byers v. Intuit, Inc., 564 F. Supp. 2d 385, 425 n.88 (stating that IANA “is responsible for the overall coordination and management of the Domain Name System . . . and especially the delegation of portions of the name space called top-level domains . . .”).

\(^{29}\) Currently two types of Internet Protocol (IP) addresses are in active use: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 was initially deployed on January 1, 1983, and is the most commonly used version. IPv4 addresses are thirty-two-bit numbers often expressed as four octets in “dotted decimal” notation (for example, 192.0.2.53). Deployment of the IPv6 protocol began in 1999. IPv6 addresses are 128-bit numbers and are conventionally expressed using hexadecimal strings (for example, 2001:0db8:582:ae33:29). Number Resources, IANA, http://www.iana.org/numbers (last visited Sept. 5, 2011).


\(^{31}\) Cf. id. (“DNS, among other things, matches the Web page addresses that end users type into their browsers (or ‘click’ on) with the Internet Protocol (IP) addresses of the servers containing the Web pages the users wish to access.”)

\(^{32}\) See generally infra notes 90-95 and accompanying text.


\(^{34}\) Id.

\(^{35}\) Id.

\(^{36}\) Id. at 99-100.
the registry,\textsuperscript{37} which includes collecting data for a WHOIS service for its own domains.\textsuperscript{38} Both registrars and registries must be accredited by ICANN.\textsuperscript{39} Lastly, the registrant, also known as the holder, is the purchaser of the SLD.\textsuperscript{40}

III. THE NEW GENERIC TOP-LEVEL DOMAIN PROGRAM

A. Preparation and Application

The applications will be accepted in rounds, with the first round beginning January 12, 2012 and lasting through April 12, 2012.\textsuperscript{41} Importantly, new users cannot sign up for the TLD Application System (the system through which applicants must apply) after March 29, 2012, meaning an applicant must take the first step of the application process by registering for the system by the above date, or else miss the first round window.\textsuperscript{42} The dates for round two and later rounds have not been announced, therefore entities that “wait and see” what the competition will do may wait years before they get another chance to apply to own a gTLD.\textsuperscript{43}

The New gTLD Program provides for two categories of gTLDs: standard and community-based. A community-based application is for a TLD that will be operated for the benefit of a “clearly delineated community.”\textsuperscript{44} The applicant has the option of classifying the gTLD as standard or community-based, so a generic term or industry term can be classified as either depending on how the applicant would like to pursue the gTLD. An applicant seeking to classify its gTLD string as community-based must satisfy more onerous requirements: a demonstrated ongoing relationship with the relevant community; a demonstration of the strength of that ongoing relationship; proposed registration and use policies consistent with a community-based purpose; and having one or more endorsements from community members.\textsuperscript{45} Anything that is

\textsuperscript{37} Id. at 100. One concomitant effect of the new program is that it creates a market for registrars, as each new gTLD will need a registrar to sell SLDs to buyers.

\textsuperscript{38} Register.com, Inc. v. Verio, 356 F.3d 393, 395 (2d Cir. 2004) (“The ICANN Agreement . . . requires the registrar . . . to preserve [the WHOIS information,]” which includes applicant’s name, address, telephone number, and email).

\textsuperscript{39} Moringiello, supra note 33, at 100.

\textsuperscript{40} Id.

\textsuperscript{41} Guidebook, supra note 7, § 1.1.1, at 5-6.

\textsuperscript{42} Id. at 6.

\textsuperscript{43} The goal is to start round two within one year of the close of the first round. Guidebook, supra note 7, § 1.1.6, at 23.

\textsuperscript{44} Id. § 1.2.3.1, at 29. Note: the cost of a community priority evaluation is $10,000. Id. § 1.5.2, at 47.

\textsuperscript{45} Id. § 1.2.3.1, at 29.
not designated as a community-based application is a “standard” application.\footnote{Id. Application classification is at the discretion of the applicant. \textit{Id}.} Importantly, this designation cannot be changed once the application is submitted.\footnote{Id. § 1.2.3.3, at 31.} The owner of a community-based gTLD must have domain registration rules that are appropriate for the community purpose and likely will not be able to, for example, purport to run a gTLD for a community but prohibit registration of domain names to competitors who would otherwise qualify as members of the purported community. Despite these added restrictions, there is a potential advantage to a community-based application if there is a dispute between competing bids for the same gTLD. In some cases, ICANN is required to delegate the gTLD to the community applicant rather than another applicant, even if other applicants also apply under a community-based application.\footnote{This happens if the applicant prevails in a community priority evaluation, see generally \textit{id}. § 4.2, at 203-215.} This advantage can prove useful if multiple entities apply for similar strings.

During the application process (January through April) there is no transparency.\footnote{Id. § 1.1.4, at 19 (showing that nothing is published until the administrative completeness check, which is to be done at the conclusion of the application period in April 2012).} Only ICANN will see who is applying and what proposed strings are sought during that period. This means unless a company has publicly made its intentions clear, it is not possible to monitor the application process this early. In late April, about two weeks after the application period is over, ICANN intends to publish all the applications it received during the first round;\footnote{Id. § 1.1.2.2, at 8.} only at that point will competitor applications be known, and it will be too late for companies to respond to those competitors in that round. Administratively deficient applications (applications missing application components) will be rejected in that first two-week period during the “administrative completeness check.”\footnote{For now, all one needs to know is that the initial evaluation is the process by which ICANN determines validity of the applicants and applications.} Thereafter, in November 2012, ICANN intends to publish its “initial evaluation” results.\footnote{Gretchen Olive, Corporation Service Company Director of Policy & Industry Affairs, Domain and Brand Protection Seminar, \textit{New gTLDs—How Brand Owners Can Prepare for Their Launch} (June 29, 2011) [hereinafter Olive Presentation].} An application for a gTLD requires substantial preparation. In total, the application requires answers to fifty questions which may entail submission of approximately 250 pages of documents,\footnote{Id. Application for a gTLD requires substantial preparation. In total, the application requires answers to fifty questions which may entail submission of approximately 250 pages of documents.}
including proof of legal establishment, financial statements,\textsuperscript{54} 
information regarding applicant’s criminal history,\textsuperscript{55} and a variety 
of technical documentation.\textsuperscript{56} Compiling such a variety of 
documents and information requires coordination by multiple 
corporate departments, including legal, information technology, 
and financial, and may take a significant amount of time.

\textbf{B. Costs}

The costs of the application are significant. Initially, an 
applicant must supply a $5,000 deposit when registering for the 
TLD Application System, followed by a payment of $180,000 upon 
fil ing the application, before ICANN will begin its review.\textsuperscript{57} There 
are opportunities for refunds if the applicant changes its mind, but 
the refundable amount of the $180,000 fee quickly diminishes at 
each stage.\textsuperscript{58} If an application requires additional evaluation, these 
costs will increase. If an applicant must undergo a registry 
services review,\textsuperscript{59} the fee can be $50,000 and more.\textsuperscript{60} An 
application requiring dispute resolution for similarity with another 
proposed or existing string may involve additional costs of 
$1,000–$5,000 per party per proceeding.\textsuperscript{61} It is important to note 
that a dispute resolution proceeding may occur despite the 
applicant’s best efforts to avoid confusion because an objection may 
be brought by a third party that was previously unknown to the 
original applicant. Therefore, these costs, if imposed, would be 
mandatory and out of the applicant’s control, unless the 
application is withdrawn with the commensurate refund, or the 
issue is settled outside of the dispute resolution process.\textsuperscript{62} If the 
applicant decides to apply under a community-based application,

\begin{itemize}
  \item \textsuperscript{54} Guidebook, supra note 7, § 1.2.2, at 27-28.
  \item \textsuperscript{55} Id. § 2.1.1, at 54-55.
  \item \textsuperscript{56} Id. § 1.4.1.2, at 42-43.
  \item \textsuperscript{57} Id. § 1.5.1, at 44.
  \item \textsuperscript{58} See id. at 44-45. Once the applications are published (two weeks after close of 
  application period), applicants can begin withdrawing applications. During this first period, 
an applicant would be refunded 70% of the fee, or $130,000. After initial evaluation results 
are published in November, withdrawing applicants would be refunded 35% of the fee, or 
$65,000. Once applicant goes through dispute resolution or an extended evaluation, if 
applicant withdraws, it is refunded 20%, or $37,000. Id.
  \item \textsuperscript{59} A registry services review determines whether the applicant’s proposed registry 
services will cause a possible adverse impact on security or stability, such as not adequately 
protecting secure information and data, or will affect the throughput of traffic. Id. § 2.2.3.1, 
at 75.
  \item \textsuperscript{60} Id. § 1.5.2, at 46.
  \item \textsuperscript{61} Id.
  \item \textsuperscript{62} The refund at the objection stage is $130,000. Id. § 1.5.1, at 44.
\end{itemize}
the entity will incur an additional fee of approximately $10,000.\textsuperscript{63} Essentially, whenever a new proceeding is required, the applicant will incur additional costs.\textsuperscript{64}

Another possible cost could be incurred in the auction process. Auctions result from a string contention set (e.g., multiple applicants file for .photo and all are equally entitled to it), which is not resolved independently.\textsuperscript{65} While it is described as a “mechanism of last resort,”\textsuperscript{66} an auction could increase costs dramatically depending on how valuable the string is to the applicants, particularly stubborn adversaries, or competitors. Whatever the final auction price is will further increase costs for the gTLD winner. The loser, at that point, will have invested thousands into the application process for nothing.\textsuperscript{67}

Lastly, when an applicant is awarded a gTLD, it also becomes the registry operator.\textsuperscript{68} This responsibility can either be undertaken by the applicant itself at its own cost, or it can be outsourced to a registry service provider, again, at its own cost. Regardless, registry operators are required to pay ICANN at least $25,000 annually, and registry agreements with ICANN require a ten year commitment.\textsuperscript{69} These figures do not include the initial and annual costs of internally supporting or outsourcing the registry function.

For any entity looking to invest in a gTLD, costs are predicted to be between $500,000 and $1 million over the first two years,\textsuperscript{70} and some entities have already stated they have budgeted $1 million toward applying for a gTLD.\textsuperscript{71} The costs of applying for a gTLD will undoubtedly be prohibitive for many potential applicants, forcing a largely passive response to the program, and will accrue potentially substantial benefits to only a few.

\textsuperscript{63} Id. § 1.5.2, at 47 (estimated).

\textsuperscript{64} Mark owners should also keep in mind that any marketing, branding, and changes in business strategy will necessarily cost more, and those costs are not accounted for in this section. Cost of outside counsel for these proceedings, or applications in general, are also not included.

\textsuperscript{65} Guidebook, supra note 7, § 4.3, at 215.

\textsuperscript{66} Id.

\textsuperscript{67} After a string contention resolution, the applicant is entitled to a 20% refund, or $37,000. Thus, applicant has spent $148,000 with no result.

\textsuperscript{68} Remember from above a registry is in charge of running the entire gTLD, maintaining required information and ensuring stability and accuracy of DNS.


\textsuperscript{71} Monitor, supra note 69.
C. Initial Evaluation—Levels of Review

There are two primary levels of review during the initial evaluation stage, which takes place between April and November 2012: review of the applicant and review of the string. Before either level of review occurs, ICANN, in conjunction with INTERPOL,72 reviews the applicant’s background to determine the general business diligence and criminal history of the applicant, as well as whether it has engaged in a “pattern” of cybersquatting behavior, defined as three or more convictions with at least one in the last four years.73 If the applicant does not pass this level of screening, the application will not proceed.74 It is noteworthy that any entity publicly traded on any of the world’s twenty-five largest stock exchanges (and listed in good standing) will pass the diligence and criminal history prong automatically.75 Once the background review is complete, ICANN will continue with the string and applicant review.

The applicant review is less involved than the string review. The applicant is primarily reviewed for its technical and operational capabilities, as well as its financial status.76 The technical and operational review focuses on whether the applicant is technically capable of operating the gTLD and the registry.77 To satisfy this, the applicant must show a clear understanding of the undertaking by completing at least some groundwork toward running the registry.78

72. Guidebook, supra note 7, § 2.1.1, at 54.
73. Id. § 1.2.1(m), at 26 (stating applicant will be automatically disqualified if it “has been involved in a pattern of adverse, final decisions indicating that the applicant or individual named in the application was engaged in cybersquatting as defined in the Uniform Domain Name Dispute Resolution Policy (UDRP), the Anti-Cybersquatting Consumer Protection Act (ACPA), or other equivalent legislation, or was engaged in reverse domain name hijacking under the UDRP or bad faith or reckless disregard under the ACPA or other equivalent legislation. Three or more such decisions with one occurring in the last four years will generally be considered to constitute a pattern”); see also id. § 2.1.2, at 55 (stating that ICANN scans Uniform Domain Name Dispute Resolution Policy cases filed with the World Intellectual Property Organization, and other legal databases.)
74. Id. § 2.1, at 54. ICANN provides a list of disqualifying criminal behavior, including crimes related to financial or corporate governance activities, crimes related to misuse of funds, and convictions of tax fraud. Id. § 1.2.1, at 24-26.
75. Id. § 2.1.1, at 54.
76. The “review” is done completely through the application process, with ICANN reviewing documents provided to it by the applicant to ensure the applicant meets ICANN’s standards. Id. § 2.2.2.1, at 73.
77. Id.
78. Id. If the applicant satisfies this requirement and passes the rest of the application process, it will undergo further technical testing as part of the transition to delegation. See generally id. § 5.2, at 229-35.
The financial documents supplied through the application process provide the basis for the financial review. Essentially, ICANN is looking for consistency across the application—for example, if the applicant has comparatively low revenues, then the entire plan should reflect that level of revenues, rather than reflecting the plan of a large entity that may be able to operate at a higher volume and afford more expensive and higher quality software and equipment. ICANN has not indicated a particular revenue or profit cut-off for applicants.

The string review is significantly more involved. The proposed string is compared with existing TLDs, other proposed TLDs, the reserved names list, and the list of ineligible strings. If the proposed string will create a “probability of user confusion” with, or is an exact match with, a pre-existing TLD or a name on the reserved names or non-delegation list, then the application is rejected. If the proposed string will create a likelihood of confusion with, or is an exact match with, another proposed string, those strings enter a “contention set.” There are four ways out of a contention set: (1) withdrawal of the application; (2) private resolution with the other applicant(s); (3) determination based on community priority; or (4) auction, if no other solutions are available.

79. Id. § 2.2.2.2, at 73-74.
80. Id. at 74.
81. Id. § 2.2.1.1.1, at 56. The applied-for gTLD is also compared to country-code top-level domains, though this article will not go into depth regarding this comparison. The reserved names list includes the following strings: AFRINIC, ALAC, APNIC, ARIN, ASO, CCNSO, EXAMPLE, GAC, GNSO, GTLD-SERVERS, IAB, IANA, IANA-SERVERS, ICANN, IESG, IETF, INTERNIC, INVALID, IRTF, ISTF, LACNIC, LOCAL, LOCALHOST, NIC, NRO, RFC-EDITOR, RIPE, ROOT-SERVERS, RSSAC, SSAC, TEST, TLD, WHOIS, and WWW. Id. § 2.2.1.2.1, at 60.
82. Ineligible strings apply to certain names encompassing OLYMPIC or RED CROSS, including the following: OLYMPIC, OLYMPIAD, and those words in various languages; REDCROSS, REDCRES, REDCRYSTAL, REDLIONANDSUN, REDSTAROFDAVID, and those words in various languages. Id. § 2.2.1.2.3, at 62.
83. Id. § 2.2.1.1.1, at 57. This determination is made by the String Similarity Panel, a panel whose primary purpose is to place strings “that would create a probability of user confusion” into string contention sets. Id. at 56. There is no explanation as to what the threshold is for “probability of user confusion.”
84. Id. at 57.
85. Id. A contention set contains at least two similar or identical strings, and the string contention process is used to decide to whom ICANN will delegate the string, as only one applicant can have it. Id.
86. The refund at this stage is 70%. Therefore, the entity spent $55,000 and received nothing in return, and the entity had no way of knowing about similar or identical strings, given the lack of transparency during the application process mentioned above.
87. A community priority evaluation requires analysis of four specific areas where an applicant can gain points: (1) community establishment; (2) nexus between proposed string and community; (3) registration policies; and (4) community endorsement. Successful priority is based on earning at least fourteen out of a possible sixteen points. An applicant...
successful.88 The string is not reviewed by ICANN for conflicts with existing trademarks.89

Second, the string is reviewed for DNS stability.90 As a result of configuration and programming errors by private networks and software and equipment manufacturers, some popular (though invalid) TLD queries do not resolve to a particular website;91 however, these invalid TLDs get tens of millions of traffic hits per day. If an entity were to register .home, for example, the registry would be unlikely to handle the traffic given the number of invalid queries it receives.92 The delegation of a TLD like .home, or any other popular invalid TLD, could have “operational difficulties that would pose a stability or availability problem for their registrants and users.”93 ICANN anticipates that some registries will receive a non-trivial load of unanticipated queries,94 but it seeks to avoid subjecting registries to a crippling amount of traffic by advising applicants whether a DNS stability issue will likely occur with its proposed string.95 In addition, if a string does not comply with a strict set of technical and stability requirements as set out by ICANN, such as the three to sixty-three character range requirement, the string will not pass initial review.96

The last review for the string is a geographic names review,97 which ensures strings comprising a country or territory name, such as .cuba, are rejected. It also ensures that any string that

who can prove its connection to the proposed mark is strong in the community deserves to own the TLD more than anyone else. Guidebook, supra note 7, § 4.2.3, at 205-15.

88. Id. § 4.3, at 215.
89. There was a proposal during the comment periods for implementation of a Globally Protected Marks List (GPML). The GPML would include globally registered and internationally recognized marks and would be used to block gTLDs for those marks on the list unless the application was filed by the mark owner. ICANN decided not to implement the GPML, arguing that it would be too difficult to develop standards for what marks belong on the list.
90. Id. § 2.2.1.3, at 62-63.
91. The top ten invalid TLDs based on traffic are the following: .invalid, .wpad, .home, .belkin, .corp, .lan, .domain, .localdomain, .localhost, .local. ICANN Security and Stability Advisory Committee, Invalid Top Level Domain Queries at the Root level of the Domain Name System 5 (2010), http://www.icann.org/en/committees/security/sac045.pdf.
92. See id.
93. Id.
94. Guidebook, supra note 7, § 2.2.1.3, at 63.
95. Id.
96. Id. § 2.2.1.3.2, at 64.
97. This article will not go into depth about Government Advisory Committee (GAC) Early Warnings, though be aware that there is a system in place for early detection of gTLDs that could cause concern with governments. See id. § 3.1, at 148-50. If an applicant receives a GAC Early Warning, it can withdraw, within twenty-one days of receiving the warning, for a 70% refund. Id. § 1.1.2.4, at 11.
comprises a geographic name requiring government support\textsuperscript{98} has the requisite documentation as required by the ICANN.\textsuperscript{99} The Geographic Names Panel reviews each application to determine if the string represents a geographic name.\textsuperscript{100} Therefore, this is an issue that must be addressed by all applicants before applying, as applicants may need to seek government approval if the proposed string is the same as or similar to a geographic name, even if the geographic term is also used as a brand name.

\textbf{D. Operating a Registry}

One of the most significant aspects of owning a gTLD is operating the registry. ICANN reviews every candidate for its technical and operational ability to run a registry, and it also reviews every applicant’s registry services proposal for any potential security or stability issues.\textsuperscript{101} Upon delegation, each applicant will enter into a registry agreement\textsuperscript{102} with ICANN and will undergo “pre-delegation testing”\textsuperscript{103} with some very technical requirements.\textsuperscript{104} Upon successful delegation, the applicant will be a registry operator, and will be held responsible for the performance of the obligations under the registry agreement.

Running the registry is a ten-year commitment, renewable for ten-year periods.\textsuperscript{105} As mentioned above, registry upkeep can be expensive, costing at least $25,000 per year in fees to ICANN alone, plus additional costs either to run the registry in-house or to outsource it. In addition, because no TLD created through this system will be removed from the root server, if an entity decides to

\textsuperscript{98} This includes capital cities of countries or territories, city names (if applicant plans to use the TLD for government purposes), exact matches of sub-national place names (province, state), or countries in the UNESCO region (available at http://erc.unesco.org/portal/UNESCOMemberStates.asp?language=en). See also \textit{id.} § 2.2.1.4.2(2)(a)-(b), at 68-70.

\textsuperscript{99} \textit{Id.} § 2.2.1.4.3, at 70-71. If an applicant were to apply for .washingtondc, the applicant would need that government’s approval, with documentation, in order for the gTLD to be delegated to applicant.

\textsuperscript{100} \textit{Id.} § 2.2.1.4.4, at 71.

\textsuperscript{101} \textit{Id.} § 2.2.3, at 74-75. This includes whether the plan might bring about unauthorized disclosure, alteration, insertion or destruction of registry data, or whether the plan might create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. \textit{Id.} § 2.2.3.1, at 75.

\textsuperscript{102} The agreement includes operating the gTLD in a secure and stable manner, implementation of start-up and post-launch rights protection measures, agreement to pay fees ($25,000 or more, depending on number of SLDs registered) to ICANN, and implement measures to protect country and territory names. \textit{Id.} § 5.4.1, at 235-40.

\textsuperscript{103} See generally \textit{id.} § 5.2, at 229-35.

\textsuperscript{104} This includes system performance, WHOIS database support, and support for internationalized domain names. \textit{Id.} §§ 5.2.2.–5.2.3, at 231-35.

\textsuperscript{105} Olive Presentation, \textit{supra} note 53.
discontinue registry services after the initial ten years, that TLD will then be re-delegated to a third party, allowing a potentially unrelated party to take charge of an abandoned .[brand] or industry keyword, such as .toys.

The application cost and process is a significant barrier for applicants, and for good reason: ICANN wants to prevent abuse of the system because this program will likely have a dramatic effect on the functioning of the Internet, and the program should only be available to those who truly want, and have the resources and stability, to own and operate a gTLD. If the system required less onerous application costs and procedures, the possibilities of abuse either by cybersquatting or by delegation of strings that could harm the security and stability of the Internet could cause catastrophic consequences, including creation of numerous registries that do not have enough resources to function and to support the various customers who purchased domain names and built websites around those domains. The barriers seek to avoid these consequences by discouraging bad faith applications and preventing allowance of ill-founded applications.

IV. NEW PROTECTIONS AGAINST TRADEMARK INFRINGEMENT

Existing second-level domains (SLDs) already cause significant enforcement problems for trademark owners. The New gTLD Program will exacerbate infringement problems, not only through the gTLD Program itself, but through SLDs registered under new gTLDs. Brand owners need protection against potentially rampant cybersquatting opportunities the New gTLD Program presents, and ICANN has attempted to provide those protections. There are two ways for trademarks to be infringed as a result of this program: (1) a proposed gTLD string itself may infringe a trademark; or (2) an SLD registered under a new gTLD may infringe a trademark. ICANN has attempted to provide solutions for each, and both will be discussed in turn. The section will then discuss registry liability instituted in the New gTLD Program, and then will discuss possible pitfalls of the “use” requirement.

106. Id.


108. The fees set by ICANN also serve to recoup costs that ICANN incurs through running the process, Guidebook, supra note 7, § 1.5.1, at 44.

109. See generally Lipton, supra note 21, at 448-49.
A. Protections Against Infringing Top-Level Domains

The first step in protecting against infringing gTLDs is to monitor ICANN’s application process. Trademark owners can begin monitoring in late April 2012, two weeks after the application window closes, when first round applications will be published. At this time, the objection and comment period begins, which are projected to last for seven months, ending in November 2012. There are objection protocols for brand owners whether a mark is infringed directly by a gTLD or whether a competitor is applying for an industry keyword (for instance, if a toymaker were to apply for .toys). Each will be covered in this section.

1. Protecting a Brand Against Competitor Appropriation

Prior to the new mechanisms provided by the New gTLD Program, a brand owner whose rights were infringed by a new gTLD would have had to wait until it was delegated, and then bring a court proceeding to enforce its rights. The program, to avoid this result, provides four grounds for objection that can be invoked during the objection period (prior to delegation), which may obviate the need to commence a court action. These include the string confusion, legal rights, limited public interest, and community objections. Of the four, the most relevant objections for brand owners are the string confusion and legal rights objections.

The string confusion objection, to be filed with the International Centre for Dispute Resolution, can be asserted in two situations. The first is when a proposed string is identical or potentially confusingly similar to an existing.

110. Guidebook, supra note 7, § 1.1.2.6, at 13.
111. Id.
112. The limited public interest objection, which can be filed by anyone, can be asserted when the objecting party believes the proposed gTLD is “contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law.” Id. § 3.2.1, at 151. The community objection, which can be filed by an established institution with a close connection to the specifically delineated community as against any application, can be asserted when the objecting party believes the proposed gTLD has “substantial opposition” from a “significant portion of the community to which the gTLD string may be explicitly or implicitly targeted.” Id. Both objections are filed with the International Center of Expertise of the International Chamber of Commerce. Id. § 3.2.3, at 155.
113. Id. § 3.2.3, at 155.
114. The dispute resolution provider is to determine whether “the applied-for gTLD string is likely to result in string confusion.” Id. § 3.5.1, at 165.
TLD. If the existing TLD operator is successful, the remedy is that the application will be rejected. The second is when two proposed strings are identical or potentially confusingly similar to each other. The remedy for a successful complainant in this situation is placement of both strings in a contention set. However, when the initial evaluation procedures undertaken by ICANN have identified the two proposed strings as potentially confusingly similar, and they accordingly were already placed in a contention set, no party has standing to object. Contention sets may be significant in size because strings may be directly contentious, when two strings are confusingly similar to each other, and indirectly contentious, when two strings are in direct contention with a third string, but not with each other.

The legal rights objection, to be filed with the Arbitration and Mediation Center of the World Intellectual Property Organization, may be asserted when one party has legal rights over a string in a proposed gTLD and the applicant intends to use the gTLD inappropriately. This objection can be filed even if the objector is also an applicant; the only standing requirement is that the objector must be a “rightsholder.” A successful objection requires proof of legal rights in the form of either a trademark registration or a court opinion validating an unregistered trademark, a somewhat narrower set of objectors than would normally be qualified to file a traditional lawsuit. Once proven, an expert or panel of experts, appointed by the relevant dispute

---

115. *Id.* § 3.2.2, at 151.
116. *Id.* § 3.2.2.1, at 152.
117. *Id.*
118. *Guidebook,* supra note 7, § 3.2.2.1, at 152. The duplicative nature of the remedies explains why, if ICANN identifies the potential confusion first, no entity has standing to object on this basis.
119. *See id.* § 4.1.2, at 201-02 (describing impact of string confusion dispute resolution proceedings on contentions sets); *see generally id.* § 4.1.1, at 199 (describing direct and indirect contention).
120. *Id.* § 3.2.3, at 155.
121. *Id.* § 3.2.2.2, at 152-53. *See id.* § 3.5.2, at 165-66 (“Whether the potential use of the applied-for gTLD by the applicant takes unfair advantage of [or unjustly impairs] the distinctive character or the reputation of the objector’s registered or unregistered trademark . . . .”).
122. *Id.* § 3.2.2, at 151.
123. In the United States unregistered trademarks in use can acquire rights at common law, and those rights can be vindicated in court through a proceeding under the ACPA, UDRP, or the Lanham Act. Because potential objectors without a federal registration must have a previous court decision validating the mark, only a small number of common-law trademark rightsholders may use the legal rights objection against a gTLD application.
resolution provider,\textsuperscript{124} will conduct a proceeding examining factors\textsuperscript{125} that resemble the \textit{Polaroid} factors under U.S. trademark jurisprudence.\textsuperscript{126}

Both the traditional Lanham Act trademark infringement claim and the similarity determination in the legal rights objection require a determination of whether there is similarity in the sight, sound, and meaning of the two relevant marks or strings.\textsuperscript{127} In addition, both analyses include the intent behind the adoption of the string or mark, which also includes whether the junior user had knowledge of the senior user’s use of the mark.\textsuperscript{128} From here, the analyses diverge, as the legal rights objection panel will look closely at the gTLD applicant and determine whether that entity has any rights to the word or mark such that the entity would be allowed to own it. The \textit{Polaroid} factors focus more specifically on commercial aspects of the marks and realities of competition, including how consumers encounter the marks in the marketplace. These concepts do not as easily apply in the context of the New

\textsuperscript{124} Guidebook, \textit{supra} note 7, § 3.4.4, at 163. One expert presides over string confusion and community objections; three experts preside over limited public interest objections; one or three experts preside over legal rights objections, decided by the parties. \textit{Id.}

\textsuperscript{125} \textit{Id.} § 3.5.2, at 166-67 (listing the factors to be considered when trademark rights are infringed). The factors to be considered are the following: (1) whether the proposed gTLD is identical or similar (sight, sound, meaning) to the objector’s existing mark; (2) whether the objector’s acquisition and use of rights in the mark has been bona fide; (3) whether and to what extent there is recognition in the relevant sector of the public of the sign corresponding to the gTLD, as the mark of the objector, of the applicant or of a third party; (4) applicant’s intent in applying for the gTLD, including whether applicant had knowledge of the mark, or whether applicant has engaged in a pattern of similar infringing conduct; (5) whether and to what extent the applicant has used or has made demonstrable preparations to use the sign corresponding to the gTLD in connection with a bona fide offering of goods or services; (6) whether the applicant has marks or other intellectual property rights in the sign corresponding to the gTLD, and if so, whether any acquisition of such a right in the sign has been bona fide; (7) whether and to what extent the applicant has been commonly known by the sign corresponding to the gTLD; and (8) whether applicant’s use of the gTLD would create a likelihood of confusion with the objector’s mark as to source, sponsorship, affiliation, or endorsement of the gTLD. \textit{Id.}

\textsuperscript{126} Polaroid Corp. v. Polarad Elecs. Corp., 287 F.2d 492 (2d Cir.), \textit{cert. denied}, 368 U.S. 820 (1961). In this case, the Second Circuit Court of Appeals enumerated eight factors for evaluating likelihood of confusion in trademark law, consisting of the following:

(1) strength of plaintiff’s mark; (2) the degree of similarity between plaintiff’s and defendant’s marks; (3) the proximity of the products or services; (4) the likelihood that plaintiff will bridge the gap; (5) evidence of actual confusion; (6) defendant’s good faith in adopting the mark; (7) the quality of defendant’s product or service; (8) the sophistication of the buyers.

\textsuperscript{127} AMF, Inc. v. Sleekcraft Boats, 599 F.2d 341, 351 (9th Cir. 1979) (“Similarity of the marks [in a trademark infringement case] is tested on three levels: sight, sound, and meaning.”); Guidebook, \textit{supra} note 7, § 3.5.2, at 166 (stating the panel of experts may consider “whether the applied-for gTLD is identical or similar, including in appearance, phonetic sound, or meaning, to the objector’s existing mark.”).

\textsuperscript{128} \textit{Polaroid}, 287 F.2d 492 (factor six); Guidebook, \textit{supra} note 7, § 3.5.2, at 166 (factor four).
gTLD Program, since a gTLD applicant will not have made commercial use of its gTLD at the time of the analysis.

If both parties own the same mark for different goods or services, the legal rights objection is unlikely to be successful, given both entities theoretically have equal rights to the string. In such a proceeding, the objecting party must prove that the applicant will use the string to take unfair advantage of the distinctive character of the objector’s mark, and one relevant factor is whether the applicant has used the mark (string) with a bona fide offering of goods or services. A proposed gTLD matching two or more marks, as long as the applicant owns one of them and uses it on products or services, appears to meet the bona fide offering requirement. As a result, if both parties are applicants and both parties own a similar mark, a string confusion objection will likely need to be resolved by either an independent settlement or an auction. If only one party is an applicant, but both parties own the mark for different goods or services, the non-applicant party may be unable to prevent the eventual delegation of the string to the other party.

Even when the mark and the proposed string are not identical, if the marks create an “impermissible likelihood of confusion,” the legal rights objection also applies. The dispute resolution provider will look at the factors provided by ICANN and will make a fact-specific determination of whether an impermissible likelihood of confusion exists between the mark and the string. Since the factors are the same in both instances, the analysis from above still applies; namely, if an applicant owns the mark for which it is applying as a string, and the objecting party owns a similar mark, the applicant likely has a bona fide intent to use the mark in connection with goods or services, which will bolster the applicant’s defense that it should not be prevented from obtaining the gTLD.

As described above, different situations will dictate different strategies. However, if the applicant is applying for a string for

129. Guidebook, supra note 7, § 3.5.2, at 166.
130. If Delta Airlines applies for .delta and Delta Faucets attempts to object, it is unlikely that Delta Faucets could prove Delta Airlines does not offer bona fide goods and services, or that Delta Airlines is trying unfairly to take advantage of Delta Faucet’s recognition. See id.
131. If Delta Airlines and Delta Faucets both apply for .delta, perhaps a settlement would allow one to own the TLD and the other to purchase a generic or otherwise helpful SLD under .delta, such as faucets.delta, or airline.delta.
132. Guidebook, supra note 7, § 3.5.2, at 166. There is no indication of whether an “impermissible” likelihood of confusion is different from or the same as the traditional standard of likelihood of confusion.
133. Id. at 166-67.
which two or more parties own an identical or similar trademark, and the other parties do not also apply for that mark as a gTLD in the first round, the applicant may have a good chance of succeeding in securing the gTLD registration; thereafter, the applicant/owner will be protected by the string confusion objection for that mark in all future gTLD application rounds, which could preclude future applicants, including competitors, from registering that string as a gTLD. If one company owns a registration for a mark that is registered by other entities in different classes, being the first to register the mark as a gTLD may be the best option offering the most protection, so long as the applicant can afford it. Of course, at the time of the first round of applications, the company will not know if any of their competitors or other parties with interests in the same mark have made a filing until it is too late for the company to submit its own application.

2. Protecting an Industry Against Competitor Appropriation of an Industry Keyword

Industry keywords can be classified as a standard or community-based application. However, filing under a community-based application could increase a competitor’s chances of being delegated its industry keyword if it were able to prove the necessary requirements for a community-based application. Alternatively, a .[keyword] applicant may choose to submit its application as a standard application, thereby avoiding the need for community endorsement and various other requirements.

Both standard and community-based applications are subject to the community objection. To object successfully based on community grounds, the objector must prove the following four elements: (1) objector is an established institution associated with the clearly delineated community to which the proposed string refers; (2) objector has an ongoing relationship with the clearly delineated community; (3) the community opposition is

134. Id. § 3.2.1, at 151.
135. See supra note 45 and accompanying text. One competitor may obtain community endorsements from other competitors with which the entity has a close relationship, or to whom it offered incentives for the endorsement. This may risk a community objection from the non-endorsing community, or the possibility that the actions run counter to antitrust law.
136. Guidebook, supra note 7, § 1.2.3.2, at 30. It is important to know that one cannot avoid the community objection simply by applying under a standard application.
137. Potential relevant factors include the following: level of global recognition of the institution, length of time the institution has been in existence, and public historical evidence of its existence. Id. §§ 3.2.2.4, at 154-55, 3.5.4, at 169-72.
138. Potential relevant factors include the following: the presence of mechanisms for participation in activities, membership, and leadership, institutional purpose related to the
substantial;\(^{139}\) and (4) whether there is a likelihood of material
detriment to the rights or interests of a significant portion of the
community to which the string may be targeted.\(^ {140}\) If the objecting
entity can establish these grounds (for instance, if Canon applies
for .photo as a standard application, and a photographer’s trade
organization objects to Canon’s ownership of that string), then it
could successfully preclude applicant from obtaining the TLD.
However, if the applicant, when it applied, categorized the
application as community-based and provided numerous
endorsements in its application, it may bolster the argument that
the applicant could successfully represent the community, and
thus deserves the TLD.

Even if competitors do not object on community grounds,
ICANN has provided an alternative mechanism: the independent
objector.\(^ {141}\) The independent objector will be selected by ICANN
and works “solely in the best interests of the public who use the
global Internet[,]”\(^ {142}\) and as such, can file objections to new gTLD
applications only on public interest or community grounds.\(^ {143}\) The
objector cannot object on the same grounds as another party,\(^ {144}\)
and its standing requirements are excused with the exception that
at least one public comment\(^ {145}\) must be made against the
application before the independent objector may proceed.\(^ {146}\) The
independent objector files its objections with the same dispute

---

139. Potential relevant factors include the following: number of expressions of
opposition, the representative nature of entities expressing opposition, the level of
recognized stature among sources of opposition, distribution or diversity among sources
of opposition, historical defense of the community in other context, and costs incurred by
objector in expressing opposition. Id. § 3.5.4, at 170.

140. This prong looks at how much damage there is to the community. Id. at 171-72.

141. Id. § 3.2.5, at 156-58.

142. Id. § 3.2.5, at 156. ICANN cannot force or coerce the independent objector to object;
it is his or her decision. ICANN just posted a notice seeking expressions of interest for
persons seeking to serve as independent objectors. See New gTLD Program: ICANN Seeks
Independent Objector, ICANN (Nov. 21, 2011), http://www.icann.org/
en/announcements/announcement-3-21nov11-en.htm.

143. Guidebook, supra note 7, § 3.2.5, at 156.

144. Id. at 156 (“The [Independent Objector] may file objections against ‘highly
objectionable’ gTLD applications to which no objection has been filed.”).

145. During the initial evaluation period (April 2012–November 2012 for the first
round), ICANN allows for public comments, which can be posted by anyone with potentially
relevant information regarding particular applications or applicants, and those comments
are viewed by ICANN staff when making initial evaluation determinations. Id. § 1.1.2.3, at
8-9. However, comments are not to be mistaken for objections, as comments have a very
limited role in the process. Id. at 9-10.

146. Id. § 3.2.5, at 157.
resolution providers as other objecting parties, the International Center of Expertise of the International Chamber of Commerce. 147

The barriers to entry for the program will likely deter cybersquatters and those with bad faith intent to profit from using another’s mark from applying for gTLDs. Fights over industry keywords have the potential to be more prevalent, as entities may seek to gain the increased Internet traffic and potential profit from laying claim to a descriptive or generic industry keyword such as .photo or .toys. Entities should consider filing a community objection if a competitor attempts such a strategy.

**B. Protections Against Infringing Second-Level Domains**

Many brand owners are familiar with cybersquatting behavior, as it has been an increasing problem since the 1990s. 148 There are already numerous cybersquatting opportunities for .com, .net, and .org. Now, as TLDs expand, each new TLD represents a potential new landscape for bad faith behavior. SLD infringement is much more likely than TLD infringement because registration of an SLD is much cheaper and the barriers to entry will likely be as low as current SLDs in most cases. 149 However, the program provides additional “rights protection mechanisms” that brand owners may use against cybersquatting.

Registry operators are required, in the registry agreement they sign with ICANN when they obtain the right to run the new gTLD, to implement rights protection mechanisms (RPMs). 150 These measures are designed to give trademark owners additional protection against cybersquatting, and to mitigate some of the challenges affiliated with monitoring and enforcing trademark rights on the Internet. ICANN created two types of rights protection mechanisms named for the stage during the process during which they can be used: start-up mechanisms, and post-launch mechanisms.

---

147. See id. (“As an objector in dispute resolution proceedings, the [Independent Objector] is required to pay filing and administrative fees, as well as advance payment of costs, just as all other objectors are required to do.”).

148. See generally Lipton, supra note 21, at 448-49.

149. In the existing gTLD landscape, some SLDs can be purchased for less than $10 with no requirements; others, such as .xxx SLDs cost more like $100 with attendant requirements regarding the applicant’s business interests.

150. Guidebook, supra note 7, § 5.4.1, at 237-38.
1. Start-up Rights Protection Measures

Start-up RPMs must be implemented at the commencement of the TLD. They are largely preventive measures designed to allow mark owners to curb some infringing behavior pre-emptively. Because of the substantial expansion of the domain space, it is more efficient for mark owners to invoke prophylactic measures to prevent infringement rather than to commence proceedings after cybersquatting has occurred. The first start-up RPM measure is the Trademark Clearinghouse and Claims Service, and the second is the Sunrise period.

The Trademark Clearinghouse provides a central repository and database that will contain a list of marks deposited by trademark owners. The Clearinghouse has two functions: (i) to validate and authenticate the rights submitted to the Clearinghouse, and (ii) to serve as the underlying database for the Sunrise and Trademark Claims services.

Inclusion in the Clearinghouse requires that the marks be either registered (regionally or nationally), validated through the court system, protected by statute or treaty, or constitute other intellectual property, such as copyright or even titles. Trademarks that are merely the subject of pending applications or are within any opposition period are not eligible. All mark holders must also submit a sworn statement that the information is true and correct and not supplied for an improper purpose, in order to provide those who may be wronged by improper submissions with additional causes of action for fraud. Mark holders must also commit to keep the information current and may be required to renew the entry.

Each new registry must provide for use of the Claims service for at least the first sixty days that registration is open for general registration. The Claims service requires registries to use the information in the Clearinghouse to notify applicants for identical strings regarding the existence of the mark owner’s rights in that

152. TMC Agreement, § 4.1, at 308. The Clearinghouse is opt-in only.
153. TMC Agreement, § 1.2, at 304.
154. TMC Agreement, §§ 3.2.1–3.2.4, at 306-07.
155. TMC Agreement, § 3.2.5, at 307.
156. TMC Agreement, § 3.8, at 307-08.
157. Id.
158. TMC Agreement, § 3.9, at 308.
159. TMC Agreement, § 6.1.1, at 309.
In response, the applicant may either maintain the application or withdraw the application. The registry must also notify the mark holder of the corresponding domain registration once effectuated. There are limits to the effectiveness of this notification. Notification alone is not likely to deter a cybersquatter from proceeding to obtain the domain name registration. Notification to the brand owner may eliminate only some of the need for a watch service because it only covers exact matches.

Each new registry must also provide for a Sunrise registration process for a minimum of 30 days during the pre-launch phase of the registry. The Sunrise period provides a mark owner a set amount of time during which to register its trademark(s) as an SLD under a newly delegated gTLD, thereby precluding third-parties from registering the identical domain under that gTLD; this is often called defensive registration. Many brand owners elect to file defensive registrations during these Sunrise periods but often have little or no use for the domain name that they obtain through these procedures.

Each registry must notify owners of marks in the Clearinghouse, in accordance with the registry’s Sunrise eligibility requirements, of Sunrise applications containing an identical match to a Clearinghouse mark. In order for marks in the Clearinghouse to qualify for this protection, however, the mark holder must have provided proof of use of the mark to the Clearinghouse, although proof of use is not required for the Claims service discussed previously. For marks not protected by a court decision or by statute, the mark holder may provide “evidence of use of the mark in connection with the bona fide offering for sale of goods or services prior to application for inclusion in the Clearinghouse, and thus gain the benefits of the Claims and Sunrise services, the Clearinghouse must validate and authenticate the information provided by the Clearinghouse applicants, which requires proof of use. TMC Agreement, § 5.2, at 309.

---

160. TMC Agreement, § 6.1.2, at 309. A sample trademark notice is provided on page 313 of the applicant guidebook.
161. Id.
162. TMC Agreement, § 6.1.4, at 310.
163. TMC Agreement, § 6.2.1, at 311. The amount of time must be thirty days or longer. Id.
165. Mikael Ricknäs, Dot-XXX STLD Registrations Begin Wednesday, PCWorld (Sept. 7, 2011, 8:10 AM), http://www.pcworld.com/businesscenter/article/239610/dotxxx_stld_registrations_begin_wednesday.html (most of the companies pre-registering dot-XXX domains are not in the adult industry, but are registering and paying to protect their trademarks).
166. TMC Agreement, §§ 7.1, 7.2, at 312-13. However, this is somewhat misleading, as to be included in the Clearinghouse, and thus gain the benefits of the Claims and Sunrise services, the Clearinghouse must validate and authenticate the information provided by the Clearinghouse applicants, which requires proof of use. TMC Agreement, § 5.2, at 309.
Clearinghouse”167 if such marks are to be used in the Sunrise process.

The Trademark Claims service will notify a trademark owner only when an applicant attempts to apply for an SLD that is an identical match with the relevant mark.168 Therefore, if an entity owns the mark BARBIE (a registered mark used in commerce),169 and an applicant attempts to register www.barbie.toy, a mark owner who has opted in to the Clearinghouse and the Claims service will be notified of the proposed application. If the same applicant attempts to register www.barbe.toy, in order to capitalize on possible typographical errors (also known as typosquatting), the BARBIE trademark owner will not be notified since “barbe” and “Barbie” would not be considered an identical match. Likewise, “ilovebarbie.toy” or even “barbiedoll.toy” would not trigger a notice since these strings are not an identical match with “Barbie.” This is a significant disadvantage of the program, given the frequent problem with typosquatting and with domain name registrations that include the mark with other terms.170 The Claims service is not intended to preclude infringement; it simply alerts parties to potentially obvious cases of infringement.

Similarly, the Sunrise service need only be made available for exact hits of marks registered with the Clearinghouse. Each Sunrise registration process is also subject to objection based on a registry’s Sunrise Registration Dispute Policy (SDRP).171 Each SDRP must allow for at least the following four grounds to challenge the Sunrise SLD registration: (i) at the time of registration of the challenged domain name, registrant’s trademark rights were not of national effect (or regional effect), were not court-validated, or were not protected by statute or treaty; (ii) the domain name is not identical to the Sunrise registration; (iii) the trademark registration providing the basis for the Sunrise registration is not of national effect (or regional effect), is not court-validated or protected by statute or treaty; or (iv) the

167. TMC Agreement, § 5.2, at 309.
168. TMC Agreement, § 6.1.5, at 310 (“‘Identical Match’ means that the domain name consists of the complete and identical textual elements of the mark. In this regard: (a) spaces contained within a mark that are either replaced by hyphens (and vice versa) or omitted; (b) only certain special characters contained within a trademark are spelled out with appropriate words describing it (@ and &); (c) punctuation or special characters contained within a mark that are unable to be used in a second-level domain may either be (i) omitted or (ii) replaced by spaces, hyphens or underscores and still be considered identical matches; and (d) no plural and no ‘marks contained’ would qualify for inclusion.”).
169. BARBIE, Registration No. 689,055.
171. TMC Agreement, §§ 6.2.2–6.2.4, at 309.
trademark registration providing the basis for the Sunrise registration did not issue on or before the effective date of the Registry Agreement and was not applied for on or before ICANN announced the applications received.\textsuperscript{172} The Clearinghouse will hear challenges regarding marks involved in an SDRP.\textsuperscript{173}

2. Post-Launch Rights Protection Measures

While it is recommended that most trademark owners (whose marks are susceptible to cybersquatting) participate in the start-up rights protection mechanism described above, this may not always be possible as in the case, for example, when the mark does not qualify for deposit in the Clearinghouse. Also, it may not be immediately obvious from a new gTLD application that the gTLD in actual operation infringes a mark holder’s rights. Therefore, in addition to the Uniform Dispute Resolution Policy already available to victims of cybersquatting,\textsuperscript{174} ICANN imposed a post-launch measure to protect trademark owners from infringement—the Uniform Rapid Suspension System.\textsuperscript{175}

The Uniform Rapid Suspension System (URS)\textsuperscript{175} is designed to suspend domains representing “clear cases of trademark abuse,”\textsuperscript{176} which must be proven by clear and convincing evidence.\textsuperscript{177} Because the URS provides an expedited resolution to infringement at a relatively low price,\textsuperscript{178} the infringement must be unequivocal, and the complainant must prove the domain registrant had no rights to the name, and it registered the domain name in bad faith.\textsuperscript{179} A finding a bad faith requires behavior consisting of or similar to the following situations: (1) where the allegedly infringing registrant’s primary purpose of registering the domain name was to sell, rent, or otherwise transfer it to the real trademark owner, or its competitor; (2) where the allegedly infringing registrant registered the name to prevent the owner of the trademark from owning the

\textsuperscript{172} TMC Agreement, § 6.2.4, at 311.
\textsuperscript{173} TMC Agreement, § 6.2.5, at 311.
\textsuperscript{175} Credit must be given to the Implementation Recommendation Team for this suggestion as well as a number of others. IRT Recommendations, ICANN, 11-69 (May 29, 2009), http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf.
\textsuperscript{176} Guidebook, supra note 7, Module 5, app. “Uniform Rapid Suspension System (URS),” § 8.5, at 321 [hereinafter URS Agreement].
\textsuperscript{177} URS Agreement, § 8.2, at 320.
\textsuperscript{178} The fee for a URS proceeding will likely be in the range of $300, and the loser pays. URS Agreement, §§ 2.1, 2.2, at 316.
\textsuperscript{179} URS Agreement, §§ 1.2.6.2–1.2.6.3, at 315.
corresponding domain; (3) where the allegedly infringing registrant’s primary purpose was to disrupt the business of a competitor; or (4) where the allegedly infringing registrant was attempting to attract, for commercial gain, Internet users to its website by creating a likelihood of confusion with another’s mark. Proving bad faith by clear and convincing evidence could be difficult.

The final resolution of a URS proceeding takes a mere twenty days, unless the registrant requests an extension or defaults. During the pendency of the proceeding, the domain is “locked” so that no registry information can change and the domain name cannot be assigned, although the domain still resolves to the registrant’s website. If the complainant is ultimately successful, the remedies are limited to suspension of the domain name. Upon suspension, the website reverts to a URS information page, and the complainant is given the opportunity to extend the registration period for up to a year. The URS does not provide for transfer of the domain to a successful complainant.

The URS allows a complainant to challenge domain name strings that are similar to its trademark, just as the UDRP does. However, the URS requires that there be no genuine issue of fact in order for the complainant to prevail; therefore, a URS complainant should exercise some caution in challenging similar domains to ensure that the panelist will not hold that there is a genuine issue of fact as to infringement. Further, URS complainants who rely on registered trademark rights must have used the trademark in question, and must submit proof of use with the URS complaint. To borrow an earlier example, if a third-party were to register barbie.toy, the owner of BARBIE could bring a URS proceeding to suspend the domain. Additionally, if a third-

---

180. URS Agreement, § 1.2.6.3(a)-(d), at 315.
181. One extension may be granted at the request of the registrant for a maximum of seven days, URS Agreement, § 5.3, at 317. A registrant may default by not responding within the fourteen-day time period allotted for responses. If it does so, it has six months to file a response in order to exercise its right to seek relief from default via de novo review. URS Agreement, § 6.4, at 319.
182. URS Agreement, § 10.2a [sic], at 322.
183. URS Agreement, §§ 10.2a, 10.2b [sic], 10.3, at 322.
184. URS Agreement, supra note 174, § 4(a).
185. UDRP, supra note 174, § 4(a).
186. URS Agreement, § 8.5, at 320. This is borrowed from the summary judgment standard in civil procedure. Ashcroft v. Iqbal, 129 S.Ct. 1937, 1947 (2009) (stating “determining whether there is a genuine issue of material fact at summary judgment is a question of law . . . [that] is a ‘fact-related’ inquiry.”).
187. URS Agreement, § 1.2.6.1, at 315.
188. Id.
party were to register www.barbe.toy (an example of typosquatting), the entity could also challenge this registration, and have that domain suspended as well, so long as the panelist agreed that there is no genuine issue of fact regarding infringement. A URS decision can be appealed, with the costs being borne by appellant.\textsuperscript{189} The venue for the URS and any appeal will be up to the rules of the provider(s) chosen to provide the URS service.

As mentioned above, the URS is designed to be used for obvious cases of infringement and requires the complainant to prove bad faith and meet the clear and convincing evidentiary standard.\textsuperscript{190} In United States jurisprudence, there are generally three standards of proof from least to most onerous, (1) “preponderance of the evidence,” (2) “clear and convincing,” and (3) “beyond a reasonable doubt.”\textsuperscript{191} Because ICANN requires the clear and convincing standard for a URS, the URS panelist will take a more exacting look at the facts and evidence than is required in a UDRP proceeding, where the preponderance of the evidence standard applies.\textsuperscript{192} Perhaps the obvious nature of the infringement will aid the complainant in meeting this higher burden—for example, it seems that the complainant could likely meet its burden if the complainant can show that the domain name is being used for a site selling counterfeits.

In the United States, the clear and convincing evidence standard is “appropriate for cases where the interests are greater than the mere loss of money, but where it is nevertheless appropriate to reduce the risk to the defendant of having his reputation tarnished.”\textsuperscript{193} Such cases include the following: overcoming the presumption of patent registration validity,\textsuperscript{194} proving the criminal defense of insanity,\textsuperscript{195} and proving insanity for civil commitment.\textsuperscript{196} The use of the clear and convincing evidence standard in the domain name cybersquatting context does not comport with the rationale for the higher burden, nor is

\textsuperscript{189} URS Agreement, §§ 12.1–12.2, at 323.
\textsuperscript{190} URS Agreement, § 8.2, at 320.
\textsuperscript{192} Clear and convincing evidence is “[e]vidence indicating the thing to be proved is highly probable or reasonably certain.” Black’s Law Dictionary (9th ed. 2009). The UDRP’s burden is “on balance” or “preponderance of the evidence.” The Uniform Domain Name Dispute Resolution Policy and WIPO, World Intell. Prop. Org. 11 (Aug. 2011).
\textsuperscript{193} W. David Ball, The Civil Case at the Heart of Criminal Procedure: In Re Winship, Stigma, and the Civil-Criminal Distinction, 38 Am J. Crim L. 117, 154 (2011) (internal quotation marks omitted).
\textsuperscript{194} Microsoft Corp. v. i4i Ltd. P’ship, 131 S. Ct. 2238 (2011).
cybersquatting comparable to other causes of action that require heightened burdens of proof. This heightened standard of proof is designed to protect defendants in cases where reputation is at risk. In a case brought by a legitimate trademark holder against a cybersquatter (and especially when cybersquatting is obvious) there is no need to protect the reputation of the defendant or respondent; it is the plaintiff or petitioner’s reputation, or the reputation and goodwill in their trademark, that the tribunal is seeking to protect in URS proceedings. The URS’s heightened burden of proof arguably overcompensates and protects the respondent too much, as ACPA proceedings have invoked a lower burden of proof with success.\textsuperscript{197} Thus, the price for quick summary proceedings against domain names via the URS is a heightened burden of proof that may be considered otherwise inappropriate. The result is also underwhelming—the ultimate remedy does not include transfer of the problematic domain name.

Besides the additional burden of a higher standard of proof, the benefits of the URS are somewhat illusory when compared with outside remedies. It may be more fruitful for a trademark owner, confronted with a cybersquatter, to send a notice-and-takedown request to the ISP hosting the offending website (resulting in a speedy removal of the website contents), and to simultaneously file a UDRP claim against the website’s owner. Because the UDRP allows for the transfer of ownership,\textsuperscript{198} the trademark holder has a better remedy, arguably, through use of the takedown and UDRP rather than the URS on its own. Alternatively, the trademark holder could institute a URS proceeding to quickly remove the offending content and then file a UDRP claim to have the domain name transferred to it.\textsuperscript{199} Either way, the benefits of having a URS proceeding seem to be a negligible improvement over existing alternative remedies that could potentially be more effective.

\textbf{C. Action Against Registries for Infringing TLDs and SLDs Under Their Control}

The Post Delegation Dispute Resolution Procedure (PDDRP) is designed to hold registry operators liable for their conduct, whether it is unfair use of a TLD that is similar to a registered trademark, or whether it is a pattern of infringing behavior by the

\textsuperscript{197} Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214 (4th Cir. 2002).
\textsuperscript{198} UDRP, \textit{supra} note 174, § 4(i).
\textsuperscript{199} However, the URS determination “shall not prejudice the party in UDRP or any other proceedings[,]” so a successful complainant in a URS proceeding should not expect that determination to be dispositive in the UDRP proceeding. URS Agreement, § 13, at 323.
operator. The evidentiary standard for imposing liability in this proceeding is, again, clear and convincing evidence. Where a complaint concerns an infringing TLD string, the registry operator will be held liable for infringement only if a trademark owner (whose mark is identical or confusingly similar to the delegated TLD) successfully asserts that the registry operator’s affirmative actions have contributed to (1) taking unfair advantage of the distinctive character of the mark owner’s rights, (2) impairing the mark’s distinctive character, or (3) creating a likelihood of confusion with the mark owner’s mark. For infringing SLDs, the complainant must prove the registry operator’s conduct represents a substantial pattern of bad faith intent to profit from registering infringing domain names, or bad faith intent to profit from registration of domains that (1) take unfair advantage of the mark, (2) impair its distinctive character, or (3) create a likelihood of confusion. The remedies in a PDDRP are limited. While the PDDRP does provide fee reimbursement for a prevailing complainant at the expense of the registry operator, there is no provision for recovery of monetary damages, nor will a successful complaint result in the deletion of offending SLD registrations. The sole remedy of the PDDRP is the imposition of enforcement tools. These may include remedial measures to ensure future registrations do not infringe the legal rights of others, a suspension of the registry’s ability to accept new domain name registrations until the violations are cured, or a termination of the registry agreement if the registry’s behavior has been particularly malicious. Complainants may take limited solace in the fact that, upon success, they are reimbursed for all panel and provider fees by the registry operator.


201. PDDRP Agreement, supra note 200, § 6.1, at 326. An example is the registry operator holding itself out to be a beneficiary of the mark. Id.


203. PDDRP Agreement, supra note 200, § 14.3, at 332.

204. PDDRP Agreement, supra note 200, §§ 18.1-18.2, at 333. In order to delete the registrations, an entity would have to bring a URS proceeding, if possible, or a court proceeding under the Anti-cybersquatting Consumer Protection Act, or a Uniform Domain Name Dispute Resolution Policy proceeding with the World Intellectual Property Organization.

205. PDDRP Agreement, supra note 200, § 18.3, at 333.

206. PDDRP Agreement, supra note 200, §§ 18.3.1-18.3.3, at 333.

207. PDDRP Agreement, supra note 200, § 14.3, at 332.
Again, any asserted rights in a mark must be accompanied by proof of use of the mark, and in addition, the complainant must assert that it has been materially harmed as a result of the trademark infringement. The dispute will be decided by one panelist, whose determination can be appealed within twenty days. The appeal board will consist of three experts. The venue for the PDDRP and subsequent appeals will be determined by the provider that is selected to offer the PDDRP service.

Before the implementation of the PDDRP, there was essentially no cause of action against a domain name registrar or registry for secondary liability for trademark infringement (under the Lanham Act and the ACPA) because they neither have the requisite control over the activities of third-party infringers, nor do they provide a “product” in order to be held secondarily liable under the Inwood Labs test. In most cases, the registrar must have “unequivocal knowledge” of the third-party infringement, obviously a very high burden. When no “product” is provided such as with a domain name registrar, a court must look to the amount of control the defendant (registrar) exercised over the third party’s means of infringement. As stated above, most registrars will argue, and courts tend to agree, that registrars do not have sufficient control over registrants to merit imputation of secondary liability. TLD registries could make the same argument if sued for secondary trademark liability, as they are even more attenuated from the sale process or ability to control registrants than in the case of registrars. A court would likely side with the registry as a result of the very narrowly interpreted “product.”

208. PDDRP Agreement, supra note 200, § 9.2.1.1, at 329.
209. PDDRP Agreement, supra note 200, § 9.2.2, at 329.
210. A three-person panel may be requested by both parties. PDDRP Agreement, supra note 200, § 13.2, at 331.
211. PDDRP Agreement, supra note 200, §§ 20.2–20.3, at 334-35.
212. Size, Inc. v. Network Solutions, Inc., 255 F. Supp. 2d 568, 572 (E.D. Va. 2003). The Inwood Labs test requires, for a defendant to be liable under a contributory trademark infringement theory, to have (1) intentionally induced another to infringe a trademark, or (2) to continue to supply a product to a third party with actual or constructive knowledge of the infringement. Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 854 (1982).
213. Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949 (C.D. Cal 1997) (“[I]t is inappropriate to extend contributory liability to [a registrar] absent a showing that [the registrar] had unequivocal knowledge that a domain name was being used to infringe a trademark.”), aff’d, 194 F.3d 980 (9th Cir. 1999).
215. Id. at 984-95 (“Although [Network Solutions’s] routing service is only available to a registrant who has paid [Network Solutions’s] fee, [Network Solutions] does not supply the domain-name combination any more than the [United States] Postal Service supplies a street address by performing the routine service of routing mail.”).
“knowledge,” and “control” terminology from the Inwood Labs test and its progeny. When domain names infringe registered marks, registrars and registries are not to be held liable except for “a showing of bad faith intent to profit from [infringing] registrations.”

There appears to be some room for argument, however, regarding registrar liability, because some plaintiffs have been successful against registrars. Verizon sued a few domain name registrars for secondary trademark liability, at least one of which resulted in a decision, although in the context of a default judgment. Transamerica Corporation was able to survive a motion to dismiss on a claim of secondary liability (arguing inducement, knowledge, and control) by arguing that defendant, Moniker Online Services, acted in concert with its registrants to profit from cybersquatting. A registrar may also be held liable when it is acting as a registrant. While these cases represent the exception to the general rule that registrars are not secondarily liable, it does signal that some courts are willing to accept that in limited circumstances, registrars can act with such bad faith that secondary liability is appropriate. To extend this reasoning to registries would be unlikely with only the Lanham Act and the ACPA available to plaintiffs.

At this point, the PDDRP provides the only realistic chance for secondary liability to be imputed to a registry. Now that registry ownership will be widespread, ICANN appears to be increasingly worried about lax SLD registration procedures that will lead to mass trademark infringement. The solution, for now, is a PDDRP proceeding.

As seen above, ICANN has provided a variety of ways a mark owner can protect itself from infringing behavior in the New gTLD Program. If a proposed TLD string is the source of the infringement, a party with standing can object based on legal rights or string confusion. If the TLD has already been delegated and the issue is with domain names issued under the new TLD,
there are post-delegation protective measures that provide trademark owners a faster way to shut the domain down or impute liability to a registry rather than undertaking a federal court proceeding such as under the Anti-Cybersquatting Consumer Protection Act, or a proceeding under the Uniform Domain Name Resolution Policy. If SLD infringement is a problem, an entity can participate in preventive measures such as the Clearinghouse and Claims service or the Sunrise period. If the SLD has already been registered, and the infringement is obvious, the URS proceeding is the cheapest and fastest way to shut down the domain. If the source of the problem is the registry operator itself, the PDDRP provides a mechanism to hold the registry operator liable, and potentially shut it down.

D. Use Requirement to Claim Rights

Unlike the existing UDRP, the Clearinghouse (for Sunrise services), the URS proceeding, and the PDDRP require the complainant to have “use[d]” the trademark for which it is asserting rights. However, whether a trademark has been “used” is not always clear. In the United States, a U.S.-based trademark applicant cannot acquire federal protection unless the mark has been “used” in interstate commerce in the ordinary course of trade, such as sales across state lines, store locations in multiple states, or the provision of services from one location to patrons from multiple states. “Use” in commerce in the United States is also established if goods are made in the United States and shipped abroad, or made abroad and shipped to the United States or if patrons from the United States purchase the services or goods from a mark owner located in a foreign country.

220. TMC Agreement, supra note 151, § 5.2, at 309, § 7.2 at 312 (requiring national or regional registration and current use of trademark in order to validate the trademark); URS Agreement, supra note 176, § 1.2.6.1, at 315 (requiring national or regional registration and current use of trademark to bring a claim).


222. Lanham Act § 45, 15 U.S.C. § 1127 (stating that “commerce” means “all commerce which may lawfully be regulated by Congress”); Larry Harmon Pictures Corp. v. Williams Restaurant Corp., 929 F.2d 662 (Fed. Cir. 1991) (decided that BOZO’s pit barbeque restaurant, which did not provide services in multiple states but provided service to interstate customers at one location constitutes use in commerce sufficient to satisfy the Lanham Act).

223. This constitutes trade with a foreign nation that can be regulated by Congress. For an example, see International Bancorp, LLC v. Société des Bains de Mer et du Cercle des Étrangers à Monaco, 329 F.3d 359 (4th Cir. 2003).
However, the Clearinghouse and the URS panel are unlikely to know if the specimen provided to it meets those burdens, or if the marks were used “merely to reserve a right in the mark[,]” such that the use would not actually count as bona fide use in commerce under the Lanham Act.\(^\text{224}\)

The situation is further complicated because the registered trademark rights that can form the basis for a complaint can be located in any jurisdiction which presumably means that the use requirements from that jurisdiction should apply to the registered rights which are being enforced. There is no universal concept of trademark use applicable to all countries. The United States has a significant body of case law, both judicial and administrative, that has addressed what type of activity constitutes trademark use and what type of evidence is necessary to support a claim of trademark use, largely because trademark rights in the United States are based on and derived from use under a common law system that is not similar to the civil law systems of many other countries.\(^\text{225}\)

Relatively few countries have significant jurisprudence on the issue of what constitutes use. Some, such as Canada,\(^\text{226}\) are like the United States in requiring use information during the registration process. Most countries require no use to register a trademark, although they may require that a mark be used within a certain period of time, usually three to five years from registration, in order for the mark not to be vulnerable to a third-party action for cancellation on the ground of non-use. Some countries, such as Chile, do not even have a use requirement. South Africa even has a provision that allows use on goods for an associated mark to count as valid use for another associated mark.\(^\text{227}\)

While it may be possible to establish “current use” in the Clearinghouse by submitting “a declaration and a single specimen of current use,”\(^\text{228}\) it may be challenging for a panelist in an SDRP, URS or PDDRP proceeding to be persuaded that a trademark is actually in use by such meager evidence. Having no single, consistent definition of “use” made applicable in ICANN

\(^{224}\) Lanham Act § 45 (definition of “use in commerce”).

\(^{225}\) 2 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition, § 16:6 (4th ed.).


\(^{228}\) PDDRP Agreement, supra note 200, § 5.2, at 309.
proceedings may well be the greatest weakness in any attempt by ICANN to put into place effective enforcement mechanisms. ICANN’s use requirement leaves many questions unanswered, and they will likely continue to be left unanswered until litigation and proceedings begin to amass.

V. REMEDIES OUTSIDE THE ICANN SYSTEM

Despite the procedures ICANN put in place, disputes will inevitably arise after TLDs and SLDs are delegated. Not all trademark owners will closely monitor the application process or take advantage of the procedures the program provides. Even an entity that fully participates in the ICANN Program, by filing an application for a new gTLD for its brand, by monitoring other gTLD applications for potential infringements, by enrolling its brand in the Clearinghouse, by receiving Claims Notices for its brand and by registering its brand in available Sunrise Periods, will undoubtedly face increased Internet infringement issues.

Entities seeking redress will encounter difficulties once allegedly infringing TLDs are delegated. The three primary vehicles for post-delegation redress, not including the ICANN mechanisms discussed previously, are the Anticybersquatting Consumer Protection Act (ACPA),229 the Uniform Dispute Resolution Policy (UDRP),230 and the Lanham Act.231 Both have been used to redress cybersquatting second-level domains,232 and will likely continue to be used similarly against SLDs in the new gTLDs; redress against TLDs themselves, however, presents a different challenge.

A. Anti-Cybersquatting Protection Act

The ACPA provides a remedy where a cybersquatter “registers, traffics in, or uses a domain name” that comprises a trademark.233 The ACPA will continue to be a successful enforcement mechanism against cybersquatting in the SLD space.

When the ACPA was passed in 1999, expansive registration and ownership of TLDs, in the same sense as SLD ownership and

---

registration, was not contemplated. The idea that an owner of a gTLD would infringe upon another’s trademark rights was simply unfathomable because gTLDs were tightly controlled by ICANN by that point.\textsuperscript{234} Also, in 1999, there were only seven gTLDs (.com, .edu, .gov, .int, .mil, .net, and .org).\textsuperscript{235} Now that trademark infringement in the gTLD space itself is a greater threat, the question is whether the ACPA would apply to such gTLD infringement. The answer appears to be no.

The ACPA’s definition of “domain name” is narrow in order to address the problem sought to be remedied by the act, namely, cybersquatting.\textsuperscript{236} In fact, the legislative history specifically mentions that the act is “technology neutral enough to accommodate names other than second-level domains . . . as may be the case should Internet domain name registrars begin to issue third and fourth level domains.”\textsuperscript{237} Congress planned for the act to apply to domains further to the left of the TLD, as those had the potential to be delegated in 1999. However, though the legislative history mentions TLDs twice, neither time is it to extend the reasoning or the language of the act to apply to TLDs alone.\textsuperscript{238} Case law has followed this reasoning, extending the ACPA protections to second-level domains at most,\textsuperscript{239} although the protection should also extend to third-level domains where the second-level domains are controlled by the registry (e.g., firm.law.pro). Unless Congress revisits the ACPA, it will not provide useful protection for trademark owners against infringement at the TLD level.

Furthermore, the ACPA may not be useful against TLDs for the simple reason that a registrant of a TLD is unlikely to meet the definition of cybersquatting. To be successful under the ACPA, the complainant must prove the respondent registered the name in bad faith, and factors include respondent’s prior use of the mark with a bona fide offering of any goods or services.\textsuperscript{240} Given the significant barriers to entry to owning a TLD mentioned above, and the fact that ICANN reviews each entity for a history of

\textsuperscript{234} About, ICANN, http://www.icann.org/en/about (last modified Aug. 12, 2011) (stating ICANN was founded in 1998, the year before ACPA was passed).

\textsuperscript{235} Top-Level Domains (gTLDs), ICANN, http://www.icann.org/en/tlds/ (last modified Aug. 13, 2010).


\textsuperscript{237} Id. (emphasis added). Note that this has not happened, the owner of SLDs generally control third- and fourth-level domains.

\textsuperscript{238} Id. at 5, 10.

\textsuperscript{239} See, e.g., Coca-Cola Co. v. Purdy, 382 F.3d 774, 783-84 (8th Cir. 2004) (“[When applying ACPA,] courts generally look to the second level domain name to determine whether it is identical or confusingly similar to a given mark.”).

cybersquatting behavior, it is unlikely a cybersquatter would either decide to spend so much time and money, and, if he or she did so, the application would not be likely to pass ICANN’s strenuous evaluations.

**B. Uniform Domain Name Dispute Resolution Policy**

The UDRP is a proceeding created by ICANN and is available through one of four dispute resolution providers,241 the most used of which is the WIPO Arbitration and Mediation Center.242 The UDRP will probably continue to be one of the most effective tools against cybersquatting in the SLD space. However, similar to the ACPA, the UDRP’s scope encompasses only cybersquatting behavior, and does not apply to gTLDs per se. Therefore, the UDRP would not provide the victim of TLD infringement any redress.243

**C. The Lanham Act**

Where SLD infringement is present, and the factors for liability under the ACPA or UDRP cannot be met, the Lanham Act provides relief for the infringement of federally registered,244 unregistered,245 and “famous” marks246 that comprise an SLD. The trademark infringement provisions of laws in other countries may also provide relief where jurisdiction and nexus requirements are satisfied.247 Because the Lanham Act has a provision for damages resulting from infringement,248 as well as preliminary injunctive


242. For information regarding WIPO’s role, see Domain Name Dispute Resolution, World Intell. Prop. Org., http://www.wipo.int/amc/en/domains (last visited Sept. 30, 2011). Note this is the same service provider as will be used for Legal Rights Objections under the New gTLD Program.


246. Lanham Act § 43(c), 15 U.S.C. § 1125(c) (providing remedies for dilution of a “famous” mark by blurring and tarnishment).


relief,\(^{249}\) it may be an attractive avenue for redress. However, the question remains whether courts will, in fact, apply the Lanham Act to infringing gTLDs.

The Lanham Act should be flexible enough to apply to gTLDs in the same way it was used to apply to domain name infringement cases before passage of the ACPA. Prior to the ACPA, the Lanham Act provided three actions to trademark owners: (a) registered trademark infringement, where the plaintiff must show that the mark is a registered trademark, the defendant is making commercial use of the mark in commerce, and such use is likely to cause confusion, to cause mistake, or to deceive;\(^{250}\) (b) unfair competition, where the plaintiff must show that the defendant is making commercial use of a registered or unregistered mark in commerce, and such use is likely to cause confusion;\(^{251}\) and (c) trademark dilution where the plaintiff must show that the mark is famous, the defendant is making commercial use of the mark in commerce, the defendant’s use began after the mark became famous, and the defendant’s use of the mark dilutes the quality of the mark.\(^{252}\) The greatest difference between SLD infringement under the previous case law and potential TLD infringement going forward is to what extent the use of a TLD will be considered “commercial use.”

Most successful pre-ACPA cases were brought under the dilution theory. If the mark is “famous,” previous federal court decisions have held that purchasing an SLD incorporating a famous mark and holding the famous mark’s reputation at the registrant’s “mercy” constitutes dilution.\(^{253}\) Importantly, courts have held, for the purposes of a dilution claim, that simply owning a domain name constitutes “commercial use.”\(^{254}\) Additionally, for the purposes of domain name dilution, courts will go beyond the traditional dilution theories (tarnishment and blurring) and hold that a particular domain name “diminished ‘the capacity of the [plaintiff’s] marks to identify and distinguish [the plaintiff’s] goods and services on the Internet.’”\(^{255}\) If anything, these arguments take on more significance in the TLD context: TLDs will likely be seen

---


253. Panavision Inter., L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) (the cybersquatter’s attempt to sell it back for $13,000 did not appease the court); Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1240 (N.D. Ill. 1996).


255. Id. at 1326 (quoting Intermatic, 947 F. Supp. at 1240).
to constitute the newest source indicator and more prominent than an SLD, so that TLDs will diminish the distinguishability of famous marks even further. However, gTLD applicants with federal registrations for their string would be immune from a dilution suit based on reputational damage, meaning Delta Faucets is safe from a dilution claim from Delta Airlines if it registers .delta first. This leaves the dilution claim open only to those gTLD applicants who do not have federal registrations.

It is probable that courts would apply the likelihood of confusion test to TLDs in a way that will resemble its traditional application to non-domain-name trademark infringement. Minute differences exist, however. First, courts analyzing the “area” or trade channels in which the TLDs are marketed or have a presence may conclude the area is the “Internet” generally. Second, sophistication of Internet users has surely improved since the mid-1990s, meaning courts now would probably hold consumers to a slightly higher standard than before.

Remedies outside the New gTLD Program are limited, but in some cases might produce favorable results, such as with the Lanham Act and, specifically, dilution. However, as discussed, Lanham Act remedies can be more fruitful, resulting in damages and injunctive relief, and may be pursued more vigorously than anything that ICANN provides.

VI. BEST PRACTICES FOR TRADEMARK OWNERS

A. Decisions, Decisions

By the time this article is published, trademark owners should already have made an informed decision either to participate in the first round of the New gTLD Program or to refrain from doing so, after careful consultation with their executive, legal, sales, marketing, communications, and information technology personnel.

258. Jews for Jesus v. Brodsky, 993 F. Supp. 282, 304 (D.N.J. 1998) (“[B]oth [domain names, being accessible from an Internet browser,] are marketed in the same manner—i.e., through the Internet.”); Intermatic, 947 F. Supp. at 1235 (“The distribution channel in this case is cyberspace.”).
259. The court in Jews for Jesus stated “[A]n individual may be a sophisticated user of the Internet but may be an unsophisticated consumer of information about religious organizations.” Jews for Jesus, 993 F. Supp. at 303. This distinction probably no longer applies, as consumers become more savvy in regard to using the Internet for research, shopping, learning, and communicating, among other things.
B. The New .[Brand] Owners

Aside from navigating through the application and delegation process, trademark owners who plan to obtain their own .[brand] domain need to ensure that the use of the new .[brand] does not undermine the strength, purpose, and function of their trademark rights. Traditionally, a TLD has been considered a non-distinctive element and, therefore, not capable of being a trademark.260 However, there is some room for argument that TLDs could identify source, even if it is commonly understood that consumers do not consider existing TLDs to have any trademark or brand significance.261 As gTLDs become more numerous, it is probable that consumer perception will change, and at least some new gTLDs will be seen as source identifiers, although that process may not be quick and the change in perception will be incumbent upon the few new .[brand] owners to educate consumers that a gTLD can indicate source rather than simply indicating the “type of entity using the domain name.”262

The primary risk in developing a .[brand] is that the brand loses distinctiveness through improper use. Just as a trademark owner must ensure that its trademark is used by others in a manner that it controls and endorses,263 known as quality control, SLDs controlled by a .[brand] TLD registry may present a similar quality control challenge. If a trademark owner controls its own .[brand] and allows others to register SLDs under that .[brand], it should ensure that the use of such SLDs complies generally with its quality control provisions, just as it requests of its own trademark licensees. In fact, a .[brand] owner should consider having SLD registrants commit to the trademark owner’s quality control requirements as a condition of SLD registration. Otherwise, allowing uncontrolled use or misuse of its .[brand]

260. TMEP (7th ed. Oct. 2010), § 1215.02 (“Generally, when a trademark . . . is composed, in whole or in part, of a domain name . . . the TLD [does not have] any source-indicating significant.”).

261. TMEP (7th ed. Oct. 2010), § 1215.08(a) (“[T]he commercial impression created by the second-level domain name usually remains the same whether the TLD is present or not. [However, i]f the TLD does function as a source indicator, its deletion from the domain name mark may constitute a material alteration of the mark.”). The TMEP provides the following example: “Amending the mark from ABC.PETER to ABC would materially change the mark because the essence of the original mark is created by both the second-level domain and the TLD.” Id.

262. Id.

263. Dawn Donut Co. v. Hart’s Food Stores, Inc., 267 F.2d 358, 367 (2d Cir. 1959) (“If the licensor is not compelled to take some reasonable steps to prevent misuses of his trademark in the hands of others the public will be deprived of its most effective protection against misleading uses of a trademark . . . Clearly the only effective way to protect the public where a trademark is used by licensees is to place on the licensor the affirmative duty of policing in a reasonable manner the activities of his licensees.”).
SLDs may be regarded as losing control over the trademark, resulting in loss of distinctiveness and loss of trademark rights.264

C. All Trademark Owners

Regardless of whether they decide to participate, all trademark owners should take precautions and measures to police and enforce their marks in the new gTLD space. Trademark owners bear the burden of policing their marks.265 Trademark owners are expected to be vigilant in that policing, and may seek to secure the greatest scope of protection for their marks.266 If a trademark owner does not police its mark and act against infringers, the mark may become increasingly diluted by similar uses, and eventually could become, if not generic, narrowly protected.267 However, a mark owner is not required to go after “every possibly infringing use.”268 Trademark owners should be able to bring action strategically, without the need to pursue every possible infringement, and in a manner that is appropriate to the scale of the marketing budget supporting the brand. Part of that strategy should incorporate preventive measures, in particular the less expensive administrative mechanisms, and effective monitoring.

Trademark owners should first monitor the applications for new gTLDs, to identify those that are relevant to their industry (the [.keyword], [.community], or [.place] domains), those that contain strings that are the same as or similar to their trademarks, and those that are being sought by competitors. This form of monitoring should begin promptly when the list of new gTLD applications is expected to be released—late April or early May 2012.

264. Barcamerica Intern. USA Trust v. Tyfield Imps., Inc., 289 F.3d 589, 596 (9th Cir. 2002) (“[W]here the licensor fails to exercise adequate quality control over the licensee, a court may find that the trademark owner has abandoned the trademark, in which case the owner would be estopped from asserting rights to the trademark.”) (quoting Moore Bus. Forms, Inc. v. Ryu, 960 F.2d 486, 489 (5th Cir. 1992)) (internal quotation marks omitted).

265. 2 McCarthy, supra note 225, § 11:91.

266. James Burrough Ltd. v. Lesher, 309 F. Supp. 1154, 1161-62 (S.D. Ind. 1969) (“In view of the strength of the mark and the very substantial good will attaching to it, plaintiffs can be expected to be, and are entitled to be, aggressive in asserting their rights against others. Any coercion involved, or monopolization effected, is no more than plaintiffs are entitled to exert and effect under the law.”).

267. 3 McCarthy, supra note 225, § 17:17; see also Wallpaper Mfrs., Ltd. v. Crown Wallcovering Corp., 680 F.2d 755, 766 (C.C.P.A. 1982) (“Without question, distinctiveness can be lost by failing to take action against infringers. If there are numerous products in the marketplace bearing the alleged mark, purchasers may learn to ignore the “mark” as a source identification. When that occurs, the conduct of the former owner, by failing to police its mark, can be said to have caused the mark to lose its significance as a mark.”).

268. Wallpaper Mfrs., 680 F.2d at 766.
For .[keyword] domains that are relevant to a business, the business must decide whether to file objections pursuant to the procedures outlined in Part IV.A (above).

New .[keyword], .[community], or .[place] domains should also be analyzed for relevance to the trademark owner’s branding and marketing strategy. If, for example, the trademark owner markets to the “green” movement, then it may identify .green as a potential space for its marks. Likewise, if a trademark owner has a presence in New York City, .nyc may be relevant to its marketing plans. The domains that are identified as relevant should be monitored so the trademark owner can ensure that they can participate in any sunrise or “land-rush” registration periods for such domains to obtain registrations that will serve their marketing and business needs and will proactively protect their marks from cybersquatting.

New gTLD applications for strings that are the same as or similar to a trademark must be identified early. A new gTLD is a significant piece of intellectual property because it will be a monopoly on the string for potentially all purposes, unlike trademarks that are confined to protection in connection with specific goods and services. Thus, if .apple is delegated to Apple Records, Apple, Inc. will be at a distinct disadvantage so long as Apple Records owns that TLD. Likewise, the owner of a trademark that is similar to a new gTLD string application should carefully consider whether to challenge the application since once a gTLD is delegated, it will trump future gTLD applications for confusingly similar strings. 269 Trademark owners may wish to file string confusion objections and legal rights objections for strings that they believe could dilute the distinctiveness of their trademarks. They cannot rely on ICANN to take action for them.

In addition to monitoring the new gTLD applications, trademark owners should also strongly consider enrolling their marks in the Trademark Clearinghouse. 270 Importantly, however, trademark owners should consider supplementing the Trademark Clearinghouse entry with their own domain name watch service, to the extent they do not have one already, or ensure that their current service will be watching the new gTLD domain names and picking up non-identical matches that will not be picked up by the Claims Service.

Once relevant new gTLDs are delegated, trademark owners should also continue to monitor the progress of the TLDs over time in order to be prepared if they should apply to ICANN for any changes to their initial charter and purpose that might have

269. Guidebook, supra note 7, § 3.2.1, at 151.
270. See supra Part IV.B.1.
adverse consequences to their trademarks. For example, some TLDs may not initially allow for registration of one- or two-character second-level domains, or may have other restrictions at the beginning, but may apply at a later date to ICANN to allow for changes; trademark owners will want to know when this happens to take advantage of any sunrise periods.  

VII. CONCLUSION  
The New gTLD Program is the most ambitious plan undertaken by ICANN since its inception. The program will dramatically affect how the Internet functions, for better or for worse. If ICANN does not carefully administer this initial round, the consequences for the Internet itself could be very damaging.

Notwithstanding several years of debate and extensive input from the trademark community, ICANN also has fallen short in terms of the protections needed for trademark owners. While the Clearinghouse and Claims Services offer some protection, primarily by providing notice of cybersquatters who are seeking to register domain names that exactly match registered trademarks, the explosive availability of new cybersquatting opportunities will be felt by all. If trademark owners do not choose to monitor activity in these new gTLDs, they may risk exposing their brands to increased cybersquatting, which may negatively impact the image and reputation of their trademarks. If trademark owners increase spending as required to monitor and maintain their intellectual property portfolios, they may also need to raise the prices for their products or services to offset the increased monitoring costs—a result few would like to see. Trademark owners will not like either option.

The efficacy of this program in changing the way gTLDs are used and experienced is largely untested. Consumers may adjust to and accept the new gTLDs and experience the internet in new ways, as ICANN predicts. Or, the program may fail as have other gTLD rollouts, whose predicted success and acceptance did not

271. This happened when RegistryPro proposed expansive contract amendments for the .pro registry contract. Included in the requests was expanding the list of professions eligible for a .pro TLD. Proposed Contract Amendments from RegistryPro Posted for Public Comment, ICANN (Mar. 14, 2008), http://www.icann.org/en/announcements/announcement-14mar08.htm.

272. See Tina Dam, ICANN, the New gTLD Program, and Our Responsibility for the Internet, Circle ID (Aug. 2, 2011, 7:45AM), http://www.circleid.com/posts/icann_the_new_gtdl_program_and_our_responsibility_for_the_internet/ (arguing that it is the responsibility of all of us Internet users to ensure this new program is a positive experience for everyone, because any other result will be problematic).
nearly match the results. Unsuccessful launches of hundreds of new gTLDs could have significant negative consequences for the Internet as a whole, which is also to no one’s benefit. However, regardless of whether the New gTLD Program will yield benefits for successful gTLD applicants or consumers, the cost and the time required to monitor the program and to learn and subsequently invoke the protection mechanisms provided by the program, will surely increase—to the detriment of trademark owners and their customers.

273. See Mark Jeftovic, Who Will Be the Big Winners and Losers of the New gTLDs?, Domain Name News (Aug. 5, 2011, 12:27 PM), http://www.domainnamenews.com/editorial/big-winners-losers-tlds/9646 (“So far every attempt to roll [a New gTLD Program] out owes it’s [sic] sustenance to purely defensive registrations (.biz, .info) or else it’s degraded into an utter fracas (.jobs) or just plain flopped (.pro.”).