MITCHELL | HAMLINE School of Law

Cybaris®

Volume 4 | Issue 2 Article 2

2013

Reverse Domain Name Hijacking and the Uniform Domain Name Dispute Resolution Policy: Systematic Weaknesses, Strategies for the Respondent, and Proposed Policy Reforms

Catherine A. Schultz

Courtney A. Hofflander

REVERSE DOMAIN NAME HIJACKING AND THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY: SYSTEMATIC WEAKNESSES, STRATEGIES FOR THE RESPONDENT, AND PROPOSED POLICY REFORMS

CATHERINE A. SHULTZ[†] AND COURTNEY A. HOFFLANDER[‡]

[†] Catherine A. Shultz is a 2009 graduate of Notre Dame Law School and an associate at Kinney & Lange, P.A. Catherine is a U.S.P.T.O. registered patent attorney, and her practice includes all aspects of intellectual property law, including prosecution and litigation of patents, trademarks and copyrights.

[‡] Courtney A. Hofflander is a second-year law student at William Mitchell College of Law, J.D. Candidate May 2014. The author would like to thank the Cybaris® staff for their effort and dedication.

I. INTRODUCTION

A trademark owner engages in Reverse Domain Name Hijacking[1] (RDNH) by filing a frivolous Domain Name Hijacking[2] (DNH) claim in an attempt to improperly capture a domain name from a legitimate domain name registrant. The Uniform Domain Name Dispute Resolution Policy[3] and attendant Rules of Procedure[4] (collectively, the UDRP) were designed to resolve and remedy DNH, and generally perform those functions well. The UDRP does not, however, sufficiently discourage RDNH or provide adequate remedies for a legitimate domain name registrant responding to a frivolous claim.[5] Given the importance of Internet commerce, the hardship cast by RDNH, and the complex challenges of keeping up with new technology and law, it is critical to explore RDNH in order to develop and implement sound solutions to systematic weak points in the UDRP that lead to these abusive claims.

II. THE CONNECTION BETWEEN DOMAIN NAME REGISTRATION AND TRADEMARK LAW

A. The Function of Domain Names and Trademarks

The purpose of a domain name is to serve as an easily memorable path to an Internet resource.[6] A domain name is a substitute for the unique Internet Protocol (IP) address assigned to the source computer of a website, which ultimately enables Internet users to access the online resource.[7] A domain name incorporates alpha characters that can serve as a commercial advertisement or an "indication of source"[8] for a product or service offered on the website.[9] Thus, distinct from its

---

[1] *See infra* Part II.C.

[2] *See infra* Part II.C.

[3] *Uniform Domain Name Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. (Oct. 24, 1999) [hereinafter *UDRP Policy*], http://www.icann.org/en/help/dndr/udrp/policy.

[4] *Rules for Uniform Domain Name Dispute Resolution*, INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS (Oct. 30, 2009) [hereinafter *Rules of UDRP Procedure*], http://www.icann.org/en/help/dndr/udrp/rules.

[5] Andrew Allemann, *UDRP panelists don't do their job deciding reverse domain name hijacking*, DOMAIN NAME WIRE, (Aug. 20, 2012), http://domainnamewire.com/2012/08/20/arbitration-reverse-domain-name-hijacking/.

[6] *See Archives*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. [hereinafter *ICANN Archives*], http://archive.icann.org/tr/english.html (last visited Feb. 16, 2013).

[7] *Id.*

[8] In the trademark sense of "indication of source." *See infra* note 9.

[9] Wal-Mart Stores, Inc. v. wallmartcanadasucks.com, Case No. D2000-1104, 2000 WL 35641872 (WIPO Arbitration & Mediation Ctr. Nov. 23, 2000) (Perritt, Jr., Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1104.html.

technical function of routing data, a domain name has the capacity to act like a trademark.

In general, the "role that a designation must play to become a 'trademark' is to identify the source of one seller's goods and distinguish that source from other sources."[10] Trademark infringement occurs when an unauthorized party uses a mark in commerce in a way that is "likely to cause confusion" as to the source or origin of the product or service.[11] There is not an international registry,[12] or a standard set of international rights and remedies for trademark owners.[13] Acquiring trademark protection in one country does not give rise to reciprocal rights in any other country.

To foster effective participation in today's significant online marketplace, a trademark owner might seek to use all or part of its trademark as its second-level domain name,[14] thereby enabling consumers to easily locate its website. This may lead to significant financial gains, considering it is predicted that sales influenced by the Internet "will reach $1.409 trillion, and that direct [Internet] sales and those influenced by the Internet will account for 53% of all retail sales in 2014."[15] Using the trademark in its domain name may also increase the likelihood that

---

[10] 1 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 3:1, (4th ed. 2013); *e.g.*, Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189, 198 (1985) (stating trademarks deserve protection to preserve "the ability of consumers to distinguish among competing producers.").

[11] 15 U.S.C.A. § 1114(1)(a) (West 2012).

[12] Todd W. Krieger, Note, *Internet Domain Names and Trademarks: Strategies for Protecting Brand Names in Cyberspace*, 32 SUFFOLK U. L. REV. 47, 72 (1998) ("[T]here is no international centralized trademark registry . . . .").

[13] *See Madrid Protocol*, U.S. PATENT & TRADEMARK OFFICE, http://www.uspto.gov/trademarks/law/madrid/index.jsp (last updated Jan. 1, 2013) (the Madrid Protocol "is a *filing* treaty and not a substantive harmonization treaty. . . . [I]t remains the right of each country or contracting party designated for protection to determine whether or not protection for a mark may be granted. Once the trademark office in a designated country grants protection, the mark is protected in that country just as if that office had registered it.")*;* *see also FAQS: Trademark Clearing House*, ICANN NEW GENERIC TOP-LEVEL DOMAINS (May 6, 2013), http://newgtlds.icann.org/en/about/trademark-clearinghouse/faqs ("The Clearinghouse is a repository of data only, and trademarks from many jurisdictions can coexist in the Clearinghouse. Clearinghouse processes are designed to confirm the validity of data, not to make determinations on the substance or scope of rights held by a particular party.").

[14] A second-level domain is a domain that is directly below a top-level domain. Information Technology Services, *Understanding How Domain Names Work*, THE UNIVERSITY OF TEXAS AT AUSTIN (Nov. 16, 2012), http://www.utexas.edu/its/help/utnic/848.

[15] *Take Your Business to the Next Level*, VERISIGN, http://www.verisigninc.com/en_US/information-for-small-business/index.xhtml (last visited May 23, 2013).

Internet search engines will return to the trademark owner's website when a search for the trademark is performed. This could lead to higher traffic and cause the trademark owner to realize a greater return on its investment in maintaining a web presence than if it had used a different domain name. Thus, because a significant portion of today's economic activity takes place online, having a website that consumers can easily find is an important part of staying competitive for large and small businesses alike, and is facilitated by incorporating the company's trademark into its domain name.

Domain name registration occurs on a first-come, first-served basis.[16] This poses a problem for a trademark owner that wants to use a domain name that contains all or part of its trademark if the domain name has already been registered by another individual or entity. Not only will the trademark owner have to choose a different and possibly less easily found domain name, but the trademark owner will likely want to exclude the prior domain name registrant from continuing to use the domain name in an effort to retain brand control and prevent expropriation of its mark. When a third party uses a domain name with all or part of another's trademark, a consumer might be confused as to the owner of the website and unwittingly associate the website with the trademark owner. Another reason for a trademark owner's desire to prevent a third party from using a domain name with all or part of the trademark is that there is a risk of losing rights in the mark itself through genericism if unauthorized use of the mark goes unchecked.[17]

In all, the ability of a domain name to give information to a consumer about the source of the goods or services offered on the site overlaps with the essential purpose of a trademark—to identify the source of goods or services.[18] As a result, trademark owners often want to use and protect their marks in cyberspace to prevent confusion and to maintain existing trademark rights, particularly because the Internet has such a heavy influence on sales. With the existence of over 196.3

[16] Jessica Litman, *The DNS Wars: Trademarks and the Internet Domain Name System*, 4 J. SMALL & EMERGING BUS. L. 149, 151 (2000).

[17] 15 U.S.C.A. § 1064(3) (West 2012). "The primary significance of the registered mark to the relevant public . . . shall be the test for determining whether the registered mark has become the generic name of goods or services on or in connection with which it has been used." *Id.* Most importantly, a registered mark may be canceled at any time on grounds that it has become generic. *Id.*; *see* Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189, 194 (1985) (citing Abercrombie & Fitch Co. v. Hunting World, Inc., 537 F.2d 4, 9 (2d Cir. 1976) ("A generic term is one that refers . . . to the genus of which the particular product is a species.").

[18] 1 MCCARTHY, *supra* note 10, § 2.3.

million registered domain names,[19] and a wave of new generic top-level domains approaching,[20] it is unsurprising that practitioners increasingly confront domain name issues.

B. Trademark Law Policy in Domain Name Registration

Trademark owners are afforded protection in the context of domain names because trademarks and domain names can both indicate source. However, this protection is limited. Federal courts[21] and other dispute resolution forums only recognize a trademark owner's interest in preventing a third party from registering and using the owner's mark in a domain name if the third party has registered and used the domain name in bad faith.[22] A trademark owner cannot exclude a third party from using a domain name solely by virtue of the domain name containing the trademark; a trademark owner does not automatically have rights in the domain name.[23] Rather, a domain name registrant can, in some circumstances, legitimately obtain rights in a domain name that contains all or part of another's trademark by registering it for as little as $7.85.[24]

Trademark protection as applied to domain names is, to the extent it exists, consistent with basic trademark law principles: reducing consumer transaction costs,[25] "prevent[ing] the expropriation of protected marks in cyberspace[,] and . . . abat[ing] the consumer confusion resulting therefrom."[26] Preventing a third party from registering a domain name that includes a trademark in bad faith often results in the actual trademark owner's website being easier to locate, resulting in both time and money savings for the consumer. It also reduces the likelihood that a consumer will visit and/or buy from an illegitimate third-party website as a

[19] Press Release, Verisign, Internet Grows to More than 196 Million domain Names in Second Quarter of 2010, (Sept. 21, 2010) (on file with the SEC), *available at* http://www.sec.gov/Archives/edgar/data/1014473/000119312510213453/dex991.htm.

[20] *New gTLD Program Timeline*, INTERNET CORP. FOR ASSIGNED NAMES & NOS., http://newgtlds.icann.org/en/about/program/timeline (last visited May 23, 2013) (e.g., example.genericTLD).

[21] The "court" as used in this paper refers to the federal court system in the United States.

[22] *See infra* Part II.C.

[23] *See infra* Part III.B.

[24] *See Verisign Announces Increase in .com/.net Domain Name Fees*, VERISIGN (July 14, 2011), https://investor.verisign.com/releaseDetail.cfm?ReleaseID=591560.

[25] Providing protection, albeit limited, to domain names reduces time and financial costs associated with a consumer's Internet search for the desired source. *See* Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 163–64 (1995) (holding that one basic objective of trademark law is "reduc[ing] the customer's costs of shopping and making purchasing decisions").

[26] Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 271 (4th Cir. 2001) (discussing the Anticybersquatting Consumer Protection Act).

result of being confused as to the source. These traditional policy goals of trademark law are preserved in the domain name context by allowing a trademark owner to attempt to protect its trademark rights by bringing a DNH claim in court[27] or under the UDRP when a confusingly similar domain name is registered in bad faith by a third party.

C. Differentiating Domain Name Hijacking and Reverse Domain Name Hijacking

A DNH claim is narrowly targeted at remedying improper domain name registrations.[28] It is not intended to resolve disputes among competing trademark claims to a domain name.[29] A domain name registration is improper when a third party registers a domain name that includes a trademark owner's mark in bad faith, without the authorization or consent of the trademark owner.[30] Typically, the third party then tries to sell the domain name to the trademark owner at an inflated price.[31] This practice is commonly referred to as "cybersquatting."

Generally, DNH "can create havoc for a company Web site, resulting in lost time, money, and business."[32] It is estimated that DNH costs trademark owners one billion dollars each year as a result of "diverted Internet traffic, the loss of consumer trust[,] and expenses related to combating the issue."[33] DNH has negatively impacted many companies and institutions including Nike, Exodus,

---

[27] S. REP. NO. 106-140, at 4 (1999), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-106srpt140/pdf/CRPT-106srpt140.pdf (stating Congress's goals in enacting the ACPA were to promote online commerce, protect American consumers and businesses, and prevent cybersquatting by prohibiting "the bad-faith and abusive registration of distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks").

[28] *See Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. (Oct. 24 1999), http://archive.icann.org/en/udrp/udrp-second-staff-report-24oct99.htm.

[29] *Id.*

[30] *See UDRP Policy*, *supra* note 3.

[31] *See* Chris Irvine, *Top Ten Most Expensive Domain Names*, THE TELEGRAPH (Mar. 10, 2010), http://www.telegraph.co.uk/technology/news/7412544/Top-10-most-expensive-domain-names.html (suggesting that sought-after domain names can sell for large sums of money).

[32] *Trademarks on the Internet*, CORP. COUNS. Q., at 2 (Aug. 2011) ("These cyberthieves can create havoc for a company Web site, resulting in lost time, money, and business from the time the company actually discovers that its site has been hijacked to when the Web site is finally under the control of the original owner.").

[33] Erik Siemers, *Nike aims to squash cybersquatters*, PORTLAND BUS. J. (Mar. 14, 2010, 9:00 PM), http://www.bizjournals.com/portland/stories/2010/03/15/story4.html?b=1268625600%5E3021521.

and Emory University.[34] The elements and consequences of DNH vary depending on whether the claim is brought as an administrative proceeding or in court,[35] and the particular venue selected within those two categories.

Some trademark owners have developed strategies to attempt to wrongfully capture a sought-after domain name under current DNH laws and policies through a transfer order[36] issued by the court[37] or administrative body, even when it is clear that the prior domain name registrant legitimately obtained rights in the domain name. Essentially, a trademark owner brings, or simply threatens to bring, a frivolous[38] cybersquatting claim.[39] This practice is known as Reverse Domain Name Hijacking (RDNH). Typically, the domain name is identical or similar to a reverse domain name hijacker's trademark, though this is not always the case. In making a RDNH determination, the court[40] or administrative body[41] often considers the complainant's ability to prove the basic DNH factors. The presiding

[34] *See Trademarks on the Internet*, *supra* note 32, at 2 (stating cybersquatting victims are often harmed by lost sales and/or damaged reputations).

[35] *UDRP Policy*, *supra* note 3, ¶ 4(k).

[36] Rather than threatening or bringing a RDNH claim, the complainant instead could buy the domain name from the registrant or simply register and use a different domain name.

[37] Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 621 (4th Cir. 2003) (stating courts have interpreted § 1114 (2)(D)(v) to mean that the ACPA "authorizes a domain name owner to seek recovery or restoration of its domain name when a trademark owner has overstepped its authority in causing the domain name to be suspended, disabled, or transferred.").

[38] Complainant knows or should know that the claim is not likely to succeed on the merits. BLACK'S LAW DICTIONARY (9th ed. 2009) (defining frivolous as "Lacking a legal basis or legal merit; not serious; not reasonably purposeful.").

[39] *See supra* Part II.B–C.

[40] 15 U.S.C.A. § 1114(2)(D)(iv)–(v) (West 2012) ("(iv) If a registrar, registry, or other registration authority takes an action described under clause (ii) based on a knowing and material misrepresentation by any other person that a domain name is identical to, confusingly similar to, or dilutive of a mark, the person making the knowing and material misrepresentation shall be liable for any damages, including costs and attorney's fees, incurred by the domain name registrant as a result of such action. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant. (v) A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii)(II) may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this chapter. The court may grant injunctive relief to the domain name registrant, including the reactivation of the domain name or transfer of the domain name to the domain name registrant.").

[41] *Rules of UDRP Procedure*, *supra* note 4, ¶ 3(b)(ix)(1)–(3) (stating a service provider considers whether the domain name contains the trademark of the complainant, when the domain name was registered, whether the registrant has a legitimate interest in the domain name, and how the domain name has been used since registration).

body might also consider whether counsel represents the trademark owner,[42] actions of the trademark owner before and during the DNH claim,[43] and other factors deemed relevant to the particular case.

For example, in the case of *Mama May I, LLC v. Phillips*, Jessica Perkins and James Perkins (the Perkins) wanted to acquire the domain name mamamayi.com.[44] However, a legitimate domain name registrant had previously registered the domain name in February of 2009.[45] After unsuccessful and frustrating negotiations with the domain name owner, the Perkins decided to take a different approach.[46] They applied for and were granted a U.S. trademark registration for MAMA MAY I, and immediately thereafter filed a UDRP complaint for transfer of the domain name.[47] The Perkins filed the complaint despite the fact that the trademark application for MAMA MAY I claimed a first-use date that post-dated the domain name registration, which indicates that the UDRP claim was frivolous because a domain name cannot be registered in bad faith against a nonexistent trademark.[48] Therefore, the panel rightly found the Perkins' claim as an attempt at RDNH.[49]

Though it is hard to determine the exact frequency of RDNH as many instances do not make it to a forum for resolution (the registrant simply transfers the domain upon a threat or demand of the trademark owner), it occurs more than desired and can be "equally as onerous" as cybersquatting due to the time and resources required for resolution.[50]

---

[42] Windsor Fashions, Inc. v. Windsor Software Corp., Case No. D2002-0839, 2002 WL 31681426 (WIPO Arbitration & Mediation Ctr. Nov. 14, 2002) (Foster, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0839.html.

[43] Viking Office Prods., Inc. v. Natasha Flaherty, Claim No. FA1104001383534 (Nat'l Arbitration Forum May 31, 2011), http://domains.adrforum.com/domains/decisions/1383534.htm.

[44] Mama May I, LLC v. Phillips, Claim No. FA1205001445335 (Nat'l Arbitration Forum July 2, 2012), http://domains.adrforum.com/domains/decisions/1445335.htm.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] Milton Muller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, CONVERGENCE CTR., http://dcc.syr.edu/PDF/roughjustice.pdf (last visited May 23, 2013).

III. INTERNATIONAL STRUCTURE OF DOMAIN NAME DISPUTE RESOLUTION

A. International Regulatory Body: Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit, private organization "dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes." [51] ICANN achieves these objectives by coordinating the Domain Name System (DNS), IP addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) top-level domain name system management, and root server system management functions.[52] ICANN provides a structure through which registrants and third parties can resolve domain name disputes. According to ICANN, "most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name."[53] Pursuant to this statement, ICANN developed a uniform domain name dispute resolution structure to facilitate the administrative resolution of trademark-based domain name disputes worldwide.[54]

B. The Foundation of ICANN's Domain Name Dispute Resolution Structure: The Uniform Domain Name Dispute Resolution Policy and Rules of Procedure

Since October 24, 1999, ICANN has promulgated the Uniform Domain Name Dispute Resolution Policy to resolve domain name disputes for all .com, .net, and .org domain names. The UDRP incorporates a second document by reference that is integral to the functioning of the uniform system, the Rules of Uniform Domain Name Dispute Resolution Policy.[55] When a domain name is registered with any ICANN-accredited Registrar, the registrant confirms that registering the domain name "will not infringe upon or otherwise violate the rights of any third party"[56]

---

[51] *ICANN Archives*, *supra* note 6.

[52] *Welcome*, INTERNET CORP. FOR ASSIGNED NAMES & NOS., http://www.icann.org/en/about/welcome (last visited May 23, 2013).

[53] *Uniform Domain Name Dispute Resolution Policy—General Information*, INTERNET CORP. FOR ASSIGNED NAMES & NOS., http://www.icann.org/en/help/dndr/udrp (last visited May 23, 2013).

[54] *See infra* Part II.B.

[55] *UDRP Policy*, *supra* note 3.

[56] *UDRP Policy*, *supra* note 3, ¶ 2.

and agrees to comply with terms of the UDRP in the event that a third party asserts a claim arising from an alleged abusive registration.[57]

The UDRP also sets forth the terms and conditions that an administrative dispute resolution service provider (service provider) will use to govern a domain name dispute.[58] A service provider may impose supplemental rules on the parties.[59] An ICANN proceeding costs about $1,500,[60] and the trademark owner submitting the claim is responsible for paying the associated fees.[61]

Engaging in dispute resolution under the UDRP is "mandatory" to the extent that a registrant's domain name is subject to a proceeding initiated by a trademark owner.[62] However, if the trademark owner or domain name registrant is unsatisfied with the outcome[63] or if the domain name registrant did not participate in the UDRP proceeding,[64] he or she may file suit for judicial relief under the Anticybersquatting Consumer Protection Act (ACPA),[65] assuming the ACPA[66] and other traditional jurisdictional requirements are satisfied.[67] The finding of the

[57] *UDRP Policy*, *supra* note 3, ¶ 4(a).

[58] *List of Approved Dispute Resolution Service Providers*, INTERNET CORP. FOR ASSIGNED NAMES & NOS., http://www.icann.org/en/help/dndr/udrp/providers (last visited May 23, 2013) (listing the four ICANN-approved dispute resolution providers).

[59] *Rules of UDRP Procedure*, *supra* note 4, ¶ 1.

[60] *Fee Schedule*, NAT'L ARBITRATION FORUM (Aug. 1, 2008), http://www.adrforum.com/users/naf/resources/2008FeeSchedule-FinalPrint1.pdf; *Schedule of Fees under the UDRP*, WIPO (Dec. 1, 2002), http://www.wipo.int/amc/en/domains/fees/index.html.

[61] *Rules of UDRP Procedure*, *supra* note 4, ¶ 19(a) (noting the cost varies according to the number of panelists. Respondent is responsible for the additional costs of a three-person panel created upon his/her request).

[62] *UDRP Policy*, *supra* note 3, ¶ 4.

[63] *See* Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 626 (4th Cir. 2003) (noting that a WIPO panel decision "is relevant only to serve as the reason for [registrant's] . . . bringing an action under § 1114(2)(D)(v) . . . .").

[64] If the domain name registrant fails to respond to the UDRP compliant, it may lead to the uncontested loss of the domain name. *Rules of UDRP Procedure*, *supra* note 4, ¶ 5(e) ("If a Respondent does not submit a response, in the absence of exceptional circumstances, the Panel shall decide the dispute based upon the complaint.").

[65] 15 U.S.C.A. § 1125(c)(1) (West 2012).

[66] *UDRP Policy*, *supra* note 3, ¶ 4 (k) (providing that a trademark owner can assert a cybersquatting claim in a court of competent jurisdiction, and "[i]n general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database").

[67] Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745, 751 (E.D. Va. 2001) ("[I]t would not be appropriate to 'compel' participation in UDRP proceedings under § 4 as a prerequisite to litigation because UDRP complainants, as strangers to the registration agreement, are under no obligation to avail themselves of the UDRP.").

UDRP panel has no preclusive effect,[68] and the court does not give the panel's finding any deference.[69] Further, a trademark owner can avoid the UDRP entirely and instead, under the ACPA, choose to only assert a DNH claim against the domain name registrant in court.

To prevail on a DNH claim under the UDRP,[70] the complainant must show that (1) it has trademark rights in the mark, (2) the respondent's domain name is confusingly similar to the complainant's trademark,[71] (3) the respondent does not have rights or a legitimate interest in the domain name,[72] and (4) the respondent's domain name was registered and is being used in bad faith.[73]

In regard to the bad faith element, the UDRP includes a non-exhaustive list of factors: (1) circumstances suggesting the respondent's registration was primarily for the purpose of selling or transferring the domain name, (2) the respondent engaging in a pattern of conduct to prevent the trademark owner from reflecting the mark in a domain name, (3) the respondent registering the domain name primarily for the purpose to disrupt business of the complainant, and (4) the respondent using the domain name to intentionally attract users for commercial

---

[68] *See, e.g.*, Storey v. Cello Holdings, L.L.C., 347 F.3d 370, 381 (2d Cir. 2003) (holding that a UDRP action has no *res judicata* effect; the UDRP was structured to allow "two bites at the apple").

[69] Hawes v. Network Solutions, Inc., 337 F.3d 377, 386 (4th Cir. 2003) ("[A]n action brought under § 1114(2)(D)(v) on the heels of an administrative proceeding under [the UDRP] . . . is independent of, and involves neither appellate-like review of nor deference to, the underlying proceeding.").

[70] *UDRP Policy*, *supra* note 3, ¶ 4(a) (stating that "[i]n the administrative proceeding, the complainant must prove that each of these three elements are present," which assumes that (1) in the list that follows is met).

[71] Sumner v. Urvan, Case No. D2000-0596, 2000 WL 33939204 (WIPO Arbitration & Mediation Ctr. July 24, 2000) (Christie, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0596.html (holding "the Uniform Policy is not limited to a 'registered' mark; an unregistered, or common law, mark is sufficient for the purposes of paragraph 4(a)(i)").

[72] Volvo Trademark Holding AB v. e-motordealer Ltd., Case No D2002-0036, 2008 WL 4892129 (WIPO Arbitration & Mediation Ctr. Mar. 22, 2002) (Blackshaw, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-0036.html (holding that a registrant can legitimately use another's trademark in its domain name according to "the wording of paragraph 4(c)(iii) of the Policy, only in a *non-confusing and non-diverting manner*.") (emphasis in original).

[73] Recordati S.P.A. v. Domain Name Clearing Company, Case No. D2000-0194 (WIPO Arbitration & Mediation Ctr. July 21, 2000), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0194.html ("'[U]se in bad faith' in subsection 4(a)(iii) does not refer to 'use in commerce' in the trademark sense of use but refers in the broad sense to a pattern of conduct respecting the registered domain name in dispute.").

gain by creating a likelihood of confusion with complainant's mark.[74] Notably, to satisfy the bad faith element, a complainant must show that the domain name was registered in bad faith and then used in bad faith. Proof of one of these subparts alone is insufficient to constitute bad faith under the UDRP.[75]

The panel considers a different set of factors in determining whether the respondent has a legitimate interest in the domain name. The UDRP indicates that the respondent might show its legitimate interest by providing evidence that it made a bona fide offer of goods or services in connection with the domain name prior to receiving notice of the dispute; that the registrant is commonly known by the domain name; or that its use is legitimate, noncommercial, or constitutes fair use.[76] Per the UDRP, this is a nonexclusive list of situations that suggest a registrant's legitimate interest in the domain name at issue.[77]

To avoid a transfer order by a UDRP panel, a domain name registrant can simply negate one or more *prima facie* elements of a DNH claim in its response.[78] In addition, the domain name registrant may request an RDNH finding, if applicable, and provide the panel with relevant evidence to support its request. If the panel finds that the claim was filed in an attempt at RDNH, the panel shall declare in its published decision that the claim was asserted in "bad faith and constitutes an abuse of the administrative proceeding."[79]

IV. THE PURPOSE OF THE UDRP AND ITS WEAKNESSES

A. The UDRP and a Measure of Its Success for Domain Name Dispute Resolution

The UDRP is intended to be a shield against cybersquatting, not a sword through which a trademark owner can improperly acquire a domain name. ICANN adopted the URDP to facilitate the efficient and inexpensive resolution of "abusive [domain name] registrations."[80] The UDRP provides an alternative for trademark owners who would otherwise be coerced into negotiating with a domain name hijacker, filing an expensive lawsuit, or simply allowing the domain name hijacker to continue use[81] of a domain name that clearly infringes the

[74] *See UDRP Policy*, *supra* note 3, ¶ 4(b).
[75] *UDRP Policy*, *supra* note 3, ¶ 4(b).
[76] *UDRP Policy*, *supra* note 3, ¶ 4(c).
[77] *UDRP Policy*, *supra* note 3, ¶ 4.
[78] *See Rules of UDRP Procedure*, *supra* note 4, ¶ 5(b)(i).
[79] *Rules of UDRP Procedure*, *supra* note 4, ¶ 15(e).
[80] *Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. (Oct. 24 1999), http://archive.icann.org/en/udrp/udrp-second-staff-report-24oct99.htm.
[81] This is an undesired result according to basic trademark policy. *See supra* Part II.B.

owner's mark.[82] In the context of traditional cybersquatting, the UDRP has performed well as a reliable dispute resolution mechanism within the international domain name system.[83]

A major advantage of the UDRP is that it costs less than litigation. Filing a lawsuit presents a significant expense that many trademark owners cannot afford. In 2006, average trademark litigation costs "ranged from $250,000 to $650,000, depending on the size of the lawsuit."[84] One way that costs are reduced under the UDRP is the mandatory administrative proceeding provision,[85] which eliminates jurisdictional complexities of traditional litigation and allows for the proceeding to simply focus on the domain name dispute instead of venue, choice of law, and other issues that make litigation costly and representation by counsel almost a necessity. Plus, the UDRP eliminates traditional litigation costs related to traveling to appear in a particular forum because UDRP proceedings are administered solely through written submissions of the parties.[86]

Similarly, the UDRP enables disputants to avoid the historically lengthy time span of a formal lawsuit. For example, the time it takes a trademark infringement lawsuit to reach trial is often "longer than one year – more likely closer to two years, and possibly three."[87] In contrast, the typical UDRP proceeding is completed within sixty days.[88] Notably, the UDRP also conserves judicial

---

[82] As trademark owners are responsible for policing their marks to prevent genericism and loss of rights. The UDRP is an effective tool to assist with this in the context of infringing domain names.

[83] *See* MARGIE MILAM, FINAL GNSO ISSUE REPORT ON THE CURRENT STATE OF THE UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY 14 (2011), *available at* http://gnso.icann.org/en/node/27051 ("[T]he UDRP has proven to be a flexible and fair dispute resolution system."). However, even within the UDRP system there is inequity between trademark owners and the cybersquatting community because a trademark owner faces thousands of dollars in UDRP fees compared to a cybersquatter who is not required to respond to a UDRP claim and only incurs the negligible cost of registering the domain name.

[84] Leah C. Grinvald, *Resolving the IP Disconnect for Small Businesses*, 95 MARQ. L. REV. 1491, 1529 (2012).

[85] *UDRP Policy*, *supra* note 3, ¶ 4.

[86] *See Rules of UDRP Procedure*, *supra* note 4, ¶ 13 (providing that an in-person hearing may only be held in exceptional circumstance).

[87] Julie A. Katz, *The Long and Winding Road: Successful Trademark Litigation in the United States*, INTELLECTUAL ASSET MGMT. MAGAZINE 45 (Apr. 2009), *available at* http://www.iam-magazine.com/issues/Article.ashx?g=c4552580-e53b-4247-9008-b1bb6b7c27eb.

[88] *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*, WIPO [hereinafter *WIPO Guide to UDRP Policy*], http://www.wipo.int/amc/en/domains/guide/index.html (last visited May 23, 2013) ("The Administrative Procedure normally should be completed within 60 days of the date the WIPO Center receives the Complaint.").

resources by keeping disputes over clearly abusive registrations out of the court system.[89] Since its inception, the UDRP has been used to resolve over 30,000 domain name disputes,[90] and without ICANN-approved service providers more of these disputes would have end up in the court system.

Another strength of the UDRP is that it allows for bodies that are well versed in domain name and trademark policy to resolve the disputes. Other types of intellectual property have similar bodies that specialize in resolving disputes pertaining to the subject matter in controversy. For example, the Federal Circuit Court of Appeals has exclusive jurisdiction over patent appeals.[91] In the context of the UDRP, a de facto two-step quality regulation process of the service providers naturally leads to more experienced panelists, and arguably more consistent results within the system. First, ICANN assumes an active role in examining potential service providers. In its selection process, ICANN emphasizes the importance of the potential service provider having a positive track record of handling disputes, a demonstrable level of understanding of the UDRP, and a proven ability to recruit highly qualified panelists.[92] Second, the service providers select panelists for their individual rosters based on the applicant's trademark or bench experience.[93] Service providers then continue to educate their panelists on an annual basis on topics that specifically address developments in the procedure and substance of domain name dispute resolution.[94] The dual-track vetting process sets a sound foundation for fair outcomes under the UDRP. A final strength of the UDRP related to quality

[89] Thomas C. Folsom, *Missing the Mark in Cyberspace: Misapplying Trademark Law to Invisible and Attenuated Uses*, 33 RUTGERS COMPUTER & TECH. L.J. 137, 249 n.157 (2007) ("[T]he high volume of domain names resolved under the private UDRP system, compared to the far smaller number under the public court system appears to be a significant private diversion away from . . . the public judicial system.").

[90] *Uniform Dispute Resolution Policy*, GENERIC NAMES SUPPORTING ORGANIZATION, INTERNET CORP. FOR ASSIGNED NAMES & NOS., http://gnso.icann.org/en/council/policy/udrp (last visited May 23, 2013).

[91] 28 U.S.C.A. § 1295(a)(1) (West 2012) (stating the Federal Circuit Court of Appeals has exclusive jurisdiction "of an appeal from a final decision . . . in any civil action arising under . . . any Act of Congress relating to patents").

[92] *See List of Approved Dispute Resolution Providers*, INTERNET CORP. FOR APPROVED NAMES & NOS., http://www.icann.org/en/help/dndr/udrp/providers (last visited May 23, 2013).

[93] *WIPO Guide to UDRP Policy*, *supra* note 88 (stating advantages of the UDRP include having "decision-makers [that] are experts in such areas as international trademark law, domain name issues, electronic commerce, the Internet and dispute resolution").

[94] *See* MILAM, *supra* note 83, at 48 (noting that WIPO holds annual Workshops and Panelists Meetings).

control is ICANN's requirement that all UDRP decisions be published, which allows for public comment and maintains transparency.[95]

The generally recognized consistency of the UDRP system has led to it serving as a model for several ccTLD registries' dispute resolution polices, such as .cn and .hk.[96] Yet, even with its success at providing an efficient, economical, and effective forum for cybersquatting claims, some trademark owners have developed techniques to manipulate the system and attempt to wrongfully deprive a legitimate registrant of a domain name (e.g., engage in RDNH). Acknowledging that the UDRP has many strengths, it also has a variety of weaknesses, as discussed below, which allow for trademark owners to abuse the domain name dispute structure and give rise to the need for UDRP reform.

B. The UDRP and Its Susceptibility to RDNH

While the UDRP certainly has advantages over existing alternatives for resolving domain name disputes, it also has a number of limitations and inadequacies that can lead to frivolous DNH complaints against legitimate domain name registrants.[97] The problem of RDNH was anticipated by the ICANN Board even before the UDRP was adopted, and it was suggested during the drafting phase that "[t]he dispute policy should seek to define and minimize reverse domain name hijacking."[98] The UDRP does not incorporate sufficient incentives for a legitimate domain name registrant to advocate for a RDNH finding, or maintain a sufficient level of risk to deter a potential reverse domain name hijacker from asserting a frivolous claim, unlike traditional litigation. Ultimately, these and other structural weaknesses of the UDRP lead to the suboptimal resolution of some RDNH claims.

---

[95] *UDRP Policy*, *supra* note 3, ¶ 4(j).

[96] *See* MILAM, *supra* note 83, at 9.

[97] Muller, *supra* note 50 (stating the UDRP "was supposed to be aimed at the most egregious types of cybersquatting, leaving other disputes to the courts").

[98] *See Resolution Approved by the Board, Santiago Meeting*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. (Aug. 26, 1999), http://archive.icann.org/en/meetings/santiago/santiago-resolutions.htm#anchor16725 (requesting measures designed to minimize RDNH); *see also Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES & NOS. (Sept. 29, 1999) [hereinafter *Staff Report*], http://archive.icann.org/en/udrp/staff-report-29sept99.htm (responding to ICANN Board's request to minimize RDNH by incorporating Rule of Procedure ¶ 15(e) definition of RDNH, Rule of Procedure ¶ 2(a) notice requirement, UDRP ¶ 4(a) clarification complainant's burden, and UDRP ¶ 4(k) provision for a longer time for a domain-name holder to seek out court review).

1. Advocating for RDNH: More Trouble Than It Is Worth

An overriding systematic weakness of the UDRP is that a legitimate domain name registrant simply lacks sufficient incentive to spend time and resources to lobby the presiding panel for a RDNH finding. There is no potential for a legitimate domain name registrant to recover a monetary award from a RDNH finding under the UDRP. According to the UDRP, RDNH is an "abuse of the administrative proceeding," which does not carry any official penalty beyond the mere declaration that the complaint was brought in bad faith.[99] Further, while a legitimate domain name registrant can advocate for a RDNH finding, a panel can also find RDNH *sua sponte*, making it unnecessary for the registrant to raise the issue or provide factual support in order for the panel to find RDNH.[100] Therefore, a legitimate domain name registrant might decide to forgo the extra effort required to proffer evidence of RDNH and instead focus on negating one or more of the *prima facie* elements to ensure the domain name is not transferred.

It is also possible that *pro se* registrants, who amount to over seventy percent of all UDRP respondents,[101] are intimidated by the administrative proceeding. These respondents might lack the sophistication necessary to identify and appreciate the opportunity to call the panel's attention to RDNH. And while a RDNH finding might initially sound attractive to some legitimate domain name registrants as retribution for the attempted hijacking, upon further reflection, an unrepresented registrant is probably more interested in returning to its normal course of business than advocating for a RDNH and then using the negative "hijacker" label to publically shame the reverse domain name hijacker. The opportunity cost associated with advocating for RDNH in the UDRP process, including the additional time and effort to provide support for a RDNH finding as distinct from simply negating the *prima facie* elements of the complaint and utilizing the finding thereafter, might simply be too great. Thus, a RDNH finding is an underutilized tool in the battle against cybersquatting.

---

[99] *Rules of UDRP Procedure*, *supra* note 4, ¶ 15(e).

[100] Though not officially required, many panels have declined to find RDNH stating in their decisions that the registrant did not provide enough evidence relating to RDNH. *See* Max Mara Fashion Group, S.r.l. v. Ashantiplc Ltd., Case No. FA1208001458069 (Nat'l Arbitration Forum Oct. 4, 2012), http://domains.adrforum.com/domains/decisions/1458069.htm; Atlanta Network Technologies, Inc. v. ANT.COM LIMITED, Case No. FA0903001253155, 2009 WL 1454399 (Nat'l Arbitration Forum May 11, 2009) (Tatham, Banks, Pfeuffer, Arb. Panel), *available at* http://domains.adrforum.com/domains/decisions/1253155.htm.

[101] *See* MILAM, *supra* note 83, at 15 (noting that "[q]uestionnaire responses also reveal that in a large percentage of cases, respondents are not represented by counsel (approximately 86% for NAF, 80% for the Asian Domain Name Dispute Resolution Centre, and 70% for the Czech Arbitration Court)").

2. Absence of Meaningful Deterrents to Frivolous Claims Under the UDRP

Apart from the UDRP lacking an incentive for a legitimate domain name registrant to advocate for a RDNH finding, the UDRP is missing an important deterrent to prevent a potential reverse domain name hijacker from filing a frivolous claim in the first place. It is clear that the UDRP does not allow for a panel to levy a financial penalty against the complainant upon a finding of RDNH.[102] The full extent of remedies under the UDRP is cancellation or transfer of the domain name.[103] Yet, neither of these outcomes will deter a reverse domain name hijacker from asserting a frivolous claim because the hijacking party does not originally possess the domain name, and it lacks a legitimate reason to object to the domain name's use at the outset. Nonetheless, even in the event that the presiding panel does find RDNH, the most the potential domain name hijacker can lose is its $1,500[104] investment in administrative filing fees, which is a much smaller sum to forego than that of traditional litigation.

There are more significant risks associated with RDNH in traditional litigation than under the UDRP. One reason for this is that the reverse domain name hijacker is less likely to face a *pro se* respondent by filing in court,[105] and the respondent's counsel is better positioned to assert a RDNH claim because of his or her legal education and experience. By filing in court, the reverse domain name hijacker is also more likely to be confronted with the issue of RDNH because the ACPA, which governs court proceedings but does not apply to the UDRP, provides monetary damages as a consequence of RDNH in some circumstances.[106] The prospect of monetary damages under the ACPA serves as a strong incentive for a legitimate domain name registrant to raise RDNH in court, which is absent under the UDRP.

Finally, filing a traditional lawsuit over a domain name could present more of a risk for the reverse domain name hijacker than a dispute filed under the UDRP because the outcome might be less predictable. A judge may be amenable to traditional trademark arguments, such as nominative fair use [107] and

---

[102] *See UDRP Policy*, *supra* note 3, ¶ 4(i).

[103] *See id.*

[104] *Fee Schedule*, *supra* note 60.

[105] *See* Marissa C.M. Doran, Note, *Lawsuits as Information: Prisons, Courts, and A Troika Model of Petition Harms*, 122 YALE L.J. 1024, 1043 n.87 (2013) (indicating *pro se* representation rate is around ten percent across the federal docket).

[106] S*ee* 15 U.S.C.A. § 1114(2)(D)(iv)–(v) (West 2012).

[107] There is a strong argument that fair use should not be incorporated into the UDRP at all because it is outside the scope for the UDRP, which is to provide a remedy in extreme

incontestability, whereas the UDRP does not allow a panel to address these doctrines.[108] By filing in court, the reverse domain name hijacker also risks liability and other consequences arising from counterclaims that are available in court but are outside the scope of the UDRP—such as unfair competition, fraud, and cancellation of its trademark.[109]

3. Unaltered Availability of Independent Judicial Resolution Following a UDRP Proceeding

The overall domain name dispute resolution structure, including both the UDRP and judicial forums, can be construed as advantageous to a reverse domain name hijacker that first files under the UDRP. If the reverse domain name hijacker loses the administrative proceeding, it may still file a claim in a court of mutual jurisdiction.[110] This structure specifically benefits a well-funded reverse domain name hijacker that might take advantage of going to court to get a second opinion[111] after losing under the UDRP. Notably, many RDNH targets do not have the resources to file a claim in court following an unfavorable panel decision. In practice, the dual option structure, providing for the resolution of domain name disputes under the UDRP or in court, exists mainly for the reverse domain name hijacker and not the legitimate domain name registrant.[112] The UDRP, which is intended to provide a fair and accessible method of domain name

---

cybersquatting cases, not to function as global law regulating freedom of expression. *See UDRP Policy*, *supra* note 3, ¶ 4(c)(iii) (addressing briefly the fair use doctrine).

[108] *See UDRP Policy*, *supra* note 3, ¶ 4(i).

[109] David E. Sorkin, *Judicial Review of ICANN Domain Name Dispute Decisions*, 18 SANTA CLARA COMPUTER & HIGH TECH. L.J. 35, 47 (2001) ("A legal action that challenges a UDRP decision therefore does so only incidentally to the legal claims that the action involves, claims potentially involving trademark and unfair competition law, contract law, fraud, conversion, privacy and personality rights, free speech, due process, public policy, and other matters related to the parties' overarching dispute. The scope of UDRP proceedings, on the other hand, is extremely narrow, encompassing only the three elements set forth in the policy (identicality/similarity to a trademark, lack of legitimate interests, and bad faith registration and use). While a UDRP panel also has discretion to consider other matters, it is unusual for panels to journey far beyond the UDRP and general principles of trademark law.") (citations omitted).

[110] *Rules of UDRP Procedure*, *supra* note 4, ¶ 3(b)(xiii).

[111] Dluhous v. Strasberg, 321 F.3d 365, 366 (3d Cir. 2003) (declining to accord the panel's finding any deference because the UDRP is an administrative proceeding).

[112] Victoria Holstein-Childress, *Lex Cyberus: The UDRP as a Gatekeeper to Judicial Resolution of Competing Rights to Domain Names*, 109 PENN ST. L. REV. 565, 587 (2004) ("Collectively, . . . complainants . . . prevail in the overwhelming majority of UDRP cases, without significant risk that an aggrieved domain name holder will be sufficiently motivated or able to overcome the hurdles to judicial resolution of their dispute posed by the exceedingly short filing period and prospect of costly litigation.").

dispute resolution across the board,[113] does not provide sufficient safeguards to legitimate domain name registrants from reverse domain name hijackers that seek to abuse the system and take advantage of unequal access to facets of the domain name dispute resolution structure.

4. Potential Access to Information Differentials Between the Parties

A reverse domain name hijacker with significant financial backing can exploit an access to information differential between the parties, and can potentially craft a bias in the proceeding based on a more nuanced understanding of the domain name dispute resolution landscape.[114] If a reverse domain name hijacker elects to file under the UDRP in an attempt to improperly capture a domain name, it might rely on statistical data to make a strategic decision about which particular ICANN-approved service provider to choose when initiating the dispute,[115] whether to request a one- or three-person panel, which panelists to nominate to sit on the three person panel,[116] and whether it is advantageous to consolidate claims, among other important decisions. The reverse domain name hijacker may accumulate such information over months or even years, rely on personal experience within the system, and/or hire outside consultants that specialize in

[113] Patrick D. Kelley, *Emerging Patterns in Arbitration Under the Uniform Domain-Name Dispute-Resolution Policy*, 17 BERKELEY TECH. L.J. 181, 182 (2002) ("Some commentators maintain that the UDRP has exceeded expectations, by providing a quick method for fairly resolving domain name disputes at a relatively low cost.").

[114] America West Airlines, Gerber Products Company, The Hoover Company, Seiko Corporation, Wells Fargo & Company, Xerox Corporation, the International Olympic Committee and the United States Olympic Committee each received domain name transfers through domain name dispute arbitration. *List of Proceedings Under Uniform Domain Name Dispute Resolution Policy*, INTERNET CORP. FOR NAMES & NOS., http://archive.icann.org/en/udrp/proceedings-list.htm (last visited May 23, 2013).

[115] In 2001, UDRP complainants won 82.2% of the time with WIPO and 82.9% of the time with the National Arbitration Forum (NAF), compared to 63.4% of the time with the third major provider at that time, eResolutions. Following the release of a 2001 study detailing forum shopping grounded in provider bias under the UDRP, the least complainant friendly provider, eResolutions, lost its remaining market share and ceased providing UDRP dispute resolution services. Michael Geist, *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, 6 (Aug. 2001), *available at* http://www.udrpinfo.com/resc/fair.pdf.

[116] Service providers are required to publically maintain a record of the basic qualifications of each panelist. *Rules of UDRP Procedure*, *supra* note 4, ¶ 6(a); *see, e.g.*, *Qualified Dispute Resolution Panelists*, NAT'L ARBITRATION FORUM, http://domains.adrforum.com/panel.aspx (last visited May 23, 2013). The availability of additional, up-to-date data on panelists maintained by third parties seems to have declined since the initial period after the adoption of the UDRP when there might have been more attention on the UDRP in general. *See, e.g.*, *UDRP Panelists,* UDRPINFO.COM, http://www.udrpinfo.com/panl.php#data (last visited May 23, 2013) (noting that information on panelists after 2002 is not available).

URDP proceedings.[117] The opportunity for a respondent to aggregate similar information and come to a comparable degree of understanding is significantly constrained by the fact that the UDRP affords a domain name registrant a mere twenty days to prepare and submit a response.[118]

Ultimately, though the UDRP provides fast and inexpensive domain name dispute resolution, some of its provisions have led to a number of undesirable consequences.[119] Some speculate that RDNH has increased because of the "simplified process provided by the UDRP."[120] For a reverse domain name hijacker, a UDRP proceeding is a quick and low-risk alternative to filing a frivolous lawsuit or negotiating with the legitimate registrant to acquire a domain name.

V. STRATEGY RECOMMENDATIONS FOR LEGITIMATE DOMAIN NAME REGISTRANTS CONFRONTED WITH A DNH CLAIM UNDER THE UDRP

Reverse domain name hijackers will continue to exploit the limitations of the UDRP and initiate claims that amount to RDNH until sufficient disincentives are put into place to stop the abusive practice.[121] In the meantime, there are several ways that a domain name registrant can resist an erroneous domain name transfer and encourage a RDNH finding, thereby discouraging the overreach of a reverse domain name hijacker to the extent it is possible under the current UDRP.

A. Prior to the Initiation of a UDRP Proceeding

At the most basic level, it is essential for the domain name registrant to keep the entire situation related to its initial registration and subsequent contact with a potential reverse domain name hijacker well documented. If the potential complainant contacts the legitimate domain name registrant prior to commencing a UDRP proceeding, the legitimate registrant should put the potential complainant

---

[117] *CitizenHawk Maintains its Preeminence in UDRP Filings*, YAHOO! FINANCE (Jan. 7, 2013, 8:00 AM), http://finance.yahoo.com/news/citizenhawk-maintains-preeminence-udrp-filings-130000269.html (stating CitizenHawk uses "a team of domain name recovery experts" to manage UDRP disputes on behalf of trademark owners, and past clients include Orbitz, Brooks Brothers, and FreeCreditReport.com).

[118] *Rules of UDRP Procedure*, *supra* note 4, ¶ 5(a).

[119] Pamela Segal, *Attempts to Solve the UDRP's Trademark Holder Bias: A Problem that Remains Unsolved Despite the Introduction of New Top Level Domain Names*, 3 CARDOZO ONLINE J. CONFLICT RESOL. 1, 13 (2001) (stating the UDRP has become "a weapon that makes it easier for trademark holders to take domain names away from those who have registered them").

[120] Wayde Brooks, *Wrestling Over the World Wide Web: ICANN's Uniform Dispute Resolution Policy for Domain Name Disputes*, 22 HAMLINE J. PUB. L. & POL'Y 297, 309 (2001).

[121] *See infra* Part V.II.

on express notice of facts that point to the weaknesses of any potential UDRP complaint. Several RDNH findings cite such notice as a reason for the finding of RDNH.[122] The domain name registrant should also inform the potential complainant that any further attempts to prosecute the matter would be abusive and constitute RDNH.[123]

The legitimate domain name registrant should be wary of a potential reverse domain name hijacker's offer to buy the domain, especially at a price higher than the amount the legitimate registrant paid to originally acquire it. If a UDRP claim is filed after an offer to buy the domain name at an inflated price, these facts should be brought to the attention of the panel. The fact that the complainant was willing to pay more for the domain name than it would cost to register an alternative domain name might indicate the domain name's value to the complainant and suggest that the UDRP filing is a last-ditch effort to capture it after negotiations with the legitimate domain name registrant failed. Under such circumstances, a legitimate domain name registrant should seriously consider whether the claim amounts to RDNH when writing its response. Bearing on this decision is the fact that some panels interpret prior negotiations to sell the domain name to the reverse domain name hijacker, particularly for an arbitrarily high price, as an indication of the legitimate registrant's bad faith, thus weakening the prospect of a RDNH finding.[124]

B. Tactics for a Respondent After Initiation of a UDRP Proceeding

If the reverse domain name hijacker files a complaint with an ICANN service provider under the UDRP, the legitimate domain name registrant can take a number of steps to encourage a RDNH finding. The fact that a respondent, or legitimate domain name registrant, prevails is not in itself sufficient for a RDNH finding. Therefore, the legitimate domain name registrant should start by specifically asking the panel to find RDNH under Rule 15(e).[125] The burden of

[122] *See*, *e.g.*, Koninklijke KPN N.V. v. Telepathy Inc., Case No. D2001-0217, 2001 WL 1700829 (WIPO Arbitration & Mediation Ctr. May 7, 2001) (Gielen, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0217.html; Wave59 Techns. Int'l Inc. v. VolumeDomains.com, Claim No. FA1110001413550 (Nat'l Arbitration Forum Nov. 30, 2011), http://domains.adrforum.com/domains/decisions/1413550.htm.

[123] Goldline International, Inc v. Gold Line, Case No. D2000-1151, 2001 WL 36141920 (WIPO Arbitration & Mediation Ctr. Jan. 4, 2001) (Bernstein & Limbury, Arbs.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1151.html.

[124] *See* Lockheed Martin Corp. v. Domain Park Ltd., Claim No. FA0708001059748, 2007 WL 2776570 (Nat'l Arbitration Forum Sept. 18, 2007) (Peppard, Arb.), *available at* http://domains.adrforum.com/domains/decisions/1059748.htm.

[125] *Rules of UDRP Procedure*, *supra* note 4, ¶ 15(e) ("If after considering the submissions the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse

proving RDNH is generally on the respondent,[126] so the request should be substantiated with relevant evidence.[127] For example, the respondent can show that the claim was clearly frivolous by evidencing that the complainant knew or should have known that it lacked the relevant trademark rights or knew of the respondent's legitimate interest in the domain name at the time of filing.[128] It is also persuasive if the registrant has any evidence showing the complainant knew of the domain name registration for a long period of time before filing the complaint. A frequent basis for a RDNH finding is that the registrant can demonstrate that it registered the domain name before complainant gained any trademark rights.[129]

The number of panelists and the tendencies of the specific panelists selected to preside over the dispute may be determinative in the ultimate findings of the panel, as some individual panelists appear to be uncomfortable with making a RDNH even under the proper circumstances. In *Shoe Land Group LLC v. Development, Services c/o Telepathy Inc*., the domain name was registered seven years prior to the trademark registration.[130] The complainant had originally

---

Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding.").

[126] Default by a respondent does not necessarily prevent a finding of RDNH. Panels may enter a RDNH finding on their own initiative, namely when the complainant intentionally omitted material evidence in attempt to mislead the panel. *See* Goway Travel Ltd. v. Tourism Australia, Case No. D2006-0344, 2006 WL 3949420 (WIPO Arbitration & Mediation Ctr. June 6, 2006) (Bernstein, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0344.html.

[127] *See WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition ("WIPO Overview 2.0")*, WIPO, ¶ 14.7 (2011) [hereinafter *WIPO Panel Views on UDRP Questions*], http://www.wipo.int/amc/en/domains/search/overview/#417.

[128] *See, e.g.*, Futureworld Consultancy Ltd. v. Online Advice, Case No. D2003-0297, 2003 WL 22000608 (WIPO Arbitration & Mediation Ctr. July 18, 2003) (Anand, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0297.html.

[129] *See, e.g.*, Live Earth, LLC v. Designers for Change Ltd., Claim No. FA0908001280449, 2009 WL 3419609 (Nat'l Arbitration Forum Oct. 15, 2009) (Foster, Arb.), *available at* http://domains.adrforum.com/domains/decisions/1280449.htm; HTL Automotive, Inc. v. Techshire, Claim No. FA1203001435046 (Nat'l Arbitration Forum Apr. 16, 2012), http://domains.adrforum.com/domains/decisions/1435046.htm; Media Rain LLC v. Verio Inc., FA0908001279419, 2009 WL 3166112 (Nat'l Arbitration Forum Sept. 29, 2009) (Lyons, Hill, Safran, Panel Arb.), *available at* http://domains.adrforum.com/domains/decisions/1279419.htm; Albir Hills Resort, S.A. v. Telepathy, Inc., Case No. D2012-0997, 2012 WL 3177577 (WIPO Arbitration & Mediation Ctr. July 19, 2012) (Barbero, Larramendi, Brown, Panel Arb.), *available at* http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-0997.

[130] Shoe Land Group LLC v. Development, Services c/o Telepathy Inc., Claim No. FA0904001255365, 2009 WL 1712834 (Nat'l Arbitration Forum June 9, 2009) (Petillion,

attempted to buy the domain name, but the parties could not agree on a price.[131] The complainant then used the failed negotiations and other facts to file a UDRP complaint.[132] Some of the complainant's assertions in its UDRP complaint were less than truthful to the point of being egregious. For example, the complainant alleged that respondent initially registered the domain name in bad faith to divert Internet traffic even though the complainant did not have any Internet presence until four years *after* the domain registration.[133] Nonetheless, two of the panelists refused to support a RDNH finding based on weak arguments about a common law trademark before the domain registration date.[134] However, it is easy to imagine that substituting these two panelists for other qualified individuals might have led to a RDNH finding under the facts of this proceeding. Thus, the choice of panelists and their comfort level with a RDNH finding can be a significant factor in the outcome of the dispute. This is something the parties can influence through electing to have a one- or three-person panel and also by nominating a panelist that has a record consistent with the party's position.

Another way to support a RDNH finding is to provide evidence of past abuse of the UDRP process or similar bad conduct by the complainant.[135] For example, one can highlight that the complainant has previously abused the UDRP process by bringing meritless claims, or engaged in bad conduct in the present case by repeatedly sending cease and desist letters, such that it amounts to harassment. Additionally, panels tend to look very unfavorably upon a complainant who is not forthcoming, misconstrues facts[136] and/or has waited years to file the complaint

---

Atkinson, Jr., Brown, Panel Arb.), *available at* http://www.adrforum.com/domains/decisions/1255365.htm.

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *See WIPO Panel Views on UDRP Questions*, *supra* note 127, ¶ 14.17.

[136] *See, e.g.*, usDocuments, Inc. v. Flexible Designs, Inc., Case No. D2003-0583, 2003 WL 25693619 (WIPO Arbitration & Mediation Ctr. Sept. 17, 2003) (Donahey, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0583.html; carsales.com.au Ltd. v. Flanders, Case No. D2004-0047, 2004 WL 3254858 (WIPO Arbitration & Mediation Ctr. Apr. 8, 2004) (Thorne, Ryan, Sorkin, Panel Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0047.html; Trailblazer Learning, Inc. v. Trailblazer Enters., Case No. D2006-0875, 2006 WL 4008237 (WIPO Arbitration & Mediation Ctr. Aug. 25, 2006) (Isenberg, Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0875.html; Altru Health Sys. v. Altruism Network, Claim No. FA0805001195584, 2008 WL 2808883 (Nat'l Arbitration Forum July 15, 2008) (Rindforth, Arb.), *available at* http://domains.adrforum.com/domains/decisions/1195584.htm; Viking Office Prods., Inc. v.

after finding out about the domain registration.[137] Finally, if applicable, the legitimate domain name registrant should bring to the panel's attention other available domain names that contain the trademark or that the domain name is a common word, making it less likely that the legitimate registrant was attempting to extort the trademark owner.

Panels have declined to find RDNH when the complainant has succeeded in presenting the elements of a DNH claim. Panels have also declined to find RDNH when, even though the complainant does not succeed, it was not obvious the claim would fail at the time it was filed or when respondent has failed to provide evidence of bad faith on the part of complainant.[138] The panel might also decline to find RDNH when there is a question of unclean hands on the part of both parties as when, for example, the respondent's domain name has links that explicitly refer to the complainant in attempt to generate revenue.[139] As such, a domain name registrant that requests a RDNH finding should avoid these situations whenever possible.

Although proffering support for a RDNH may require additional time and effort on behalf of the legitimate domain name registrant, a collective effort on behalf of all RDNH victims to make diligent requests for RDNH findings might be exactly what is needed to instigate UDRP reforms essential to reducing RDNH.

Natasha Flaherty, Claim No. FA1104001383534 (Nat'l Arbitration Forum May 31, 2011), http://domains.adrforum.com/domains/decisions/1383534.htm.

[137] *See, e.g.*, 3DCafe, Inc. v. 3d Cafe.com, Claim No. FA1010001351489 (Nat'l Arbitration Forum Dec. 20, 2010), http://domains.adrforum.com/domains/decisions/1351489.htm; North Country Bus. Prods. v. Jim Christopher, Claim No. FA1006001332468, 2010 WL 3116427 (Nat'l Arbitration Forum Aug. 4, 2010) (Gulliksson, Arb.), *available at* http://domains.adrforum.com/domains/decisions/1332468.htm; Noonan v. Sneed, Claim No. FA1008001343308 (Nat'l Arbitration Forum Oct. 22, 2010), http://domains.adrforum.com/domains/decisions/1343308.htm; Jelly Belly Candy Co. v. S.K. Indus. Private Ltd., Claim No. FA0709001082263, 2007 WL 4249828 (Nat'l Arbitration Forum Nov. 19, 2007) (Foster, Arb.), *available at* http://domains.adrforum.com/domains/decisions/1082263.htm; Jazeera Space Channel TV Station v. AJ Publ'g, Case No. D2005-0309, 2005 WL 1900290 (WIPO Arbitration & Mediation Ctr. July 19, 2005) (Smith, Loutfi, Lambert, Panel Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2005/d2005-0309.html; Dreamgirls, Inc. v. Dreamgirls Entm't, Case No. D2006-0609, 2006 WL 4006357 (WIPO Arbitration & Mediation Ctr. Aug. 10, 2006) (Bernstein, Hudis, Donahey, Panel Arb.), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0609.html.

[138] *See WIPO Panel Views on UDRP Questions*, *supra* note 127, ¶ 14.17.

[139] *Id.*

VI. DOMAIN NAME SUSPENSION UNDER THE UNIFORM RAPID SUSPENSION SYSTEM: AN ADD-ON POLICY FOR NEW GENERIC TOP-LEVEL DOMAINS

The Uniform Rapid Suspension (URS) system[140] is an add-on policy to the UDRP[141] that will apply to 1,400 new gTLDs launching in 2013. The URS aims to be faster and less expensive than current UDRP proceedings, allowing only fourteen days for a respondent to locate counsel and to prepare and file a response.[142] The URS system differs from UDRP proceedings in that it only allows for the suspension of a domain name, but not a transfer of the domain name to the complainant.[143] A complainant with a new gTLD has the option of filing a URS proceeding or instigating a proceeding under the UDRP.[144] Currently, one of the leading UDRP service providers, the National Arbitration Forum, will be the sole service provider and will render a URS decision for a speculated fee of $500.[145]

In developing the URS system, ICANN recognized the need to create a system with some "teeth" to dis-incentivize potential reverse domain name hijackers and address other issues associated with UDRP proceedings. The URS incorporates a "two strikes rule" under which there are penalties upon a third finding of an "abusive filing" against a complainant.[146] After a third finding of an "abusive filing," the complainant is no longer allowed to file URS complaints.[147] URS proceedings also incorporate an internal appeals procedure.[148]

---

[140] Natalie Dreyfus, *The Trademark Clearing House – a useful tool for defending trademarks and registering domain names in the new generic top-level domains (gTLDs)*, LEXOLOGY (Feb. 18, 2013), http://www.lexology.com/library/detail.aspx?g=676f06ee-c0e9-44ee-afba-1b2609c9f152 (noting unique features of the URS system include its trademark clearing house, Sunrise service and Trademark Claims service).

[141] *See* MILAM, *supra* note 83, at 17 (quoting the Government Advisory Committee, "[U]ncertainty . . . 'would be compounded if simultaneously the future of the primary, pre-existing, and proven RPM - the UDRP - were also subject to uncertainty as a result of a long-running PDP [Policy Development Process].'").

[142] *New Generic Top-Level Domains—Uniform Rapid Suspension System*, INTERNET CORP. FOR ASSIGNED NAMES & NOS., ¶ 5.1 (Mar. 1, 2013) [hereinafter *URS Procedure*], http://newgtlds.icann.org/en/applicants/urs.

[143] *Id.* ¶¶ 10.2–10.4.

[144] *Id.* ¶ 1.1.

[145] Philip Corwin, *ICANN Announcement of NAF as First URS Provider Raises Multiple Questions*, INTERNET COMMERCE ASS'N (Feb. 26, 2013, 8:49 PM), http://www.internetcommerce.org/NAF_URS_Questions.

[146] *URS Procedure*, *supra* note 142, ¶ 11.

[147] *Id.* ¶ 11.5.

[148] *Id.* ¶ 12.

Overall, the new URS system suggests positive headway in terms of developing effective policy-based mechanisms to discourage abusive filing. However, while the URS addresses some issues of the UDRP, it is not a universal fix. It only applies to the new gTLDs, and complainants still have the option of filing a UDRP proceeding, allowing the complainant to avoid penalties available under the URS upon a finding of abusive filing. Thus, changes to the UDRP are still needed.

VII. SUGGESTED UDRP AMENDMENTS AND INITIATIVES TO REDUCE RDNH

Despite the legitimacy of ICANN's resistance to the early calls for more specific RDNH guidelines, it is remarkable that the UDRP remains unchanged since its 1999 effective date given the rapid pace at which technology and Internet law have developed.[149] Notably, however, UDRP reform might be on the horizon. While the Generic Names Supporting Organization (GNSO), ICANN's internal policymaking body, has chosen to defer the initiation of a UDRP reform inquiry[150] during the implement of the URS system,[151] it plans to reevaluate the decision in mid-2014.[152] Several amendments and initiatives are presently available and should be considered to reduce the prevalence of RDNH, including establishing clear standards for RDNH, instituting penalties upon a RDNH finding, erecting an appeals process within the UDRP, amending the mutual jurisdiction provision, and ICANN ensuring that a somewhat level amount of information is available to each party. Each of these proposed UDRP reform measures is discussed in greater detail below.

---

[149] *See Rules of UDRP Procedure*, *supra* note 4 (effective for complaints submitted on or after March 1, 2010).

[150] *See* MARGIE MILAM, SPECIAL TRADEMARK ISSUES REVIEW TEAM RECOMMENDATIONS 38 (Dec. 11, 2009), *available at* http://gnso.icann.org/en/node/8000 (stating that "[t]here is a good probability that over the next few years, the two procedures [UDRP and URS] will be reviewed and merged into a single procedure").

[151] *See supra* Part VI.

[152] Advocates of RDNH protection should prepare to defend the current notice requirements in the Rules of Procedure, which were enacted as a control on RDNH. *See Rules of UDRP Procedure*, *supra* note 4, ¶¶ 1, 2, 4. Service providers will likely seek to eliminate the notice requirement because it is a procedural barrier, especially when a cybersquatter transfers the domain name at issue, after a complaint is filed to an obscure registrar in order to change the status of mutual jurisdiction. However, by amending the mutual jurisdiction clause to cover the registrant's jurisdiction instead of eliminating the notice requirement, both the interests of the RDNH protection advocates and the service providers would be satisfied.

A. ICANN Endorsed Standards for Finding RDNH

The UDRP has significant areas for improvement. Fundamentally, there is no clear articulation of when a RDNH finding is appropriate. Even during its initial development, some members of the drafting committee felt that the UDRP should offer more detailed guidelines as to how a panel might find RDNH.[153] Yet, the ICANN staff and counsel decided that such elaboration would be "more prudently deferred until experience with the proceedings under the policy and rules accumulates."[154] Time has shown, however, that panelists are uncomfortable with leading the development of the UDRP, and for over ten years panelists have encouraged ICANN to develop criteria for RDNH in their decisions.[155]

While data suggests that panelists are gradually becoming more comfortable with finding RDNH, it is still rare.[156] One reason for the slow development of clear standards could be that a panel's decision has absolutely no binding effect on any other panel, and the standard is a "balance of probabilities"[157] across the board. Thus, the basis of finding RDNH must indirectly achieve some critical amount of acceptance before it will be consistently applied. This process would be better facilitated if the panel were required to make a RDNH determination upon the respondent's request and to state the basis for its decision. As the UDRP exists today, the panel has the discretion to not address RDNH even after the respondent's request, and it is not uncommon to see panels exercising this discretion and completely ignoring the RDNH request when it comes to their findings.[158]

---

[153] *Staff Report*, *supra* note 98.

[154] *Id.*

[155] Strick Corp. v. Strickland, Forum File No. FA94801 (Nat'l Arbitration Forum July 3, 2000), *available at* http://www.adrforum.com/domains/decisions/94801.htm.

[156] *See* statistics from NAF and WIPO database searches for cases containing "Reverse Domain Name Hijacking." NAF database returned thirty-four cases where RDNH was found, compared to the 17,000 UDRP disputes NAF reports it has handled.

[157] Bella I. Safro & Thomas S. Keaty, *What's in A Name? Protection of Well-Known Trademarks Under International and National Law*, 6 TUL. J. TECH. & INTELL. PROP. 33, 45 (2004).

[158] *See, e.g.*, J Brand, Inc. v. Fundacion Private Whois, Claim No. FA1206001451383 (Nat'l Arbitration Forum Aug. 16, 2012), http://domains.adrforum.com/domains/decisions/1451383.htm; DOTMED.COM, Inc v. Hexap & Promopixel SARL, Case No. D2012-1117, 2012 WL 3561534 (WIPO Arbitration & Mediation Ctr. Aug. 9, 2012) (Pibus, Arb.), *available at* http://www.wipo.int/amc/en/domains/search/text.jsp?case=D2012-1117.

B. Specific and Significant Penalties for RDNH

In order to reduce RDNH, the UDRP should provide for specific and significant penalties to be imposed on the complainant upon a panel's finding of RDNH. For example, the complainant could be sanctioned for an abuse of administrative proceeding based on the complainant's signed statement in its initial complaint.[159] In addition, a legitimate domain name registrant could be awarded costs and attorney fees upon a RDNH finding.[160] ICANN could ban a reverse domain name hijacker from initiating another UDRP claim for a certain period of time as a consequence and maintain a public list of banned parties, which might discourage RDNH as a way to avoid public embarrassment. ICANN could even amend the UDRP to allow panels to factor in a non-dispositive prejudice against a repeat offender. These measures would serve as much needed deterrents to filing frivolous DNH claims under the UDRP.

C. Internal UDRP Appeals Process

The UDRP should incorporate an appeals process for victims of RDNH that face an adverse decision from the initial proceeding. Currently, trademark owners reap the benefit of having a low cost alternative to court to resolve a domain name dispute, an ICANN proceeding. However, following a UDRP proceeding, court is the only forum for recourse available to a RDNH victim.[161] Yet, as explained above, a RDNH victim often does not have the financial resources or time required to file a lawsuit. An internal UDRP appeals process would even out this imbalance and provide a low-cost opportunity to reverse a wrong transfer order.

D. Mutual Jurisdiction Provision Amendment

A less intensive, partial remedy to the problem of a court proceeding being prohibitively expensive for a RDNH victim would be to simply amend the mutual jurisdiction provision of the UDRP.[162] In its current state, the UDRP provides that a lawsuit can be filed in the jurisdiction of the registrar or of the domain name registrant's address as listed in the WHOIS database at the time of the complaint

[159] *Rules of UDRP Procedure*, *supra* note 4, ¶ 3(b)(xiv).

[160] Sallen v. Corinthians Licenciamentos Ltda, 273 F.3d 14, 18 (1st Cir. 2001) (stating 35 U.S.C. § 1114 (2)(D)(iv)–(v) remedies include a declaration of non-violation of the ACPA, return of the wrongfully transferred domain name and in certain circumstances, damages including attorney fees incurred by the domain name registrant).

[161] *The UDRP Process*, BECKMAN CTR. FOR INTERNET & SOC'Y, HARVARD UNIV. (2012), *http://cyber.law.harvard.edu/udrp/process.html*.

[162] *Rules of UDRP Procedure*, *supra* note 4, ¶ 3(b)(xii).

filing.[163] However, the registrar's jurisdiction may be geographically removed from the legitimate domain name registrant.[164] The UDRP could instead provide for exclusive jurisdiction according to the respondent's domicile so that travel costs would be reduced, and the victim of RDNH would not have to incur the costs of locating competent counsel in a foreign jurisdiction.

E. Enhanced Information Sharing and Technical Training

In addition to formal UDRP reforms, ICANN should undertake broad initiatives to minimize the risk of RDNH and ensure that reverse domain name hijackers are properly identified as such. First, ICANN should lessen the disparity between parties in regard to the available information. Given its purpose to offer a dispute resolution forum where parties can represent themselves,[165] ICANN should offer a layman's guide to the UDRP process and aggregate statistics on UDRP disputes to enable *pro se* respondents to make strategic arguments based on historical data.[166] Under the current system, complainants that have done their own statistical analysis can engage in forum selection between the service providers[167], which might have an impact on the outcome of the case.

Similarly, thorough information should be maintained on individual panelists. Independent research suggests this individualized tracking may highlight the need

[163] *See WIPO Guide to UDRP Policy*, *supra* note 88 ("The Mutual Jurisdiction is defined in the UDRP Rules as a court jurisdiction at the location of *either* (a) the principal office of the registrar (provided that the domain name registrant has submitted in the Registration Agreement to that jurisdiction for court adjudication of disputes concerning or arising from the use of the domain name) or (b) the domain name registrant's address as shown for the registration of the domain name in the concerned registrar's WHOIS database at the time the Complaint is submitted to a dispute resolution service provider.") (emphasis in original).

[164] *Id.* ("Under the terms of the agreement which the domain name registrant entered into when registering the domain name, the registrant must submit to the administrative proceeding. The Respondent has 20 days from the date of commencement of the administrative proceeding to submit a Response.").

[165] *See supra* note 149 and accompanying text.

[166] Some service providers voluntarily supply statistical data and analytics on the UDRP decisions their panelists render. *See Model Response and Filing Guidelines*, WIPO ARBITRATION & MEDIATION CTR., http://www.wipo.int/amc/en/domains/respondent/ (last visited May 23, 2012) ("If appropriate and the allegation can be substantiated with evidence, the Rules provide that a Respondent may ask the Panel to make a finding of reverse domain name hijacking.").

[167] Patrick Kelley, *Emerging Patterns in Arbitration Under the Uniform Domain-Name Dispute-Resolution Policy*, http://www.law.berkeley.edu/files/bclt_AnnualReview_Emerging_Final.pdf (last visited May 23, 2013).

for ICANN to formally mandate random panel assignments.[168] At the very least, compiling this information, or requiring the service providers to do so, would enable the service providers to identify panelists who appear to need more training.

If the panelists do in fact enable RDNH, ICANN could use service provider training sessions as a gateway to better educate panelists on RDNH. This would help prevent *ad hoc* policy judgments, and would steer the substantive trends for finding RDNH in a way ICANN deems appropriate. Importantly, panelists should be comfortable with finding RDNH in cases where appropriate, even when the respondent did not request it. ICANN could also remind panelists of their authority to request additional information from the parties, such as support for RDNH, and that time extensions to gather the additional information is a legitimate course of action.

VIII. CONCLUSION

While there are many reasons to support UDRP reform, there is some resistance to change within the UDRP community. Arguments against amending the UDRP mainly rely on the fact that bona fide RDNH cases are rare[169] and instituting a penalty system within the UDRP might do more harm than good. Arguments against amending the UDRP also tend to rely on anecdotal evidence, including the suggestion that lawyers inexperienced in handling domain name disputes typically file the RDNH cases because they lack a working knowledge of the UDRP's purpose and the proposition that when "big filers"[170] file a questionable claim, they tend to lose. However, such arguments do not account for the significant negative impact inflicted on legitimate domain name registrants in these situations.

Even if most questionable claims lose, it still places undue time and monetary expenses on the respondent. The arguments against UDRP reform also fail to account for the time, money, and investment losses of legitimate domain name

---

[168] *See 2012 Domain Name Dispute Study: 7 Select Panelists Decide Nearly Half of All Cases*, DNATTORNEY.COM (Aug. 28, 2012), http://dnattorney.com/NAFdomainnamedisputestudy2012.shtml.

[169] A response to this counterargument is that RDNH findings are statistically rare because panelists avoid such findings due to the general lack of criteria and the fact that panelists are not required to address RDNH even if it is raised by the respondent.

[170] "Big filers" include companies that initiate a considerable number of UDRP claims, such as Barclay's and Jimmy Choo, both of which each filed upwards of ten UDRP complaints in 2010 alone. *UK firms that are the most active in combating cybersquatting*, KEEP ALERT, ONLINE BRAND MONITORING, http://www.keepalert.com/Experts-opinions/uk-firms-that-are-the-most-active-in-combatting-cybersquatting.html (last visited May 23, 2013).

registrants in situations where the reverse domain name hijacker successfully obtains a domain name after merely threatening to bring an UDRP claim, thus skewing the statistics. A legitimate domain name registrant might sell its domain name, regardless of the merits of the claim, because of the financial incentive to avoid the dispute. In the face of a RDNH threat, a legitimate domain name registrant is in a perplexing situation. Economically, the legitimate domain name registrant needs to ask for a transfer price that accounts for not easily quantifiable costs such as losing business as a result of confusion, informing consumers of the new domain name, and reprinting common advertising material. And they must also be sensitive to the fact that an absurd demand might weigh against an ultimate finding of RDNH if a UDRP dispute is filed after unsuccessful negotiations.

While there are certainly arguments for keeping the UDRP as is since the full consequences of suggested reforms are not known, it seems clear that benefits from at least some reforms would outweigh any potential negative consequences, and result in a system more balanced for both parties. Adding monetary penalties to a finding of RDNH, having ICANN and/or service providers make data publicly available, instituting an appeals process, and amending the mutual jurisdiction provision are all tools that would work towards meeting the overall goals of the UDRP and dis-incentivizing misuse of the UDRP in attempts at RDNH.