Beyond .Com: What Risk Does the Explosive Growth of Top Level Domains Pose to Your Trademark: Can You Get Any Relief?

Robert V. Donahoe[*]

[*] Associate, Patent and Intellectual Property Group at Testa, Hurwitz & Thibeault, LLP, Boston, Massachusetts. J.D. 2001, Boston College Law School; B.S.E.E. 1985 cum laude, Northeastern University.

I. INTRODUCTION

Since the first half of the twentieth century, scientists have recognized that we live in an expanding universe.[1] Today, thanks to the Internet, the trademark universe, too, is constantly expanding. This new commercial medium has created an ubiquitous channel of trade that mark owners can use for commercial gain. Of course, the Internet has also increased the risk of consumer confusion resulting from trademark infringement because it provides a common international channel of trade that spans all business sectors.[2] Domain names are the source of a large percentage of Internet based trademark disputes. Further, cybersquatting is the primary trademark offense committed with domain names.[3]

Cybersquatting is a novel trademark offense, unique to the Internet, and has flourished with the growth of the Internet.[4] This Article explores the most effective tools in the battle against cybersquatters, identifies existing and proposed Top Level Domains (TLDs) that mark owners must monitor to prevent cybersquatting, and identifies what, if any, anti-cybersquatting actions are available in the various TLDs. The results of this study show that, despite recent legislative success and progress by international governing bodies, the ability to protect a trademark used in a domain name varies widely across the globe from jurisdiction to jurisdiction.[5] Additionally, further growth and splintering of TLDs

[1] Virginia Trimble, *Looking Backward: Themes of the 20th-Century Astronomy*, SKY & TELESCOPE, 99, Issue 1, Jan. 1, 2000. The article refers both to the development of Einstein's theory of relativity to account for the phenomena, and the observations of Hubbel who discovered physical evidence that the universe was indeed expanding.

[2] Olivia Maria Barrata & Dana L. Hanaman, Note, *A Global Update on the Domain Name System and the Law: Alternative Dispute Resolution for Increasing Internet Competition—Oh the Times They Are A-Changin'!*, 8 TUL. J. INT'L & COMP. L. 325, 333 (2000).

[3] JEROME GILSON & ANNE GILSON LALONDE, THE ANTICYBERSQUATTING CONSUMER PROTECTION ACT AND THE ICANN UNIVERSAL DOMAIN NAME DISPUTE RESOLUTION POLICY 3 (2000). The term "cybersquatter" refers to a person who registers a domain name that includes the mark of another without any intent to use the mark for a legitimate on-line activity. "Cybersquatting" literally describes the acts of one who purchases and holds, and perhaps ransoms to the legitimate owner, a domain name containing the trademark or servicemark of another. The narrow definition of "cybersquatting" does not literally include cyberpirates, those who intend to use the mark of another in a domain name in order to divert traffic and reap the benefits of the goodwill in the mark. For purposes of this Article, the terms "cybersquatting" and "cybersquatter" will be used in reference to the preceding broad definition that encompasses cybersquatters, described literally, and cyberpirates.

[4] *Id.* at 17.

[5] Nicholas Wood, Address at the WIPO Conference on Intellectual Property Questions Relating to the ccTLDs (Feb. 21, 2001) (audio recording available at http://ecommerce.wipo.int/meetings/2001/cctlds/program/index.html).

assures the continued expansion of domain name related trademark disputes for the foreseeable future.[6]

The Article concludes that the continued increase in available authorized TLDs will benefit trademark owners. However, the benefits will only accrue to mark owners who stay abreast of the continued expansion of TLDs in order to determine how to secure domain names in the new TLDs and where to most vigorously police for infringers.

II. BACKGROUND

A. *Domain Names*

It is worthwhile to spend a moment reviewing domain name related terminology because the nomenclature is often used in a confusing and inconsistent manner.[7] First, a domain name is a unique alphanumeric character string that provides a Web address for its owner.[8] Generally, an owner selects a domain name because it in some way describes the owner or the owner's on-line activities.[9] Each domain name is also associated with an Internet Protocol (IP) address. The IP address is the numerical identification used to locate a specific computer connected to the World Wide Web.[10] By eliminating the need to remember a string of numbers, the domain name creates a more user-friendly and intuitive method of locating addressees.[11]

A domain name is made up of two or more character strings separated from one another by periods.[12] A TLD appears to the right of the lower level domains and provides the foundation for the domain name, such as the familiar .com, .org, and .net TLDs. These are referred to as global TLDs (gTLDs) because they are administered on a global,

[6] Thomas Claburn, *New Domains, New Headaches*, Smart Business from ZD Wire (Mar. 12, 2001) 2001 WL 74884079.

[7] F.T. McCarthy, *Domain Strain: ICANN's Unwelcome Rival: The Body that Overseas the Internet's Address System Has to Face Down a Challenger*, THE ECONOMIST (Mar. 10, 2001) 2001 WL 7318041 (referring to the domain names based on New.net as TLDs).

[8] Presently, domain name characters are limited to Arabic numbers, Roman characters and hyphens. See VeriSign Global Registry Services, *General Information Paper on Multilingual Domain Name Resolution* (Apr. 3, 2001) http://www.verisign-grs.com/multilingual/Gen_Info_Paper.pdf.

[9] Most corporations use their trademark as their domain name; for example, ford.com for the Ford Motor Company.

[10] MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW 1094 (2000).

[11] This is particularly helpful when searching for a site that the Web surfer has not previously visited. For example, if you are planning a vacation and would like to use Priceline's reverse auction services to purchase airplane tickets, you simply enter www.priceline.com to locate the Priceline home page.

[12] Barrata, *supra* note 2, at 332.

not a regional, basis.[13] They are also referred to as unrestricted[14] because their use is not limited to a specific class of users or specific range of interests.[15] Further, these three TLDs are referred to as authorized TLDs because the Internet Corporation for Assigned Names and Numbers (ICANN) authorizes and administers their use.[16] Lastly, ICANN has recently authorized seven new gTLDs that include both sponsored gTLDs and unsponsored gTLDs.[17] The two categories have also been referred to as sTLDs and uTLDs. The importance of these last two distinctions, authorized/unauthorized and sponsored/unsponsored, as they relate to pursuing cybersquatters, is explored in greater detail in Parts IV and V of this Article.

The preceding TLDs do not appear alone as Web addresses. Instead, TLDs are combined with a user selected Second Level Domain (SLD) when a user registers a domain name. For example, "priceline.com" includes a TLD, the .com, as well as a SLD, priceline. Additional lower level domains can also be attached as prefixes to the SLD.TLD combination; for example, "infoeagle.bc.edu" identifies a central information page for Boston College. The "infoeagle" portion of the domain name is referred to as a Third Level Domain (3LD).[18]

A domain name cannot be used until it is registered with a registrar and then incorporated into the domain name system by a registry.[19] Register.com is an example of a registrar.[20] VeriSign, formerly Network

[13] As opposed to country code TLDs that are explored in greater detail in Part IV.B.

[14] Barrata, *supra* note 2, at 332. They have also been referred to as generic TLDs because they were originally aimed at a specific genus of Internet activity; for example, .com was originally planned for use by commercial entities.

[15] The Article does not address the authorized, restricted gTLDs, .edu, .gov, and .mil in any detail because of the decreased risk of cybersquatting in these domains. The lower risk is the result of preregistration requirements administered in each gTLD.

[16] LEMLEY ET AL., *supra* note 10, at 1093. ICANN is a nonprofit corporation formed in 1998 to administer IP address allocation and domain name system management. The .com, .org, and .net TLDs are referred to as authorized TLDs because they are authorized for use on the World Wide Web.

[17] The sponsored domains—.aero, .coop, and .museum—target a narrow class of registrants and carry out the policy formulation responsibilities related to the domain. ICANN is responsible for the policy formulation of the unsponsored domains—.biz, .info, .name, and .pro.

[18] Barrata, *supra* note 2, at 332.

[19] Register.com is one of the largest domestic registers. The intuitive link between their domain name and their business demonstrates the value that a domain name can provide (last visited Sept. 10, 2001) *at* http://register.com. Throughout the Article, the term "register," when referring to domain names, is used to describe the act of securing rights to a domain name through a domain name registrar. This use of "register" should not be confused with the traditional use of the term to describe the registration of a trademark with state or federal bodies.

[20] For a list of ICANN approved registers, see ICANN, *List of Accredited and Accreditation Qualified Registrars* (last modified Sept. 7, 2001) http://www.icann.org/registrars/accredited-list.html.

Solutions Inc., is an example of a registry.[21] Generally, domain name registrations are issued for a fixed term on a first come first served basis. At the risk of oversimplifying, the registrar can be compared with the wait staff at a restaurant because they are order takers. They will also let you know when your "favorite dish," perhaps your company's trademark, is unavailable. Registrars provide an interface between the registrant and the registries. The registries operate as the kitchen staff because they actually execute your request. The registry maintains the list of registered domain names and handles other behind the scenes functions that make a domain name accessible to Internet users.[22]

B. Development of Anti-Cybersquatting Law

A "landrush" in domain names began to develop during the mid-1990s when it became clear that the Internet would become a popular means of trade.[23] Early cybersquatters focused on registering domain names using trademarks of the strongest brands they could secure.[24] Thus, some of the nation's leading corporations found themselves targets of ransom requests wherein the cybersquatter offered to sell a corporation a domain name using the corporation's mark.[25]

In an effort to alleviate harm caused by cybersquatters, the courts extended the existing law, often forcing the square peg of cybersquatting into the round hole of then-existing trademark protection.[26] Generally, successful plaintiffs relied on the federal anti-dilution statute.[27] The alleged harms included: (1) dilution by blurring that results when the trademark owner cannot control the good and services displayed under the trademark,[28] (2) dilution by tarnishment created when the trademark becomes associated with low quality goods or services,[29] and (3) the

[21] *See supra* note 8.

[22] These behind the scene activities include addressing, resolution, and distribution services.

[23] Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998) (identifying over 100 marks registered as domain names by the defendant).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION, § 25:76 (4th ed. 2000).

[28] Bally Total Fitness Holding Corp. v. Faber, 29 F. Supp. 2d 1161, 1168 (C.D. Cal. 1998).

[29] Hasbro, Inc. v. Internet Entertainment Group Ltd., 40 U.S.P.Q. 1479, 1480 (W.D. Wash. 1996) (CANDYLAND for children's game held diluted by tarnishment by "candyland.com" for Web site showing sexually explicit pictures).

inability of the trademark owner to use the mark to identify their own goods and services on the Internet.[30]

However, potential plaintiffs found it difficult to craft an effective cause of action based on traditional trademark law. A court may conclude that a cybersquatter did not meet the "commercial use" prong of an anti-dilution claim;[31] therefore, the anti-dilution statutes did not always reach those who bought and held a domain name.[32]

In late 1999, in response to the legal challenge posed by cybersquatting, Congress passed and the President signed into law the Anti-Cybersquatting Consumer Protection Act (ACPA).[33] The ACPA created a cause of action for persons who register domain names with a "bad faith intent to profit." At about the same time the ACPA was signed into law, ICANN established a Universal Dispute Resolution Procedure (UDRP) wherein a trademark owner can challenge a third party who "registers and uses in bad faith a domain name that is confusingly similar to a trademark."[34] Both measures provide a powerful tool for trademark owners in the battle against cybersquatting.[35] The new measures' benefits are the subject of the following section.

III. STRUCTURE AND EFFECTIVENESS OF TWO RECENTLY ADOPTED ANTI-CYBERSQUATTING MEASURES

It is worth noting at the outset that both the ACPA and the UDRP provide ex-post remedies for cybersquatting. Neither prevents a domain name from being registered with a bad faith intent to profit. Preemptive measures aimed at preventing cybersquatting and related domain name disputes are discussed in Part IV.B.4. Additionally, both the ACPA and UDRP focus solely on cybersquatting. Thus, they are aimed at only the most egregious trademark misusers.

[30] Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1319 (9th Cir. 1998).

[31] Academy of Motion Picture Arts & Sci. v. Network Solutions, Inc., 989 F. Supp. 1276, 1280 (C.D. Cal. 1997) (finding that the mere registration of a domain name does not constitute a commercial use).

[32] MCCARTHY, *supra* note 27.

[33] November 29, 1999, Pub. L. 106-113, Div. B, § 1000(a)(9) [Title III, § 3002(a)], 113 Stat. 1536, 1501A-545.

[34] ICANN, *Uniform Domain Name Dispute Resolution Policy* (last modified June 4, 2000) http://www.icann.org/udrp/udrp-policy-24oct99.htm [hereinafter *UDRP*].

[35] GILSON & LALONDE, *supra* note 3, at 38.

A. Anti-Cybersquatting Consumer Protection Act

The ACPA is aimed at those who use another's mark in a domain name for profit without the owner's consent.[36] To succeed on a claim brought under the ACPA, a plaintiff must show that: (1) plaintiff's mark is distinctive or famous; (2) defendant's domain name is identical or confusingly similar to plaintiff's mark; and (3) defendant used, registered, or trafficked in the domain name with bad faith intent to profit from sale of the domain name.[37] The law only applies where the person using the domain name is the domain name registrant or that registrant's authorized licensee.[38] Under the ACPA, a court may order that the domain name be forfeited, cancelled, or transferred to the owner of the mark.[39] The ACPA provides in rem jurisdiction in the judicial district where the registrar of the domain name is located if the trademark owner either is: (1) unable to secure personal jurisdiction over the defendant or (2) unable to locate the defendant.[40]

1. Bad Faith Intent to Profit

The "bad faith intent to profit" standard squarely targets cybersquatters and eliminates the need to force fit a cybersquatting claim within the original federal anti-dilution statute.[41] Trademark owner's success under the law rests on the court's interpretation of the bad faith standard.[42] The law also creates a defense of "innocent use." Thus, bad faith intent will not be found where the court determines the registrant had reasonable grounds to believe and did believe that the use of the domain name was either a fair use or an otherwise lawful use.[43]

The statute includes a nonexclusive list of nine factors that a court may consider in determining if a registrant has a bad faith intent to profit in using a domain name.[44] The nine factors provide the court with a

[36] 15 U.S.C. § 1125 (d)(1)(A) (2000).

[37] *Id.*

[38] *Id.* § 1125(d)(1)(D). Thus, Internet Service Providers (ISPs) and those who hyperlink to an offending site are not culpable under the ACPA.

[39] *Id.* § 1125 (d)(1)(C).

[40] *Id.* § 1125(d)(1)(E)(2)(A); *see also* Alitalia-Linee Aeree Italiane S.p.A. v. Casinoalitalia.com, 128 F. Supp. 2d 340, 344 (E.D. Va. 2001) (finding that a plaintiff cannot proceed in rem unless one of the two conditions is not satisfied because personal jurisdiction and in rem jurisdiction are mutually exclusive).

[41] Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489, 495 (2d Cir. 2000).

[42] Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 271 (4th Cir. 2001) ("The ACPA was not enacted to give companies the right to fence off every possible combination of letters that bears any similarity to a protected mark.").

[43] 15 U.S.C. § 1125(d)(1)(B)(ii).

[44] *Id.* § 1125(d)(1)(B)(i).

standard that can be used to measure both the reasonableness of a registrant's good faith belief that they were legally entitled to the domain name (factors 1, 2, 3, and 4) and the malicious intent of registrants as judged by their acts (factors 5, 6, 7, 8, and 9).[45]

The first four "good faith factors" are premised on the recognition that good faith belief is reasonable when the user of the domain name either has: (1) a legitimate claim that they are legally entitled to use the mark or (2) an established history using the mark.[46] The first factor asks what "trademark or other intellectual property rights" the user has in the domain name.[47] The second factor asks to what "extent the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person."[48] Both factors one and two recognize that a good faith belief of innocent use is supported when the domain name user is already entitled to use the mark in some other context.[49] The third factor looks to "the person's prior use . . . of the domain name in connection with the bona fide offering of any goods and services."[50] This factor recognizes that a good faith belief of innocent use is supported when user has previously applied the mark commercially.[51] The fourth factor looks to "the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name."[52] This factor acknowledges that a good faith belief of innocent use is supported when the user employs the mark to attract visitors to a Web site that provides commentary, news reporting, parody or other fair uses that could reasonably be expected to escape charges of infringement.[53]

The five "malicious intent factors" are used to evaluate the user's actions to determine if they demonstrate a conscious effort to harm trademark owners, profit from speculation in domain names, or anonymously carry on in the domain name trade.[54] The first of these is the fifth of the nine listed factors.[55] The fifth factor looks at the intent of the user to harm the goodwill represented in the mark by diverting

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] Northland Ins. Cos. v. Blaylock, 115 F. Supp. 2d 1108, 1124 (D. Minn. 2000) (finding that bad faith intent was supported where the defendant had no prior rights to the mark in any other context).

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] 15 U.S.C. § 1125(d)(1)(B)(i).

[55] *Id.*

customers "either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site."[56] This factor uses both subjective and objective components in evaluating the user's state of mind.[57] For example, the subjective test is applicable where the user acknowledges an intention to divert customers in order to promote commercial activity on the user's site.[58] Site content that includes offers of goods or services similar to those offered by the trademark holder is an example of objective indicia that supports a finding of bad faith under the fifth factor.[59] This factor indicates that malicious intent is demonstrated by either: (1) the intentional diversion of consumers for commercial gain or (2) the existence of a likelihood of confusion regardless of the domain name owner's intent.

The sixth and eighth factors look for objective evidence of the registrant's attempts to profit from speculation in domain names.[60] The seventh factor looks for objective evidence that the user has attempted to hide their identity or otherwise make it difficult to connect them with the domain name registration.[61]

The ninth factor looks to the strength of the plaintiff's mark. The defendant's registration of strong or distinctive marks may demonstrate that the mark or marks were registered in bad faith. This bad faith element presumes that cybersquatters do not waste their time registering nondistinctive marks because nondistinctive marks have a lower market value.[62]

The factors form the basis of a totality test.[63] The court may evaluate these and any other factors that it identifies based on the specific facts of each case.[64] No factor is identified as being dispositive

[56] *Id.*

[57] N. Light Tech., Inc. v. N. Lights Club, 236 F.3d 57, 59 n.3 (1st Cir. 2001) ("Plaintiff does not allege that defendants had actual knowledge of the northernlight.com registration when they registered the northernlights.com domain name").

[58] Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 269 (4th Cir. 2001) (finding that the defendant acknowledged in his deposition that he was aware of the similarity between the plaintiff's mark and the domain name that he registered).

[59] *Id.*

[60] *Id.* at 65 (finding that the defendant had a "well-established pattern of registering multiple domain names containing *famous trademarks*, such as rollingstones.com, evinrude.com, and givenchy.com").

[61] 15 U.S.C. § 1125(d)(1)(B)(i).

[62] MCCARTHY, *supra* note 27, § 25:78.

[63] *Id.*

[64] *See Virtual Works, Inc.*, 238 F.3d at 268 (finding that "[a] court is not limited to considering these nine factors when determining the presence or absence of bad faith").

or essential to the inquiry.[65] It is not a precise mathematical calculation but a comparison between evidence supporting the reasonableness of a good faith belief and evidence supporting the malicious intent of the registrant.[66]

Even where bad faith is found the defendant may escape culpability if they lacked any "intent to profit."[67] In *Northland*, the defendant, a disgruntled customer of Northland Insurance, registered the domain name "northlandinsurance.com."[68] The defendant proceeded to post a description of his negative experiences with Northland and solicit similar content from other Internet users who also felt that they had been treated poorly by Northland.[69] However, the court found that although the defendant exhibited bad faith he had not violated the ACPA because there was no evidence that he intended to profit from the Web site. The defendant had not solicited Northland in order to sell the domain name and he was not running a commercial operation on the Web site.[70]

Many commentators applaud the heightened protection provided to trademark holders by the ACPA.[71] However, the law has also attracted the wrath of members of the Internet community who argue that it tilts too heavily in favor of trademark owners.

B. Universal Dispute Resolution Procedure

The UDRP provides an international dispute resolution process that is uniformly administered under rules adopted by ICANN.[72] As advertised by one of the approved dispute resolution service providers (DRSPs), the UDRP process provides a means where parties can resolve their disputes in "a safe affordable forum without leaving home."[73] The managing organizations of all unsponsored TLDs follow ICANN approved dispute resolution procedures.[74] Thus, compliance with the

[65] *Id.* at 270 (finding that the offer to sell a domain name is not itself evidence of unlawful trafficking).

[66] *See* N. Light Tech., Inc. v. N. Lights Club, 236 F.3d 57, 65 (1st Cir. 2001) (finding that the pattern of ransoming famous trademarks trumped evidence that the defendant used northernlights.com as an e-mail domain name for several years prior to the dispute with the plaintiff).

[67] Northland Ins. Cos. v. Blaylock, 115 F. Supp. 2d 1108, 1125 (D. Minn. 2000).

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *See, e.g.*, GILSON & LALONDE, *supra* note 3, at 38.

[72] ICANN, *Rules for Uniform Domain Name Dispute Resolution Policy* (last modified Jan. 3, 2000) http://www.icann.org/udrp/udrp-rules-24oct99.htm [hereinafter *UDRP Rules*].

[73] National Arbitration Forum, *Guide to Dispute Resolution for Domain Names* (last visited Sept. 7, 2001) http://www.arbforum.com/domains/domain-guide.asp.

[74] *See* UDRP, *supra* note 34.

UDRP is mandatory for cybersquatting disputes arising from domain names that are registered in any authorized unsponsored gTLD.

Every domain name registrant agrees to submit to the UDRP when they register a domain name because the UDRP is incorporated by reference in the registration contract. The procedure became effective on December 1, 1999, when the World Intellectual Property Organization (WIPO), the first approved dispute-resolution service provide, began receiving complaints.[75] The initial proceeding commenced on December 9, 1999, and was decided on January 14, 2000.[76]

In practice, the UDRP provides an administrative proceeding where aggrieved trademark owners can rapidly secure a decision regarding rights to a disputed domain name.[77] Indeed, in-person hearings, including teleconference, videoconference, and Web conference, are prohibited by the UDRP except where the arbitrators, in their sole discretion, determine otherwise.[78]

The procedure begins when the complaint selects a DSRP from the ICANN approved list.[79] The complaint, the response, and any supplemental filings are filed with a dispute-resolution service provider who assigns an arbitrator. The decision of a single-member panel will be communicated to the parties and ICANN within a maximum of fifty days.[80] The process is also inexpensive.[81]

[75] ICANN, *Timeline for the Formulation and Implementation of the Uniform Domain Name Dispute Resolution Policy* (last modified Oct. 17, 2000) http://www.icann.org/udrp/udrp-schedule.htm.

[76] World Wrestling Fed'n Entm't, Inc. v. Bosman, WIPO Case No. D99-0001.

[77] The decision in *Nabisco Brands Co. v. The Patron Group, Inc.*, WIPO Case No. D2000-0032, was made in a mere sixteen days.

[78] UDRP Rules, *supra* note 72, Rule 13.

[79] ICANN, *Approved Providers for Uniform Domain Name Dispute Resolution Policy* (last modified Nov. 30, 2001) http://www.icann.org/udrp/approved-providers.htm. Presently, there are four dispute-resolution service providers approved by ICANN; WIPO, the National Arbitration Forum, CPR Institute for Dispute Resolution, and the Asian Domain Name Dispute Resolution Centre (ADNDRC). ADNDRC is a newly approved DRSP committed to providing panelists familiar with Asian languages. *See* ICANN, *ICANN Announces New Dispute Resolution Service Provider in the Asia Pacific Region* (last visited Dec. 26, 2001) http://www.icann.org/announcements/announcement-03dec01.htm. Former approved DRSP eResolution has closed for financial reasons. The company stopped taking new complaints beginning December 1, 2001.

[80] As follows: 3 days for the DSRP to review the complaint and forward to defendant; 5 additional days for complainant to correct any deficiencies; 20 days for defendant to respond; 5 days for an arbitrator to be assigned; 14 days for the arbitrator to render a decision; and 3 days for the dispute-resolution service provider to communicate the full text of the decision to the parties.

[81] National Arbitration Forum, *Schedule of Fees* http://www.arbforum.com/domains/domain-fees.asp (charging a fee of $950 for a single panelist hearing on a claim involving one domain name).

Domain name registrants must submit to the UDRP should a third party assert that: (1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights, (2) the registrant has no rights or legitimate interests in respect of the domain name, and (3) the domain name has been registered and is being used in bad faith.[82] Thus, the plaintiff's evidentiary requirements under the UDRP are almost identical to those required for an ACPA claim.

Complaints must specify the domain names that are being complained of, the marks on which the complaint is based, the goods and services sold under the mark, the intended future use of the mark, the grounds of the complaint, and the remedies that the complainant seeks.[83] The complainant can also provide exhibits, such as a copy of the complainant's trademark registration or an image of the offending Web site.[84] Remedies are limited to domain name cancellation or domain name transfer to the complainant.[85] The complainant must submit both a hardcopy and an electronic copy of the complaint.[86] Standard complaint forms can be found at the Web site of each of the dispute resolution service providers.[87]

The respondent must respond within twenty days of the date that the DRSP forwards the complaint.[88] An arbitrator is assigned within five days of the DRSP receiving the respondent's reply.[89] The arbitrator, or arbitrators if a three member panel is selected, will make a decision within fourteen days of being appointed.[90] Once a decision is made, the DRSP has three days to communicate the full text to the parties.[91] If the arbitrator decides against the respondent, the respondent then has an additional ten days to provide official documentation showing that it has commenced a lawsuit against the complainant.[92] Should the respondent provide the required documentation, the registrar is prohibited from canceling or transferring the domain name registration until they receive evidence of either: (1) a settlement that authorizes the transfer or

[82] *See* UDRP, *supra* note 34, para. 4(a)(i)-(iii).

[83] UDRP Rules, *supra* note 72, Rule 3.

[84] *Id.*

[85] *Id.* Rule 15(b).

[86] *Id.* Rule 3.

[87] *See supra* note 83.

[88] UDRP Rules, *supra* note 72, Rule 5(a). A decision will still be made even when the respondent fails to respond.

[89] *Id.* Rule 4.

[90] *Id.* Rule 15(b).

[91] *Id.* Rule 16.

[92] *See* UDRP, *supra* note 34, § 4(k).

(2) completion of the lawsuit wherein the respondent no longer has the right to use the domain name.[93]

The UDRP does not provide an internal appeals process. However, each complainant must agree, in advance, to submit to the jurisdiction of one of two courts should the respondent challenge the arbitrator's decision.[94] The two courts are those located at either: (1) the location of the registrar's principal office or (2) the domain name holder's address as shown on the WHOIS database when the complaint is filed.[95]

1. Registration and Use in Bad Faith

At first glance, the UDRP appears to require "use" of the challenged domain name—in other words something more than mere registration. The ACPA avoids this ambiguity by allowing liability where the defendant either "registers, traffics in, or uses" the domain name.[96] However, the UDRP includes examples of buying and holding domain names that meet the bad faith standard.[97] For example, registering a domain name in order to block the owner of the mark from using the mark in a domain name is evidence of bad faith provided that the registrant has engaged in a pattern of such conduct.[98] The very first UDRP proceeding addressed a similar situation. In "worldwrestling federation.com" the respondent registered the domain name, offered to sell it to the WWF within three days of registering it, and was not using the domain name at the time of the proceeding.[99] The arbitrator found that the registrant had "registered" and "used" the domain name in bad faith.[100] Another panel found that a respondent had "used" a domain name even though they had made no effort to sell the domain name or establish a Web site at the address.[101] The panel found other factors, including the respondent's efforts to conceal its identity, supported a

[93] *Id.*

[94] UDRP Rules, *supra* note 72, at 1, 3(b)(xiii).

[95] *Id.* The UDRP expressly allows either party to pursue the domain name dispute in court. However, the result of litigation in the various foreign jurisdictions that may have a nexus to a claim is far from certain as is the deference, if any, that a court will give a prior UDRP decision regarding the same dispute. The First Circuit Court of Appeals recently determined that a party may use the ACPA to attempt to regain ownership of a domain name following an unfavorable UDRP decision. *See* Sallen v. Corinthians Licenciamentos LTDA, No. 01-1197, 2001 WL 1518455, at *1 (1st Cir. Dec. 5, 2001).

[96] 15 U.S.C. § 1125(d)(1)(A)(ii).

[97] *See* UDRP, *supra* note 34, § 4(b)(ii).

[98] *Id.*

[99] World Wrestling Fed'n Entm't, Inc. v. Bosman, WIPO Case No. D99-0001.

[100] *Id.*

[101] Telstra Corp. Ltd. v. Nuclear Marshmallows, WIPO Case No. D2000-03.

finding that the domain name was being used in bad faith.[102] Thus, it appears that "use" is interpreted very broadly where the UDRP is applied.[103]

An offer to sell a domain name at a profit has been cited as the most common factor used by UDRP panels to support a finding of bad faith.[104] In several cases, the registration for resale of multiple domain names has also been used to support a finding of bad faith use.[105]

The nonprecedential nature of the UDRP decisions has also created concern among trademark holders regarding the consistency of panel's analysis from case to case. However, many of the panelists contracted by the DRSPs come from legal backgrounds where precedent plays a primary role. It is difficult, if not impossible, for panelists who have spent their entire careers being trained to follow precedent to suddenly ignore that approach when applying the UDRP. A recent WIPO panel, deciding a cybersquatting dispute under the modified UDRP used for the Philippines TLD, cited the complainant's 100% success rate in thirteen previous UDRP panels and the facts of those cases in their decision.[106] The panel's decision transferred two domain names to the complainant, Yahoo!.[107] References to prior UDRP decisions have become so commonplace in panel decisions that one commentator observed that reliance on precedent may harm the original objective of the UDRP.[108] The panelists' reliance on precedent forces attorneys to research past decisions, at the client's expense, in order establish the relevant UDRP "rule of law." The commentator points out that the increasing complexity created by this approach will eliminate the UDRP as a low cost alternative to the courts.

Trademark owners' success under the UDRP is extraordinarily high.[109] Further, one study indicates that the selection of DRSP may be outcome determinative, or at least a good indicator of the likelihood of

[102] *Id.*

[103] *Id.*

[104] GILSON & LALONDE, *supra* note 3, at 30.

[105] *Id.*

[106] Yahoo!, Inc. v. Yahoo Computer Servs., WIPO Case No. DPH2001-001.

[107] *Id.* The domain names were "yahoo.com.ph" and "yahoo.ph."

[108] Jo Saxe Levy, Name Blame: In Trying to Avoid a Legal Bureaucracy, ICANN May Have Created One of Its Own, Apr. 1, 2001.

[109] ICANN, *Statistical Summary of Proceedings Under the Uniform Domain Name Resolution Policy* (last modified Dec. 21, 2001) http://www.icann.org/udrp/proceedings-stat.htm. Close to eighty percent of the decisions have been in favor of the complainant. Other on-line searchable databases include cyber.law.harvard.edu/icann/search/, www.icann.org/cgi-bin/udrp/udrp.cgi, and www.dnlr.com.

success of the claim.[110] The study demonstrates that both the WIPO and the National Arbitration Forum are more favorable to complainants than decisions rendered by eResolutions.[111]

C. The ACPA and UDRP Compared

With the ACPA and the UDRP trademark owners now have two powerful tools from which to choose in the battle against cybersquatting.[112] The two procedures are not mutually exclusive but specific factual circumstances may lend one more effective than the other for a given circumstance.[113]

The UDRP proceedings are both quick and inexpensive. However, remedies are limited and arbitrators are not required to follow precedent. Further, the format and scope of the UDRP prevent arbitrators from hearing related claims or more complex or ambiguous factual situations.[114] Lastly and of great importance to trademark owners, UDRP is only available where required by ICANN or voluntarily adopted by management of other TLDs.

The ACPA provides the following benefits as compared to UDRP: (1) ACPA decisions are binding, (2) ACPA allows recovery of monetary damages,[115] and (3) the ACPA provides an adjudicative forum that is bound by precedent and is very familiar to plaintiff's counsel. Finally, the ACPA will reach any cybersquatter in personam so long as they have a presence in the United States and can be located. In rem jurisdiction is also available where the domain registry is located within the territory of any United States district court.[116]

But just how effective are these tools in combating cybersquatting outside the traditional .com, .net, and .org domains?

[110] Colby B. Springer, Comment, *Master of the Domain (Name): A History of Domain Name Litigation and the Emergence of the Anticybersquatting Consumer Protection Act and Uniform Dispute Resolution Policy*, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 315, 355 (2001).

[111] *Id.*; *see also ebusiness: Domain Name Cases 'Favour Holders'*, BIRMINGHAM POST (Aug. 28, 2001) 2001 WL 26526732 (describing a recent study by Professor Michael Geist that also demonstrated the impact of DRSP selection in UDRP proceedings). Ultimately, the more respondent-favorable outcome of eResolutions' decisions may have led to eResolutions' demise because dispute resolution is initiated by complainants.

[112] GILSON & LALONDE, *supra* note 3, at 38.

[113] *Id.* The intersection of the two proceedings has created another developing body of law. *See* Sallen v. Corinthians Licenciamentos LTDA, No. 01-1197, 2001 WL 1518455, at *1 (1st Cir. Dec. 5, 2001).

[114] *Id.*

[115] 15 U.S.C. § 1117(d) (2000). The ACPA allows statutory damages of up to $100,000 per domain name should the plaintiff elect statutory damages in lieu of actual damages.

[116] *Id.* § 1125(d)(2)(D)(i).

IV. Challenges Facing Trademark Owners Due to the Continued Growth of TLDs

As if trademark owners did not have enough concern protecting themselves in the .com, .org, and .net domains, explosive growth in TLDs has dramatically increased the risk of trademark misuse.[117] Mark owners can no longer protect their marks simply by monitoring the three open gTLDs for infringers. First, ICANN approved seven new TLDs in November 2000.[118] Second, there is a continued expansion of commercial activity in country code TLDs (ccTLDs).[119] Third, technical and marketing advances are increasing the viability of alternate TLDs.[120] Finally, multilingual TLDs (mlTLDs) are presently being tested. These mlTLDs have the potential to reach huge segments of the global population previously shutout by an English language based system. This section of the Article describes each of the preceding domains and evaluates the effectiveness of the anti-cybersquatting protection available within each.

A. *Newly Approved TLDs*

On November 16, 2000, ICANN selected seven new gTLDs; .aero, .biz, .coop, .info, .museum, .name, and .pro.[121] The new gTLDs were originally scheduled for release in June 2001. However, the release dates were delayed because detailed registration agreements first must be negotiated with the sponsors and operators of each of the new gTLDs.

Unlike the present structure of the .com, .net, and .org domains, six of the seven new gTLDs restrict the class of registrant in their domain. For example, the .biz domain is limited to use for "bona fide business or commercial purposes,"[122] .aero is limited to persons who are affiliated with the air transport industry, and .pro is limited to persons who are affiliated with a profession such as accountants, lawyers, or physicians.

[117] Barrata, *supra* note 2 (finding that there are, on average, 10,000 domain name registrations per day).

[118] Claburn, *supra* note 6.

[119] David Daggett, *Country Specific Domain Names Raise Difficult Trademark Issues* (visited Sept. 10, 2001) http://www.gigalaw.com/articles/daggett-2000-06-p1.html.

[120] McCarthy, *supra* note 7.

[121] ICANN, *New TLD Program* (last modified Dec. 17, 2001) http://www.icann.org/tlds. To date, ICANN has completed agreements relating to six TLDs. Only the .pro registry agreement is not yet complete. Currently, domain name registrations are being accepted in the .biz, .info and .name domains.

[122] ICANN, *Proposed Unsponsored TLD Agreement: Appendix L (.biz)* (last modified Apr. 18, 2001) http://www.icann.org/tlds/agreements/biz/registry-agmt-appl-18apr01.htm. The .info domain is the only domain that will not restrict the class of registrants.

Thus, trademark owners may be precluded from participating in one or more of the new domains. Of course, that does not mean that a mark owner can ignore activity in these domains. The owner of a famous mark may still be able to pursue a cybersquatting claim against a registrant who registers a domain name using the famous mark in bad faith, such as the "IBM" accounting firm.

Perhaps of greater importance to mark owners, the .aero, .coop, and .museum TLDs are sponsored domains, wherein the sponsor, not ICANN, carries out delegated domain policy-formulation.[123] The policy responsibilities include the procedures used to resolve cybersquatting claims. Conversely, the dispute resolution policies of the unsponsored domains, .biz, .info, .name, and .pro will be those adopted by ICANN.

In the context of anti-cybersquatting protection, this policy-formulating freedom, is more illusion than reality.[124] Recently, the sponsored domain's dispute resolution policies were finalized and incorporated in the registry agreements. These agreements expressly require that sponsoring organizations follow UDRP.[125] Policy-making freedom is limited by at least two additional means. First, the trademark dispute resolution policies developed by the sponsor cannot supersede those provided for by ICANN policy.[126] Also, the Base TLD Sponsorship Agreement requires, with limited exceptions, the use of ICANN-accredited registrars to provide registration services for the domain.[127] In turn, the Registration Accreditation Agreement requires that the registrar

[123] ICANN, *Proposed TLD Sponsorship Agreement* (last modified Aug. 29, 2001) http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-29aug01.htm [hereinafter Base Sponsorship Agreement]. Section 2.2 describes the delegation of authority to the domain sponsor.

[124] The .coop TLD already has named WIPO as the DRSP for the .coop domain. Under the agreement, WIPO is to administer the UDRP when resolving disputes. .COOP, *Domain Name Dispute Resolution Policy Summary* (last visited Dec. 27, 2001) http://www.cooperative.org/dispute.asp.

[125] ICANN, *TLD Sponsorship Agreement: Attachment 22–ICANN Baseline Policies* (last modified Dec. 2, 2001) *http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-att22-25aug01.htm* (treating the UDRP as a Consensus Policy to which the sponsor and their registry operator must comply).

[126] ICANN, *Proposed TLD Sponsorship Agreement: Attachment 2(.museum)—Delegated Authority*, Section 6 (last modified Aug. 20, 2001) http://www.icann.org/tlds/agreements//museum/sponsorship-agmt-att2-20aug01.htm. The agreement states that sponsors are delegated the power to develop, "[m]echanisms for resolution of disputes between owners of rights in names (such as trademarks) and registrants that do not *supplant* ICANN's dispute-resolution policies" (emphasis added).

[127] Base Sponsorship Agreement, *supra* note 123, § 3.6.

comply with UDRP.[128] The Base TLD Sponsorship Agreement accepted by the sponsors of the three existing sponsored TLDs is intended to serve as a template for use in future sponsored TLD agreements.

B. Country Code TLDs

The finite limit on the domain names available in the gTLDs not only motivated the creation of new TLDs but also a migration to ccTLDs.[129] Unlike gTLDs, the ccTLDs were established to provide the domain name system with geographic bounds and local control. A ccTLD is identified by a unique two letter abbreviation similar to the state postal abbreviations used in the United States.[130] For example, .au is the country code abbreviation for Australia. Although ccTLDs are created and issued under the auspices of ICANN and its predecessors, each country code administrator has the freedom to create the policies that it deems suitable for the domain. Often, the administrator is a nonprofit organization responsible for creating a central registry for all the domain names registered in the ccTLD, as well as, formulating policy for the domain, including domain name dispute policies.[131] For example, in the United Kingdom the administrator has created a number of second level domains associated with the .uk ccTLD.[132]

The freedom to establish customized dispute resolution procedures has led to a myriad of rules and regulations that vary from one ccTLD to the next.[133] The lack of uniformity places a huge burden on trademark owners seeking to protect their mark. First, they must educate themselves as to their rights in each venue. Second, if the mark owner chooses to pursue a cybersquatter, they must pursue their claim using the laws and procedures of the jurisdiction. The following analysis categorizes the anti-cybersquatting protection of ccTLDs using three

[128] ICANN, *Registrar Accreditation Agreement* (last modified May 17, 2001) http://www.icann.org/registrars/ra-agreement-17may01.htm. Section 3.8 provides that "Registrar shall comply with the Uniform Domain Name Dispute Policy identified on ICANN's website."

[129] *See* WIPO, *WIPO ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes* (Version: June 20, 2001) http://ecommerce.wipo.int/domains/cctlds/bestpractices/bestpractices.html [hereinafter *Best Practices*]; *see also* Nominet.uk *1999 Annual Report* (last visited Apr. 21, 2001) http://www.nic.uk/nominet/about/.report.html. The report describes a 200% increase in domain registrations for the .uk ccTLD between September 1998 and September 1999.

[130] A list of all issued country codes can be found at: *Root Zone Whois Information* (last modified June 20, 2001) http://www.iana.org/cctld/cctld-whois.htm.

[131] *Best Practices*, *supra* note 129.

[132] Second level domains .co, .ltd, .net, .org, .plc, and .sch are also managed under the auspices of Nominet.uk, the domain name administrator for the United Kingdom.

[133] Wood, *supra* note 5.

categories: (1) ccTLDs that apply UDRP or a modified version, (2) ccTLDs that do not follow UDRP but offer locally customized dispute resolution, and (3) ccTLDs that force parties to move right to litigation in order to resolve cybersquatting disputes.[134]

1. ccTLDs Applying UDRP

WIPO provides domain name dispute services for twenty-two ccTLDs.[135] Fifteen of the listed countries, including Romania and Venezuela, apply ICANN's UDRP to resolve disputes between registrants and trademark owners. Two others, Mexico and the Philippines, use a modified version of UDRP. Of course, a ccTLD administrator that has decided to name WIPO as a dispute resolution provider has done so because they understand the importance of providing trademark protection in a commercial forum.[136] The case of .tv, assigned to the country of Tuvalu, provides one clear example. The .tv Corporation, a for-profit corporation, has invested heavily in marketing the advantages of owning a domain name in the .tv domain.[137] The promoters' interests are well served by accepting the international standard of domain name dispute resolution because legitimate businesses understand and respect the intellectual property ground rules applied in the ccTLD. Theoretically, this should lead to increased commercial activity within the domain and an increasing demand for .tv domain names.

2. ccTLDs Offering Customized Arbitration Procedures

A number of countries, including Italy, the United Kingdom, and Denmark, offer customized arbitration procedures. Italy has developed its own arbitration procedure that mirrors the UDRP.[138] The elements of a successful claim in the Italian system are the equivalent to those required under UDRP.[139] However, the Italian procedure allows additional time for each step of the process. Additionally, the Italian Registry requires that

[134] *Id.* Placing ccTLD registries into one of six categories based on their preregistration screening and dispute resolution policies: (1) The UDRP Registry Model, (2) The Interventionist Registry Model, (3) The Home Team Registry Model, (4) The Prophylactic Model, (5) The Disinterested Registry Model, (6) The Not Interested Registry Model.

[135] WIPO, *Domain Name Dispute Service for ccTLDs* (visited Sept. 7, 2001) http://arbiter.wipo.int/domains/cctld/index.html.

[136] *See* Wood, *supra* note 5.

[137] Nick Wingfield, *VeriSign Makes Investment in Company that Registers '.TV' Internet Addresses*, WALL ST. J., Nov. 28, 2000, at B8.

[138] The Naming Authority Italiana, *Domain Name Reassignment Procedure* (visited Dec. 27, 2001) http://www.nic.it/NA/riassegnazione-curr-engl.txt.

[139] *Id.* Rule 8.

the arbitrator be selected from a list of Arbitration Committee Members provided the Italian Naming Authority.[140] There are three reported cases under the arbitration procedure. The complainant, L'Oreal S.A., was successful in two cases. In each case, the disputed domain name, oreal.it and lancome.it, were released by the original assignee prior to the arbitrator rendering a decision.[141]

The United Kingdom recently introduced a new dispute resolution policy that provides for mandatory dispute resolution and compliance with an expert's decision if informal mediation fails.[142] Denmark has established a three person Board of Appeals for Domain Names that has the authority to transfer the rights to a domain name where "it appears without doubt, that the domain name has been registered for use which is not in good faith concerning colliding name and trademark rights."[143] The Danish rules appear to reach cybersquatters who may have decided to buy and hold a trademark but have not yet begun to use the mark; thereby eliminating any questions regarding whether the mark must be "used" in order to establish a claim. The Danish rules do not offer any criteria for a finding that a registrant has not operated in good faith.[144] The Danish procedure is mandatory for all domains registered after February 22, 2000.[145] A Danish court following Danish law and Danish Parliamentary principles must resolve conflicts that cannot be resolved under the arbitration procedure.[146] For example, traditional trademark infringement and dilution claims.

3. ccTLDs Relying on Traditional Legal Remedies

Other ccTLDs refuse to get involved in trademark related domain name disputes and instead have opted to force trademark owners to rely on traditional legal remedies to protect against cybersquatting.[147]

[140] The Naming Authority Italiana, *The Naming Authority Arbitration Committee* (visited Dec. 27, 2001) http://www.nic.it/NA/arbitri/index-engl.html.

[141] *Id.* A third case filed Apr. 24, 2001, also involving the Lancome mark, is described as ongoing.

[142] *See* Nominet.uk *Dispute Resolution Service* (visited Dec. 27, 2001) http://www.nic.uk/ref/drs.html (replacing the previous dispute resolution policy that only subjected parties to nonbinding decisions and only allowed for domain name transfer where the parties agreed or a court so ordered).

[143] D.K. Hostmaster, *Rules for Registration, Administration and Conflict Resolution Regarding Domain Names under the Top Level Domain .dk*, Rule 5 (last modified May 30, 2001) http://www.dk-hostmaster.dk/regel-eng.html.

[144] *Id.*

[145] *Id.* Rule 5.2.

[146] *Id.* Rule 1.5.

[147] The difficulties imposed on mark owners as a result of this approach were discussed in Part II.

Reliance on traditional legal remedies typically results from one of two approaches. First, the administrators of some ccTLDs expressly disavow any interest or duty in dispute resolution. Other ccTLD administrators appear to simply ignore the issue, perhaps intentionally, and fail to address dispute resolution in their policies.

Luxembourg provides an example of a "considered hands-off" approach. Their registry makes it clear that they have considered the intellectual property issues surrounding domain names and have determined that they will not enter into cybersquatting regulation. The Luxembourg registry expressly disavows responsibility for resolving domain name disputes.[148] The Luxembourg rules advise claimants:

> [I]t is the responsibility of the entity wishing afterwards to apply for the same domain name to . . . pursue any litigation which may be necessary against the existing registrant should the applicant believe that he holds a valid title to that name and that the existing registrant has no right to the domain name.[149]

Under Revision 2 of their Registration Agreement, Singapore also employed a considered hands-off approach. The Revision 2 Agreement relied on the registrant's statement that the domain name: (1) does not infringe a trademark registered in Singapore and (2) is not confusingly similar with either a registered trademark, company, or business name in Singapore.[150] Singapore also included an express disavowal of any responsibility for arbitrating domain name disputes.[151] The registration agreement required the registrant to agree to allow Singapore courts to adjudicate disputes concerning the .sg ccTLD should voluntary alternate dispute resolution fail.[152] However, in what may be part of a continued migration to a common international standard for cybersquatting dispute resolution, effective January 1, 2002, all .sg domain names are governed by a new registration agreement that provides UDRP-style domain name dispute resolution.[153]

Other country code registries appear to have adopted a hands-off approach as an intentional strategy by which the country may encourage domain name registrations, regardless of a registrant's proclivity to

[148] DNS-LU, *Domain Name Policy for the National Top Level Domain LU*, Section 9.2 (last modified Nov. 2001) http://www.dns.lu/policy.htm.

[149] *Id.* Section 10.1.

[150] Singapore Network Information Centre, *Domain Name Registration Agreement Revision 02*, Section 6 (visited on Sept. 7, 2001) http://www.nic.net.sg.

[151] *Id.* Section 17.

[152] *Id.* Section 26.

[153] Singapore Network Information Centre, *New Domain Name Registration Agreement*, (visited Dec. 27, 2001) http://www.nic.net.sg.

cybersquat. These registries appear to be encouraging cybersquatting by creating a safe haven for cybersquatters. Tasjikistan has taken just this approach. The .tj registrars advise potential registrants to register quickly before someone else takes the domain name of choice. However, the register does not appear to demand any assurance that the registrant holds any intellectual property rights in the domain name. Further, the site provides no information regarding what, if any, dispute resolution policies are in place. In doing so, they have created a haven for cybersquatters.[154]

4. The Combined Affect of Preregistration Screening and Dispute Resolution Policies

Trademark owners may be best served in closed TLDs that apply strict prescreening requirements before they accept a domain name registration. The ccTLDs that have stringent preregistration screening requirements provide ex ante protection against cybersquatting.[155] The "sunrise" registrations and other pre-startup procedures presently being implemented in the new ICANN authorized TLDs provide an alternative attempt to prevent cybersquatting disputes.[156]

Often, ccTLDs that provide strict preregistration protections do not provide for any type of dispute resolution. For example, the Lebanese Domain Registry will not register a domain name unless the registrant first secures a trademark with the Lebanese Ministry of Commerce and Trade for the *exact* domain name.[157] The strict standards required to register a domain name in the .lb ccTLD insure that only legitimate mark owners are registering domain names.[158] However, the registry rules also advise parties to settle any disputes via "normal legal methods."[159] In this instance, the harm to trademark owners created by the absence of any direct anti-cybersquatting protection is mitigated by the registry's strict preregistration requirements. Another example is the previously mentioned .dk domain where no prescreening occurs, but the

[154] *TJ Network Information Center* (visited Sept. 7, 2001) http://www.nic.tj.

[155] Wood, *supra* note 5 (describing the Prophylactic Registry Model).

[156] ICANN *Proposed Unsponsored TLD Agreement: Appendix J (.biz)—Registry TLD Startup Plan* (last modified May 11, 2001) http://www.icann.org/tlds/agreements/biz/registry-agmt-appj-11may01.htm. Some of these provisions provide trademark owners the ability to record a preemptive claim to a domain name that is identical to their trademark. Other provisions allow a challenge or contest to a domain name application that includes a domain name matching the challenger's trademark.

[157] *Lebanese Domain Name Registry Updated Rules*, Rule 1 (last modified Sept. 22, 1999) http://www.aub.edu.lb/lbdr/lbdr-rules-19990922.html.

[158] *Id.*

[159] *Id.* Rule 11.

cybersquatting arbitration is mandatory.[160] A worst case scenario is created when a ccTLD registry provides no prescreening and no dispute resolution procedure as is done in the .tj ccTLD.

C. Alternate TLDs

Trademark owner's efforts at preventing cybersquatting are further complicated by the increasing popularity of two types of alternate TLDs. The first type, unauthorized TLDs, are accessible on the World Wide Web but are not hosted on ICANN root servers. The second type, pseudo-TLDs, provide the look and feel of a TLD but are not actual TLDs. The former variety poses the greater risk of cybersquatting because they are beyond the reach of ICANN; therefore, dispute resolution procedures, if any, are voluntarily adopted.[161]

1. TLDs Offered on Non-ICANN Root Servers

In addition to their policy responsibility, ICANN is ultimately responsible for the operation of the Domain Name System (DNS) protocol, root servers, and root files that form the foundation of the Internet's global address and domain name infrastructure.[162] The root servers are the computers that organize the hierarchy of domain names. The organization is completed using root files containing each domain name and associated Internet address. The DNS operates smoothly because these elements are properly maintained. Presently, thirteen root servers are operated under contract with ICANN. The primary root server, the A Root Server, is operated in Herndon, VA. The remaining twelve root servers, secondary servers, are located throughout the United States and the world.[163]

The current structure allows the root server operator to control the participants in the DNS. Only TLDs provided in the ICANN root servers are included in the DNS, and standard Internet browser software is configured to work only in the ICANN managed DNS. This creates a de facto checkpoint wherein ICANN may control the TLDs used over the

[160] The Danish Registry requires an electronic or physical signature that is said to represent the registrant's guarantee that the domain name does not infringe the trademark rights of others. However, the Registry does not perform any investigation into the legitimacy of the representation.

[161] Claburn, *supra* note 6.

[162] David Conrad et al., *Root Nameserver Year 2000 Status* (last modified July 15, 1999) http://www.icann.org/committees/dns-root/y2k-statement.htm.

[163] *Id.* (nine additional servers are located in the United States, and one each in England, Japan, and Sweden).

Internet.[164] For example, the seven new ICANN authorized TLDs will all be incorporated into the DNS managed by ICANN.

Alternate root servers also operate over the World Wide Web, but their Web addresses are inaccessible when using a Web browser with a standard configuration.[165] Enter Pacific Root and other members of the Open Root Server Confederation (ORSC). ORSC members offer more than fifty TLDs that work with a separate root system presently used by approximately 5% of the Internet community.[166] The registries that operate in the ORSC roots are free to register domain names without regard to ICANN policies.[167] For example, the .com TLD is not presently available on the Pacific Root server but the .biz TLD has been in use since 1996.[168] In order for a Web searchers' Web browser to recognize domain names in the alternate TLD, the searchers must first reconfigure their computer's DNS servers. The reconfiguration can be accomplished by simply downloading and running a file that automatically changes the computer's DNS server IP addresses.[169]

These unauthorized TLDs create another set of TLDs where the trademark owner must vigilantly monitor for trademark abuses.[170] Of course monitoring is only the first step; the greater challenge for trademark owners is trying to stop cybersquatting in these domains.

The nonexistent dispute resolution policies of these TLDs provide a heightened cause for concern among mark owners.[171] Some unauthorized TLD administrators have expressly disavowed UDRP and ACPA on the grounds that they violate a registrant's due process rights.[172] The administrators have also backed up their talk by failing to provide a dispute resolution procedure by which a trademark owner can challenge

[164] Jerry Berman & Alan B. Davidson, Center for Democracy and Technology, *ICANN: Towards Domain Name Administration in the Public Interest* (Testimony Before the House Committee on Energy and Commerce, Subcommittee on Telecommunications (Feb. 8, 2001)).

[165] Pacific Root, *Update Your Domain Name Service* (visited Sept. 7, 2001) http://www.pacificroot.com/updatedns.shtml.

[166] *Id.*

[167] *Id.*

[168] .BIZ Domain Registry, *About the .BIZ TLD*, (visited Sept. 7, 2001) http://www.biztld.net/aboutbiz.html (offering, among others, registration of unauthorized TLDs .bio, .golf, .kids, and .online to domain name registrants).

[169] *See supra* note 165.

[170] Claburn, *supra* note 6.

[171] *Id.*

[172] The author is unaware of any formal constitutional challenge brought against either. The private contractual agreement between parties subject to UDRP likely precludes such a challenge. Additionally, both UDRP and ACPA provide notice and hearing for the defendant/respondent.

a cybersquatter.[173] Further, the registrars include a policy of nonintervention in domain name disputes unless faced with a court order to transfer or cancel a domain name.[174]

The risk that these unauthorized TLDs create for trademark owners will increase dramatically should they begin to gain broader acceptance.[175] Napster provided a clear example of the strong attraction that a restraint-free Internet model has on broad user-segments.

2. Pseudo TLDs

Pseudo TLDs are not true TLDs, but TLD facsimiles that function as true TLDs when the user's computer is properly configured with the required software or the computer is connected to a cooperating Internet Service Provider (ISP).[176] The pseudo TLD is actually a Third Level Domain (3LD) that targets a popular market segment; for example, .biz, .kids, .travel or .games. As the preceding examples demonstrate, the pseudo TLD may be one that is or will be authorized by ICANN for use as a true TLD. The pseudo TLD provider uses the 3LD as a prefix to its own SLD-TLD combination: for example, Pseudo.com would allow customers to register custom domains such as "user-selected.biz.pseudo. com." The look and feel of a true TLD is created because users need only enter "user-selected.biz" in order to reach the Web site when using a properly configured computer.[177]

Recent entrepreneurial efforts have focused on expanding the functionality and availability of pseudo TLDs. New.net, the most well funded and well organized provider of pseudo TLDs to date, has partnered with leading domestic ISPs to immediately access sixteen million potential users.[178] This potential market may increase the scope

[173] Pacific Root Domain Registration (visited Sept. 7, 2001) http://www.pacificroot.com/register.shtml#newtlds>.

[174] *Id.* ("[O]nly those entities that are found to be infringing upon the trademark rights of others, by due process and in a court of law, will be forced to relinquish their domains and only then by court order.").

[175] Claburn, *supra* note 6. Steve Dougherty of Earthlink, the second largest domestic ISP, in reference to Earthlink making available the unauthorized TLDs via the Earthlink ISP, is quoted as saying that, "If this proves to be valuable it's something we'd consider."

[176] *New Domain Extensions that Bypass ICANN*, HitBox.com (visited Sept. 7, 2001) http://www.hitbox.com/cgi-bin/page.cgi?building/archive/domains_04132001. An ISP, also referred to as an On-line Service Provider (OSP), is a company that operates a server to provide Internet access, e-mail, chat room, Web page hosting and various other services for their customers.

[177] *Id.* As one example, the configuration software for pseudo TLD provider New.net is a 50Kbyte file that can be downloaded from the New.net Web site. Once downloaded, the user simply installs the plug-in that allows the user to view New.net TLDs.

[178] McCarthy, *supra* note 7.

of a trademark owner's search for cybersquatters but the news is not all bad. Pseudo TLDs are extensions of the ICANN authorized TLDs. Thus, this technological slight of hand will likely not strip trademark owners of their ability to effectively pursue cybersquatters.

New.net has left no doubt regarding the applicable dispute policy for their pseudo TLDs. New.net's dispute policy so closely mimics the UDRP that they have posted on their Web site a copy of the UDRP highlighted to reflect the differences between the two.[179] The majority of the revisions go to properly identifying the parties to the agreement.

So long as the pseudo TLD is an extension of an ICANN approved TLD, it is also unlikely that cybersquatters using pseudo TLDs could avoid the UDRP even where the pseudo TLD administrator has opted not to require registrants to agree to comply with UDRP.[180] The registrant may not be directly reachable under UDRP if their registration agreement does not require them to accept mandatory participation in UDRP. However, the pseudo TLD provider did accept UDRP as part of their registration agreement for the SLD that provides the basis of the cybersquatter's domain name.[181] Ultimately, pseudo TLD providers are contractually bound to comply with UDRP to address all cybersquatting claims brought as a result of their customers' activities.

The preceding description highlights a broader negative possibility facing any registrant who chooses to operate a site within the pseudo TLD. Their registration and domain are held subject to the underlying rights the provider has in the pseudo TLD. For example, the Web site operator at acme.biz.new.net will lose their Web address should the New.net business model fail and the firm abandon its business.[182] It appears that the registrant's remedies would be limited because they are not in privity with the registry that provided New.net with the underlying SLD on which the registrant's domain is based.

D. Multilingual TLDs

There is yet another set of TLDs worthy of trademark owners' consideration. Multilingual domain names, those that use non-English

[179] New.net, *Dispute Policy* (visited Sept. 7, 2001) http://www.new.net/policies_dispute_old.tp.

[180] An ICANN-accredited registrar of an unsponsored TLD would be in violation of their registry agreement if they took this approach.

[181] Jason M. Osborn, Note, *Effective and Complimentary Solutions to Domain Name Disputes: ICANN's Uniform Domain Name Dispute Resolution Policy and the Federal Anticybersquatting Consumer Protection Act of 1999*, 76 NOTRE DAME L. REV. 209, 210 (2000). UDRP is incorporated by reference into the registration agreements of all accredited registrars.

[182] This is not a far-fetched possibility given the current state of the dot-com world.

characters, are presently in the testbed phase at a number of registries.[183] Multilingual TLDs (mlTLDs)have the ability to reach a potentially huge and untapped overseas market. The sheer size of the market is enough to make a trademark owner take notice. Additionally, the mlTLDs are not being tested at the behest of ICANN. Instead, leading registries have taken a pro-active approach and begun to testbed the concept in response to global demand for non-English Web access.[184]

The mlTLD concept is an attempt to allow Internet access to billions of non-English speaking people around the globe. The mlTLDs will create any number of foreign language alternates to the existing English language domain name format.[185] Existing testbeds are formatted to add mlTLDs as SLDs to the existing .com, .net, and .org TLDs.[186] Suggested character sets include Chinese and other East Asian characters, Arabic, Hebrew, Sanskrit, and Cyrillic.

The actual risk posed by cybersquatters in the mlTLDs will depend upon whether registrants are required to comply with UDRP.[187] Registries are continuing to take a hands off approach and have offered little guidance.[188] VeriSign explains their position as follows:

> As a registry, VeriSign Global Registry Services is not involved in the intellectual property disputes surrounding domain name registration. The VeriSign Global Registry Services will advise registrars that, during the testbed, registrars should consider deleting any multilingual second level domain name registration upon receipt of a formal (written) objection from any legitimate source received by that registrar for a limited period of time to be specified by the particular registrar. In addition, the VeriSign Global Registry Services is aware that accredited registrars may continue to use the Uniform Domain Name Dispute Resolution Policy (UDRP) to resolve disputes, including those involving multilingual domain names.[189]

[183] *See* ICANN, *ICANN Melbourne Meeting Topic: Introduction of Internationalized Domain Names* (last modified Feb. 27, 2001) http://www.icann.org/melbourne/idn-topic.htm; *see also* ICANN, *ICANN Montevideo Meeting Topic: Internationalized Domain Names* (last modified Aug. 28, 2001) http://www.icann.org/montevideo/idn-topic.htm.

[184] David J. Stewart et al., *Foreign Character Domain Names and New Top Level Domains Create More Trademark Issues* (visited Sept. 7, 2001) http://www.gigalaw.com/articles/stewart-2000-11-p2.html.

[185] VeriSign Global Registry Services, *General Information Paper on Multilingual Domain Name Resolution* (Apr. 3, 2001) http://www.verisign-grs.com/multilingual/Gen_Info_Paper.pdf.

[186] The TLD is not translated to foreign characters.

[187] Doug Isenberg, *Multilingual Domain Names May Create New Trademark Disputes* (visited Sept. 7, 2001) http://www.gigalaw.com/articles/isenberg-2000-11c-p1.html.

[188] VeriSign Global Registry Services, Multilingual DNS FAQs (visited Sept. 7, 2001) http://www.verisign-grs.com/multilingual/genfaq.html#19.

[189] *Id.*

Although registries appear to be distancing themselves from the cybersquatting issues, the attitude taken by registrars accepting applications for domain names in the mlTLD testbeds is more important to determining how cybersquatting policies may develop. On its site, Register.com includes the following regarding registration restrictions and trademark rights in mlTLDs:

> There are no restrictions on registering a domain name in another character set. As long as the name is determined to be available, it is eligible to be registered. Please keep in mind, however, that register.com makes no representations as to whether or not domain names searched for through our site infringe upon or violate any trademark or intellectual property rights; it is your responsibility to determine the legality of the domain name. Please note that at this time, the central registry is supporting the registration of international character domain names in an experimental testbed. International character domain names are not yet and may not be functional on the Internet and cannot be used for Web hosting, Email Services or any other DNS related activity.[190]

The site offers no hint at what, if any, dispute resolution procedure will be applied to cybersquatting claims related to mlTLDs. Instead, registrars appear to avoid the issue and fall back on the experimental and, as of yet, nonfunctional nature of the testbeds to give themselves the latitude to change the terms of domain name registrations after the fact. The preliminary nature of the mlTLDs will likely allow the registrars to later develop well-defined dispute resolution procedures should they choose. Additionally, the registries that are leading the mlTLD testbed development historically have worked closely with the Department of Commerce, ICANN, and commercial interests. Therefore it is unlikely that they will disregard ICANN's demonstrated interest in preventing cybersquatting even where contractually permissible.[191]

V. WHAT'S A TRADEMARK OWNER TO DO?

The explosive growth of TLDs, the disparate treatment of cybersquatters among the TLDs, and uncertainty regarding the rules of proposed TLDs have created numerous strategic issues for trademark owners. Issues relating solely to cybersquatting include analysis of: (1) the scope of the trademark owner's search for cybersquatters, (2) the

[190] Registers.com, *Registering International Character Domain Names FAQs* (visited Sept. 7, 2001) http://ml.register.com/faq/multilingual-faq.cgi?1|2389698193|CO6309#5.

[191] VeriSign, *Network Solutions Registry Multilingual Domain Name Position Paper* (Aug. 24, 2000) http://www.verisign-grs.com/multilingual/positionpaper.pdf. On page 1, VeriSign makes it clear that they plan to synchronize their efforts with ICANN's policies.

available dispute resolution procedures for a given TLD, and (3) the likelihood of success of the mark owner's claim given the specific facts and the dispute resolution procedures available for a particular TLD.

Regarding the scope of the cybersquatter search, a number of intellectual property service providers offer comprehensive domain name protection services that include on-line searches of the world's TLDs. Net Searchers, a division of the Virtual Internet plc, offers what it calls "Domain Name Searching, Monitoring and Recovery Services."[192] The company identifies cybersquatters for clients, paying particular attention to TLDs where infringement is easy.[193] Virtual Internet can also streamline customer billing by consolidating the client's registration and maintenance fees from the various TLDs into a single statement. This year, Thomson & Thomson introduced a Domain Registrant search tool.[194] The new tool, designed to be used directly by the firm's customers, can be used to identify cybersquatters in TLDs around the globe.[195] Trademark owners are well advised to seriously consider these and similar options in order to protect a valuable trademark. This is particularly true in light of the minimal barriers to entry typically encountered by cybersquatters.

As mentioned previously, cybersquatter identification is only the first step to trademark protection. The trademark owner must next determine what remedies are available in the TLD. A plaintiff seeking monetary damages can rely on ACPA provided the U.S. courts have personal jurisdiction over the defendant.[196] In the ICANN authorized gTLDs, the trademark owner can rely on UDRP to transfer or cancel the offending domain name so long as the elements of cybersquatting claim exist.[197] Where neither ACPA nor UDRP are available, other options will have to be evaluated.[198]

[192] Net Searchers, *Services* (visited Dec. 29, 2001) http://www.netsearchers.com/us/services.asp; *see also* Karen Chan, *Domain-Name Firms Suffering Double as Customers, Investors Both Disappear*, WALL. ST. J., WSJ.com, Mar. 6, 2001.

[193] *Id.*

[194] Thomson & Thomson, *Thomson & Thomson Adds Three More Registrars to Domain Registrant Search on SAEGIS* (visited Sept. 8, 2001) http://ttdomino.thomson-thomson.com/www/saegisdocs.nsf/0EA3C68C1D980A9A862568E7005F3F1F/02CDA1C786EB9D4585256A7800537494?OpenDocument.

[195] *Id.*

[196] GILSON & LALONDE, *supra* note 3, at 19.

[197] UDRP, *supra* note 34, § 4(a) ((1) the domain name is identical or confusingly similar to the trademark; (2) the domain name holder has no legitimate interest in the domain name; and (3) the domain name has been registered and used in bad faith).

[198] Sandra Edleman, *Cybersquatting Claims Take Center Stage*, 18 COMPUTER & INTERNET L. 1, 5 (2001) (reminding readers not to forget traditional Lanham Act remedies).

In order to create a series of favorable decisions, trademark owners are encouraged to selectively pursue cybersquatters. A set of decisions involving the owner's mark or marks all favoring the mark owner may lend significant support to the owner's later claims. A favorable track record may assist even where a dispute is arbitrated.[199] The previously mentioned case involving Yahoo! clearly demonstrates the value created by a series of favorable decisions.[200] In the Yahoo! decision, the three panelists used evidence of thirteen previous UDRP decisions in which Yahoo! prevailed to support their decision to transfer the disputed domain names to Yahoo!.[201]

The trademark owner must also consider which domain names to protect and in which TLDs to protect them. For example, mark owners may want to register domain names that are common misspellings of their mark.[202] The cost of domain name registration and maintenance fees must also be considered when evaluating the TLD jurisdictions and specific domain names to be protected. A trademark owner may bring a common UDRP action against a cybersquatter for violations in multiple TLDs.[203] Of course, an overriding concern for trademark owners is the proper policing of their mark's use in order to maintain their rights in the mark.

Lastly, trademark owners are encouraged to continue to focus on developing Internet policy. For example, the successes and failures of "sunrise" registrations and other pre-registration procedures in the new ICANN authorized domains likely foreshadow the trademark protection policies of future newly authorized TLDs.[204]

VI. CONCLUSION

Technological changes may some day make domain names and associated cybersquatting issues obsolete. However, today, trademark

[199] Interview with Jay Monahan, Associate General Counsel, Intellectual Property, eBay, Inc. in Berkeley, CA (Mar. 10, 2001).

[200] Yahoo!, Inc. v. Yahoo Computer Servs., WIPO Case No. DPH2001-001.

[201] *Id.* The decisions involved domain names in a number of ccTLDs including the Indian, Mexican, Australian, and Uruguayan ccTLDs.

[202] *See* Nat'l Arbitration Forum Decision, Mellon Bank, N.A. v. HS Trading Comp., NAF FA0095951 (transferring melonbank.com to complainant Mellon Bank).

[203] Time Inc., v. Chip Cooper, WIPO Case No. D2000-1342 (transferring lifemagazine.com, lifemagazine.org, and lifemagazine.net).

[204] ICANN *Advisory—Advisory Concerning Unqualified .info "Sunrise" Registrations* (last modified Aug. 14, 2001) http://www.icann.org/announcements/icann-pr14aug01.htm (stating that the variety of alternate pre-registration procedures used as "proof of concept" approaches by the new domains will serve as a means of finding the optimum approach for ex ante protection against domain abuse in new TLDs).

owners are in what seems to be an increasingly frenetic race to secure or otherwise protect domain names in an ever-expanding Internet. Given the existing structure of the Domain Name System a proactive approach is the only advisable course of action.

New technology has often been the catalyst for substantial societal change. More often than not these changes require some degree of adaptation by the legal system.[205] Digital data storage and reproduction and computer software are two recent technological changes that have changed both society and the law.[206] Often in the rush to distinguish the technological and societal future from the recent past, these developments are not placed in a proper historical context. This results in demands, by some, for a wholesale shift in legal rights and duties. However, so long as the policy rationale supporting the existing balance of legal rights and duties is still desired, a more thoughtful approach must be taken. Ultimately, unless the underlying policy rationale has suddenly become defective, the goal of any legal adjustments should be to maintain the original balance of legal duties. Parties crying that "the Internet wants to be free" do not appear to appreciate this fact.[207]

The law has long protected the source-identifying abilities of trademarks. Both consumers and mark owners rely on these source-identifying qualities. Cybersquatting threatened to destroy the historical legal balance created and endorsed by the legislature and judiciary. The ACPA and the UDRP were legal responses developed to protect that balance. If there are significant societal benefits to modifying that balance then the benefits should be clearly articulated and the effects carefully evaluated so that the appropriate legal response can be determined. Legal analysis founded on the theory that technology provides us the capability to violate property owners' rights and therefore that we should be allowed to do so is ipso facto logic that may be endorsed by those "behind the looking glass" but is unsupportable in the real world.

However, those who cry foul regarding trademark protection on the Internet raise some legitimate concerns. The multijurisdictional reach and single commercial space created by the Internet doesn't fit the worldview under which trademark protection developed with its focus on

[205] USPTO, White Paper, *Automated Financial or Data Processing Methods (Business Methods)*, July 19, 2000 (reviewing the historical development of Patent and Trademark Office procedures in response to pioneering technologies).

[206] *Id.* (tracing the history of business method patents from the nineteenth century to the present). Of course, the effects on law and society of rapid advances in biotechnology are only beginning to be felt.

[207] Richard Louv, *The Future's Edge*, SAN DIEGO UNION-TRIBUNE, Dec. 10, 2000, at A3.

distinct geographic boundaries and separate channels of trade.[208] Further, some argue that a domain name that is used to provide an Internet address is not being used as a trademark.[209] This begs the question of why should the holder of famous mark be able to secure rights across all the Internet? Is this acceptable simply because the limited number of TLDs eliminate the geographic and business sector distinctions that existed pre-Internet? Does such a monopoly truly benefit society and is it supported by the policy rationale behind trademark protection?

One way to mitigate the problem is to add both artificial geographic boundaries and more specific channels of trade on the Internet in an attempt create a commercial space more akin to the commercial space in existence when trademark law originally developed.[210] The continued TLD expansion provides increased opportunities to develop these artificial boundaries. The ccTLDs have not uniformly adopted such an approach, but a strong argument can be made that trademarks in domain names in the ccTLDs should be administered in the same fashion that they are administered within the countries' jurisdictions. Such an approach would prevent a trademark holder from usurping a senior user in that geography. Of course without further geographic subdivisions within the TLDs, the preceding suggestion would only provide partial relief. For example, in the United States, the rights to a particular name in one jurisdiction, State *A*, will overlap the rights to the same mark in State *B* unless either the .us ccTLD is subdivided into smaller geographic regions or new TLDs dedicated to a specific state and country are created. Thus, in order to replicate the pre-Internet trademark landscape, there is a need for TLDs focused on more narrow geography.[211]

Additionally, the gTLDs could be administered to restrict registrants to those who participate in a specific business sector. Thus, if Ford Motor Company is not in the aerospace field then it should not be entitled to protect against the use of a domain name containing "ford" within the .aero domain. Some newly authorized TLDs offer what appears to be the start of an effort to create business-sector specific space on the Internet.

But how far should efforts go to increase the number of more narrowly focused TLDs? Eventually, such efforts reach a point of

[208] Barrata, *supra* note 2.

[209] McCarthy, *supra* note 27.

[210] See the proposed naming conventions in the .museum TLD. Musedoma, *Frequently Asked Questions—Naming Policies and Conventions* http://www.nic.museum/faqnam.html (last modified Nov. 8, 2001) (reserving all SLDs in the .museum domain for use as generic labels describing the registrant museum's discipline or geographic location).

[211] *Id.*

diminishing returns, as well as eliminating the simplicity and ease of use provided by the original gTLDs. It doesn't appear that we have come close to reaching that point yet, but when the point of diminishing returns is reached can the Domain Name System continue to support trademark rights in anything close to a traditional manner? This is the challenge that ICANN, Internet users, and other members of the Internet community face as the number of TLDs continues to expand.

The preceding suggestions are premised on the continued development of ICANN as a central policy making body for the Internet. Although there are risks in allowing a single body to be the ultimate decision-maker on Internet issues, it can be successful if ICANN insures that the voices of both commercial and noncommercial interests are heard while Internet policy continues to develop.[212]

These suggestions provide only a partial solution. But, they present one approach to developing an international standard of trademark protection for the expanding Internet universe. The suggestions are based on an interest in maintaining the balance of legal rights and duties historically protected under trademark law. The alternative, Internet chaos, likely will benefit no one.

[212] Berman & Davidson, *supra* note 164.