Valparaiso University Law Review

Volume 45
Number 2 *Winter 2011*

*pp.*505-549

Winter 2011

Imminent Domain Name: The Technological Land-Grab and ICANN's Lifting of Domain Name Restrictions

Brian W. Borchert

Notes

IMMINENT DOMAIN NAME: THE TECHNOLOGICAL LAND-GRAB AND ICANN'S LIFTING OF DOMAIN NAME RESTRICTIONS

I. INTRODUCTION

We learn from history that we learn nothing from history.[1]

On May 20, 1862, the United States Congress passed the Homestead Act, which prompted American citizens to settle and claim lands throughout the western frontier.[2] Following an application process, this legalized land-grab allotted 160 acres of land for homesteaders to live on, improve, and cultivate crops.[3] The United States Congress created this Act to encourage settling and cultivation of the previously uninhabited western territories.[4] Unfortunately, fraud plagued this new policy.[5] Land speculators and corporations often hired phony claimants to claim lands that were abundant in natural resources such as timber, coal, and oil.[6] It is estimated that between 1852 and 1904, the General Land Office granted 500 million acres through the Homestead Act, though

---

1 KEVIN GOLDSTEIN-JACKSON, THE DICTIONARY OF ESSENTIAL QUOTATIONS 72 (1983) (quoting George Bernard Shaw, an Irish playwright, critic, and political activist (1856–1950)).

2 Homestead Acts, ch. 75, 12 Stat. 392 (expired 1976); DENNIS W. JOHNSON, THE LAWS THAT SHAPED AMERICA 91 (2009) (noting that President Lincoln signed the legislation on May 20, 1862).

3 JOHNSON, *supra* note 2, at 90 (describing that homesteaders would receive either 160 acres valued at $1.25 per acre, or 80 acres at $2.50 per acre).

4 *See id.* at 79 (explaining that homesteading lands were given to settlers who could not normally afford them in exchange for their hard work to improve and settle the western lands).

5 Lee Ann Potter & Wynell Schamel, *The Homestead Act of 1862*, THE NAT'L ARCHIVES, http://www.archives.gov/education/lessons/homestead-act/ (last visited Dec. 23, 2010) (demonstrating that the misconduct included land speculators taking advantage of the legislative loophole that failed to specify if the 12x14 dwelling was to be in feet or inches, and that the underfunded Land Office had underpaid and overworked agents who were open to bribery).

6 Kathy Weiser, *The Homestead Act – Creating Prosperity in America,* LEGENDS OF AM., http://www.legendsofamerica.com/AH-Homestead.html (last visited Dec. 23, 2010) (noting that the phony claimants alleged they made "improvements" to the land when in reality all they did was sell their land to the highest bidder).

approximately only 80 million acres actually went to homesteaders.[7] A number of subsequent homesteading laws attempted to fix the initial failure, but most of the available western territory had already been distributed.[8]

Evidently, history has an interesting way of repeating itself. Some of the same issues that beleaguered the Homestead Act over 150 years ago are now playing out in the technological land-grab occurring on the Internet. The registration of domain names in the twenty-first century represents the new technological land-grab. The Internet Corporation for Assigned Names and Numbers ("ICANN"), the governing body of the Internet, plays the role of the United States Congress in 1852. The Homestead Act of today happens to be the lifting of restrictions on who can register domain names and what names can be registered. This new expansion of domain name registrations has insufficient legal backing, and as a result, fraud by way of cybersquatting is likely to occur.[9]

This Note reviews the issue of abusive domain name registration in relation to ICANN's lifting of registration restrictions. Part II explores background material such as the formation of the Internet and the domain name system as it exists today.[10] Later, it covers the numerous forms of domain name abuses and the varied public and private remedies created to combat domain name registration abuse.[11] In Part III, the public and private remedies are assessed and critiqued.[12] Following that analysis, Part IV suggests an ideal and previously unarticulated approach to accommodate ICANN's new expansion policy in regard to domain name registration.[13] For a complete understanding of this issue, it is best to review the background of the Internet and the domain name system.

---

7 *Homestead Act (1862)*, OUR DOCUMENTS, http://www.ourdocuments.gov/doc.php?flash=old&doc=31 (last visited Dec. 23, 2010) ("Of some 500 million acres dispersed by the General Land Office between 1862 and 1904, only 80 million acres went to homesteaders.").

8 Weiser, *supra* note 6 (detailing that the Homesteading Act of 1912 and Taylor Grazing Act of 1934 attempted to reconcile the shortcomings of the 1852 Act but most of the land had already been allocated).

9 *See infra* II.D (discussing the problematic expansion of domain name registrations).

10 *See infra* Part II.A–C (covering the Internet and the domain name system's formation and governance).

11 *See infra* Part II.E–F (detailing domain name registration abuses and the current remedies available).

12 *See infra* Part III (analyzing the successes and failures of the current remedial measures).

13 *See infra* Part IV (suggesting various solutions to current domain name registration issues).

II. BACKGROUND

Part II.A explores the Internet's foundation and its basic structure.[14] Then, Part II.B progresses to the formation, history, and functioning of the domain name system.[15] After covering how the domain name system works, Part II.C explores how the domain name system is governed and maintained.[16] Following an explanation of Internet administration, Part II.D discusses and explains typical domain name registration disputes.[17] Following the full explanation of domain name registration disputes, Part II.E delves into a more specific analysis and breakdown of the most prevalent domain name disputes.[18] Finally, Part II.F highlights the major remedial measures in place to adjudicate current domain name disputes.[19]

A. Internet Fundamentals

The Internet began as an experimental government research project.[20] In the Internet's infancy—as a far less complex form—the United States government maintained control of its operation.[21] Within a short period of time, the functionality and utility of the Internet began to expand.[22] By the mid-1980s, scientists linked computers all over the world into a "network of networks."[23]

---

14 *See infra* Part II.A (discussing the Internet's formation and initial structure).

15 *See infra* Part II.B (covering the history and development of the domain name system).

16 *See infra* Part II.C (reviewing the Internet's governance and administration).

17 *See infra* Part II.D (explaining the potential problems of the introduction of new generic top-level domains).

18 *See infra* Part II.E (specifically addressing the most problematic domain name disputes).

19 *See infra* Part II.F (addressing the legislative measures to combat domain name disputes).

20 *See* Peter T. Holsen, *ICANN'T Do It Alone: The Internet Corporation for Assigned Names and Numbers and Content-Based Problems on the Internet*, 6 MARQ. INTELL. PROP. L. REV. 147, 149 (2002) ("In 1965, scientists developed a way for a computer in Massachusetts to communicate with a second computer in California. The U.S. Department of Defense deemed this technology to have great potential and funded research projects to further its development.").

21 Reece Roman, Note, *What if ICANN Can't?: Can the United Nations Really Save the Internet?*, 15 SYRACUSE SCI. & TECH. L. REP. 27, 2 (Spring 2007), *available at* http://justice.syr.edu/sstlr/wp-content/uploads/what-if-icann-cant_can-the-united-nations-really-save-the-internet.pdf (describing that initially the U.S. Government oversaw the Internet with the help of a number of research institutions).

22 Holsen, *supra* note 20, at 149 (explaining that many universities and governmental agencies maintained private computer networks that transferred data and email messages).

23 Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 193 (Oct. 2000).

The contemporary Internet is an even more elaborate and complicated system of networks.[24] Each individual computer connected on the Internet is assigned a unique identifying code known as an Internet Protocol ("IP") address.[25] As the Internet became more commercialized, the long string of numbers in an IP address became increasingly cumbersome to the average Internet consumer, necessitating a more workable system.[26] To solve this problem, domain names replaced IP addresses as a more navigable tool for using the Internet.[27] The Internet has grown exponentially since the time that domain names became the standard.[28] Accordingly, commercial industries and retailers

---

[24] *See* Kevin A. Meehan, Note, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INT'L & COMP. L. REV. 345, 349 (2008) (explaining that the geography of the Internet "is not . . . easily charted"); *ICANN DNS Stability: The Effect of New Generic Top Level Domains on the Internet Domain Name System*, ICANN, 1 (Feb. 6, 2008), http://www.icann.org/en/topics/dns-stability-draft-paper-06feb08.pdf [hereinafter ICANN DNS Stability] (stating that the Internet's structure "consists of a backbone of networks and servers connected" with one another that allow for the sharing of information). These information sharing technologies include Internet Protocol ("IP") addresses and domain names and fall under the Internet's Domain Name System ("DNS"). *Id*.

[25] Lockheed Martin Corp. v. Network Solutions, Inc., 141 F. Supp. 2d 648, 650 (N.D. Tex. 2001) (describing that the IP gives each computer a unique numerical address on the Internet that consists of four groups of numbers separated by periods).

[26] *See* Amanda Rohrer, *UDRP Arbitration Decisions Overridden: How* Sallen *Undermines the System*, 18 OHIO ST. J. ON DISP. RESOL. 563, 566 (2003) (noting that the long string of numbers in IP addresses are difficult to remember).

[27] *See* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, 37–38 (2000). Froomkin explains that in their most simplistic form

> [d]omain names are the alphanumeric text strings to the right of an "@" in an e-mail address, or immediately following the two slashes in a World Wide Web address. By practice and convention, domain names can be mapped to a thirty-two-bit number consisting of four octets (sets of eight binary digits) that specifies a network address and a host ID on a TCP/IP network. These are the "Internet protocol" (IP—not to be confused with "intellectual property") numbers—the numbers that play a critical role in addressing all communications over the Internet, including e-mail and World Wide Web traffic. They have justly been called the "human-friendly address of a computer."

Id.; *see also* Nilanjana Chatterjee, *Arbitration Proceedings Under ICANN's Uniform Domain Name Dispute Resolution Policy - Myth or Reality*, 10 VINDOBONA J. INT'L COM. L. & ARB. 67, 71 (2006) (clarifying that an Internet domain name is the equivalent to a phone number or street address); Ian J. Block, Comment, *Hidden Whois and Infringing Domain Names: Making the Case for Registrar Liability*, 2008 U. CHI. LEGAL F. 431, 433 (describing that domain names identify Internet websites for the ease of user web navigation).

[28] *See Internet Usage Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited Sept. 23, 2010) (according to statistics as recent as June 30, 2009, there were over 1.6 billion internet users across the globe with an astounding 362.3% user growth from 2000 to 2009); *see also Domain Counts & Internet Statistics*, DOMAIN TOOLS,

have flocked to this new medium to reach consumers and bolster sales.[29] This increase in Internet usage, and commerce conducted therein, also exposed problems.[30] For a complete understanding of these issues, further explanation of how the Internet Domain Name system functions is necessary.

B. The Domain Name System ("DNS")

Contrary to popular belief, the Internet DNS does not consist of one single file but rather is a complex, leveled system similar to a pyramid.[31] At the apex of the DNS pyramid is the root zone.[32] The root zone consists of the general category of top-level domains ("TLDs").[33] Three

---

http://www.domaintools.com/internet-statistics/ (last visited Jan. 30, 2011) (calculating that as of October 6, 2009, there were 111,971,495 currently active and registered domain names in the world).

[29] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741, 31,743 (June 10, 1998) ("From its origins as a U.S.-based research vehicle, the Internet is rapidly becoming an international medium for commerce, education and communication."); *see also* Kiran Nasir Gore, Comment, *Trademark Battles in a Barbie-Cyber World: Trademark Protection of Website Domain Names and the Anticybersquatting Consumer Protection Act*, 31 HASTINGS COMM. & ENT. L.J. 193, 200 (2009) (summarizing that in the late 1990s the Internet became an avenue for businesses to better reach consumers); U.S. CENSUS BUREAU, E-STATS (May 28, 2009), *available at* http://www.census.gov/econ/estats/2007/2007reportfinal.pdf. The most recent U.S. Census Bureau statistics show that U.S. retail online commerce reached almost $127 billion in 2007, up from $107 billion in 2006. U.S. CENSUS BUREAU, *supra*, at 1. Further, from 2002 to 2007 online retail sales grew at an annual rate of 23.1%, compared to a meager 5% for total retail sales. *Id.* at 3.

[30] *See* Sallen v. Corinthians Licenciamentos LTDA, 273 F.3d 14, 19 (1st Cir. 2001) (relating that the number of disputes over domain names have increased with the growing commercialization of the Internet); Kenneth S. Dueker, Note, *Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses*, 9 HARV. J.L. & TECH. 483, 483 (1996) ("The phenomenal growth of the Internet as a commercial medium has brought about a new set of concerns in the realm of intellectual property."); David S. Magier, Note, *Tick, Tock, Time is Running Out to Nab Cybersquatters: The Dwindling Utility of the Anticybersquatting Consumer Protection Act*, 46 IDEA 415, 417 (2006). The author notes that "[b]ecause of the borderless, ubiquitous, and often anonymous nature of cyberspace, the increase in e-commerce brings to the fore significant jurisdictional challenges for those seeking to protect their intellectual property." *Id.*

[31] *See* Globosantafe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 618 (E.D. Va. 2003) (explaining that the DNS is not a single master file in a single location but instead a hierarchical system with each "name server" providing information for its "zone").

[32] *See* ICANN DNS Stability, *supra* note 24, at 1 (outlining that the root zone which contains information regarding TLDs is found at the top of the DNS pyramid).

[33] *See, e.g.*, Am. Girl, L.L.C. v. Nameview, Inc., 381 F. Supp. 2d 876, 879 (E.D. Wis. 2005) (detailing the overall structure of top-level domains); *see also* Solid Host, N.L. v. Namecheap, Inc., 652 F. Supp. 2d. 1092, 1094 (C.D. Cal. 2009) ("A domain name is composed of two parts, separated by a period. The portion to the right of the period, i.e., the 'com' in <google.com>, is known as the 'top level domain' or 'TLD.'"); Smith v. Network Solutions, Inc., 135 F. Supp. 2d 1159, 1161 (N.D. Ala. 2001) ("An SLD [second-

different types of TLDs encompass all of the existing TLDs.[34] The most common type is the generic top-level domain name (known as a "gTLD"), which includes the .com, .org, and .net extensions and are not associated with any specific region or country.[35] In the 1980s, seven gTLDs were created.[36] Additional debates among the world Internet community led to the introduction of numerous more gTLDs within the last decade.[37] Currently, the comprehensive list of all the three types of authorized TLDs, known as the root domain's authoritative list, contains 265 official TLDs.[38] Numerically, the largest of the 265 TLDs in the DNS by far is the .com gTLD.[39]

Beyond the technical aspects of the DNS, the overall system is maintained by two groups: the registry and the registrars.[40] According

---

level domain] name is a string of numbers and/or letters immediately to the left of the dot in the address . . . . For instance, in the domain name 'example.com,' '.com' is the TLD and 'example' is the SLD name."). *See generally* Roman, *supra* note 21, at 8 ("TLDs provide a mechanism for name servers to recognize websites requested by Internet users.").

34 *See* Roman, *supra* note 21, at 7–8. The other two types of TLDs include the country specific (known as ccTLD), for example, .uk (United Kingdom), .ch (Switzerland), .au (Australia), or .jp (Japan). *Id.* The third type is used solely for infrastructure purposes and is not important to the average Internet user. *Id.*

35 *See id.* (noting that country specific top-level domains are known as ccTLDs).

36 *See Top-Level Domains (gTLDs)*, ICANN, http://www.icann.org/en/tlds (last visited Dec. 23, 2010) (noting that the following top-level domains were created in the 1980s; .com, .edu, .gov, .int, .mil, .net, and .org).

37 *See id.* (illustrating that within the last decade a number of other top-level domains such as .biz, .info, .name, .pro, .aero, .coop, and .museum have been unveiled).

38 *See* Scott P. Sonbuchner, Note, *Master of Your Domain: Should the U.S. Government Maintain Control over the Internet's Root?*, 17 MINN. J. INT'L L. 183, 186–87 (2008); *see also New gTLDs – Frequently Asked Questions*, ICANN, http://www.icann.org/en/topics/new-gtlds/strategy-faq.htm (last visited Dec. 23, 2010) [hereinafter ICANN FAQs] (stating twenty-one gTLDs currently exist).

39 *See* Dennis Carlton, *Report of Dennis Carlton Regarding ICANN's Proposed Mechanism for Introducing New gTLDs*, ICANN, 5 (June 5, 2009), http://www.icann.org/en/topics/new-gtlds/carlton-re-proposed-mechanism-05jun09-en.pdf (highlighting that more than 80 million .com TLDs exist while only 12 million and 7 million .net and .org TLDs exist, respectively); *see also* ICANN Registry Operator Monthly Reports January 2009, ICANN, http://www.icann.org/en/tlds/monthly-reports/ (last visited Dec. 23, 2010). A review of all the ICANN Accredited Registrars demonstrates that .com is the most commonly accredited TLD. *ICANN-Accredited Registrars*, ICANN, http://www.icann.org/en/registrars/accredited-list.html (last visited Oct. 7, 2010); *see also* Donna L. Howard, Note, *Trademarks and Service Marks and Internet Domain Names: Giving ICANN Deference*, 33 ARIZ. ST. L.J. 637, 639–40 (2001) (stating that the .com top-level domain name is the most commonly used by commercial entities and generally seen as a catchall top-level domain); C. Kim Le, Comment, *Genericness Need Not Apply: Employing Generic Domain Names in Cyberspace*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1093, 1095 (2004) (noting that approximately ninety-eight percent of all words found in Webster's English Dictionary are currently registered as domain names).

40 *See* Globosantafe Corp. v. Globalsantafe.com, 250 F. Supp. 2d 610, 619 (E.D. Va. 2003). Registrars deal directly with individual domain name registrants in a retail domain name

to the most recent statistics, there are currently 943 accredited domain name registrars and twenty official registries.[41] For an average Internet user, registering a domain name is a relatively streamlined and efficient process.[42] Once a registrar has received a domain name registration request, its obligations are minimal, which in turn results in some of the Internet's common governance and administrative issues.[43]

---

selling capacity. *Id*. The registry, in turn, operates in a more limited capacity by mainly maintaining and organizing the Registry Database. *Id.* That database consists of all the domain names registered by all registrants and registrars in each top-level domain. *Id.*; *see also* Solid Host, N.L. v. Namecheap, Inc., 652 F. Supp. 2d. 1092, 1095 (C.D. Cal. 2009) ("The registry maintains a centralized, publicly accessible database of information concerning all domain names in a TLD, known as the WHOIS (or Whois) database; this database is compiled from information submitted by registrars.").

41 *See generally ICANN-Accredited Registrars*, ICANN, http://www.icann.org/en/registrars/accredited-list.html (last visited Dec. 23, 2010) (indicating that there were 943 accredited registrars, 54.6% of which were located in the United States as of September 30, 2009); *Registry Listing*, ICANN, http://www.icann.org/en/registries/listing.html (last visited Dec. 23, 2010) (noting that there are currently twenty official registries).

42 *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 415–16 (2d Cir. 2004). The registration process occurs

> [w]hen an individual or an organization desires to register a domain name, it may do so through any accredited registrar . . . . The applicant first chooses one of the TLDs offered by the registrar and then creates an accompanying SLD name, thereby fashioning a potential domain name, which is then submitted electronically to the registrar for approval. However, *no two SLD names within a given TLD can be identical*. Accordingly, if someone submits an application for a particular domain name that already exists in the Registry WHOIS database by virtue of a prior registration, that name cannot be registered again, and the applicant is advised that the sought domain name is unavailable. The applicant may then choose to submit an application for an alternate domain name, either by changing or adding or subtracting a letter(s) or number(s) or a dash(es) to his initially submitted SLD name within the same TLD, or by going to another TLD where the initially submitted SLD name is still available. If there is no existing registration for a given SLD name within a given TLD, that domain name is considered available and generally may be registered on a first-come, first served basis.

Id. (quoting Smith v. Network Solutions, Inc., 135 F. Supp. 2d 1159, 1161–62 (N.D. Ala. 2001). The court also determined that, at a minimum, applicants must supply their name, postal address, telephone number, and an e-mail address. *See id*. at 395.

43 *See* Howard, *supra* note 39, at 640 (explaining that in the domain name registration process the registrar audits to make sure the same name is not already registered). If it is not, then the registration is approved. *Id.* During the application process, the applicant must assure that its use of the domain name does not violate a third party's rightful ownership and also that any use of the domain name will not be for unlawful activity. *Id.* The registrar itself does not conduct its own investigation into the applicant. *Id.*

C. Domain Name Governance and Administration

Following the adoption of a federal policy favoring competitive domain name registration, the Clinton administration issued two plans that formed a private non-profit corporation responsible for governing the DNS.[44] As part of those plans, the Internet Corporation for Assigned Names and Numbers stepped in to govern the complex DNS.[45] From its inception, ICANN had specific strategic objectives in mind regarding the governance of the DNS.[46] The federal government surrendered the DNS

---

[44] *Solid Host, N.L.*, 652 F. Supp. 2d at 1095 ("In 1998, the federal government adopted a policy favoring competitive domain name registration. 'In furtherance of this policy, a private, non-profit corporation, the Internet Corporation for Assigned Names and Numbers ('ICANN'), was formed to assume responsibilities for managing the allocation of Internet Protocol numbers and the domain name system.'") (citations omitted). The Clinton administration addressed these concerns by "issuing a White Paper titled *Management of Internet Names and Addresses*. The White Paper recognized a 'need for change' regarding the Internet's administration. . . . [and] called on the Internet community to create an administrative body 'based on a broad consensus among industry stakeholders,' that would be free from government control." Roman, *supra* note 21, at 6 (parenthetical omitted) (citing and quoting Management of Internet Names and Addresses, 63 Fed. Reg. 31, 741 (proposed Feb. 20, 1998) [hereinafter White Paper], *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm)); *see also* Howard, *supra* note 39, at 655 ("[The Clinton administration] issued two plans, the 'White Paper' and 'Green Paper,' that 'would confer upon this non-profit corporation much responsibility in the domain naming system,' granting ICANN 'leeway in how it carried out its functions' and allowing ICANN 'to set forth certain standards.'") (quoting Adam Silberlight, Comment, *WWW.How to Be a Master of Your Domain.com: A Look at the Assignment of Internet Domain Names Under Federal Trademark Laws, Federal Case Law and Beyond*, 10 ALB. L.J. SCI. & TECH. 229, 270–71 (2000)).

[45] *See* Roman, *supra* note 21 ("In response to these criticisms the Internet Corporation for Assigned Names and Numbers (ICANN) emerged as the recognized authority charged with DNS governance."); *see also* Rod Beckstrom, *Message from the CEO*, ICANN, http://www.icann.org/en/ceo/ceo-message-21jul09-en.htm (last visited Dec. 23, 2010) ("[ICANN's] original 1998 memorandum of understanding with the U.S. Government stated one of [ICANN's] key responsibilities this way: 'Oversight of the policy for determining the circumstances under which new top level domains would be added to the root system.'"). *See generally Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers*, ICANN, http://www.icann.org/en/general/icann-mou-25nov98.htm (last visited Dec. 23, 2010) (documenting the agreement between the Department of Commerce and ICANN).

[46] *See* Lockheed Martin Corp. v. Network Solutions, Inc., 141 F. Supp. 2d 648, 651 (N.D. Tex. 2001). ICANN stated that it

> has four mandates . . . . First, ICANN bears responsibility for overseeing the infrastructure of the Internet. Second, it bears responsibility for ensuring competition among domain name registrars of the TLDs. Third, ICANN bears partial responsibility for establishing domain name dispute resolution policies. And, fourth, ICANN bears responsibility for determining whether and when to add new TLDs.

governance power to ICANN because a private governing organization had certain advantages.[47] Nonetheless, the federal government was not willing to allow ICANN to have complete autonomy.[48] ICANN, however, used its delineated powers to create a more regimented system for its registries and registrars.[49] This system operated rather smoothly for nearly eleven years and only recently had some substantial complications.[50]

Id.; *see also ICANN Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*, ICANN (as revised Nov. 21, 1998), http://www.icann.org/en/general/articles.htm . The Articles state ICANN

> shall . . . pursue the charitable and public purposes of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet by (i) coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet; (ii) performing and overseeing functions related to the coordination of the Internet Protocol ("IP") address space; (iii) performing and overseeing functions related to the coordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system; (iv) overseeing operation of the authoritative Internet DNS root server system; and (v) engaging in any other related lawful activity in furtherance of items (i) through (iv).

Id.

47 *See* Roman, *supra* note 21, at 6 (explaining that a nongovernmental organization was more favorable to govern the Internet because private entities are more flexible, specialized, and capable of quick action); *see also* White Paper, *supra* note 44 (stating that private administration of the Internet would better effectuate the goals of Internet stability, competition, private coordination, and representation of the whole Internet community).

48 *See* Sonbuchner, *supra* note 38, at 192 (explaining that the U.S. Government willingly handed over the control of the Internet's infrastructure but maintained oversight of ICANN); *see also* Kim G. von Arx & Gregory R. Hagen, *A Declaration of Independence of ccTLDs from Foreign Control*, 9 RICH. J.L. & TECH. 4, ¶ 17 (Fall 2002), *available at* http://jolt.richmond.edu/v9i1/Article4.html#_ednref1 ("[The Department of Commerce] controls ICANN through a contractual framework underpinned by the DoC control of the A root domain server."); Roman, *supra* note 21 (pointing out that ICANN derives its authority from a series of contracts with the Department of Commerce).

49 *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 415 (2d Cir. 2004) ("ICANN policies regarding domain name registrations 'are mainly implemented through ICANN's entry of agreements with domain-name registries and registrars.'") (quoting *Second Status Report Under ICANN/US Government Memorandum of Understanding*, ICANN (June 30, 2008), http://www.icann.org/general/statusreport-30jun00.htm); *see also* Sonbuchner, *supra* note 38, at 194 ("ICANN's solution was a mandatory registrar accreditation system: all registrars would have to meet ICANN specified qualifications before they could sell domain names to the public."). *See generally Registrar Accreditation: Overview*, ICANN, http://www.icann.org/registrars/accreditation-overview.htm (last visited Dec. 23, 2010) (summarizing the role of registrars).

50 *See* ICANN, *2008 Annual Report*, iv (Dec. 31, 2008), http://www.icann.org/en/annualreport/annual-report-2008-en.pdf. Since ICANN's inception

D. Introduction of New gTLDs as a Potential Problem

Recently, ICANN ratified a groundbreaking new policy that would allow it to accept registrations for new gTLDs from private entities.[51] ICANN determined that such an expansion was mandatory for the continued technological advancement and innovation of the Internet.[52]

> we have witnessed tremendous growth in the ICANN community with more government engagement through the Government Advisory Committee, an increased multi-stakeholder participation and an enhanced bottom-up process. Despite all of the changes and challenges that the Internet has faced, ICANN has made remarkable evolution in its structure and has continued to grow towards a truly global and stable organization, operating in an open and transparent manner.

Id.

[51] Christine Haight Farley, *Convergence and Incongruence: Trademark Law and ICANN's Introduction of New Generic Top-Level Domains*, 25 J. MARSHALL J. COMPUTER & INFO. L. 625, 626 (2009). This policy is seen as radical because

> it is not meant to just provide a handful of new gTLDs. Nor is it meant to provide a set [sic] a period for applications or specific ideas about what areas these new gTLDs will designate. Instead, what ICANN is considering is a uniform system to approve generic top level domains that is expected to have profound implications. ICANN expects to approve hundreds of new gTLDs annually in the future.

Id.; s*ee, e.g.*, Danny Younger, *Languages in the Root: A TLD Launch Strategy Based on ISO 639*, CIRCLEID (Oct. 5, 2004 8:23 PM), http://www.circleid.com/posts/languages_in_the_root_a_tld_launch_strategy_based_on_iso_639 (claiming that over 400 language-affiliated TLDs alone are currently being proposed); *see also* Reinhardt Krause, *Name Game Challenges ICANN's New Chief*, INVESTOR'S BUS. DAILY, Nov. 27, 2009, *available at* 2009 WLNR 23859645 (noting that the new policy has vast global, political, and financial implications). In an interview, ICANN CEO Rod Beckstrom reasoned that the expansion was necessary to "increase competition in the domain name market." *Id.*; *see also* ICANN, *Draft Applicant Guidebook, v3*, 2-1 (Oct. 2, 2009), http://www.icann.org/en/topics/new-gtlds/draft-rfp-clean-04oct09-en.pdf (detailing that all new gTLD applicants will undergo an initial evaluation and those who do not pass all necessary elements will be subject to further evaluation).

[52] *See* Carlton, *supra* note 39, at 13. ICANN determined the following:

> An increase in the number of gTLDs increases the number of alternatives available to customers, and thus offers the potential for increased competition, reduced prices, and increased output. The availability of new gTLDs also offers increased opportunities for registries and registrars to develop innovative services or business models that could provide significant opportunities for increases in consumer welfare.
>
> . . . .
>
> A variety of innovations are likely to be facilitated by expansion of the number of gTLDs. For example: A gTLD dedicated to serving the financial services industry might require registrants to provide secure transactions. The certification provided in the gTLD name thus provides valuable information to consumers who desire secure financial transactions over the Internet.

Many private organizations and entities have expressed interest in establishing their own gTLD under this new policy.[53] However, many organizations and scholars have also criticized the proposed plan, mainly because of the expansion's uncertain future and also potential intellectual property problems that may arise as a result of the expansion.[54] Specifically, many U.S. businesses recognize that such a Wild West-like expansion to domain name registration could potentially create legal problems related to trademark protection, consumer fraud, and cybersquatting.[55] To date, ICANN does not have a policy in place to

---

Id. at 6, 13 (bulleted format omitted); *see also* Beckstrom, *supra* note 45. Beckstrom states the following:

> The Internet has historically thrived whenever the system is opened up further to allow users to express their creativity and innovation. We are now working on opening up the top-level domains so that not only nations but also other peoples and groups can have a unique identity on the Internet.
>
> . . . .
>
> The original limitations on domain names had to do with the limited capabilities of computers and networks in decades gone by. Given today's advances in power, bandwidth and memory, the time has clearly come to open up the myriad possibilities in Internet naming.

Id.; *see New gTLD Program Explanatory Memorandum*, ICANN, 1 (May 30, 2009), https://www.icann.org/en/topics/new-gtlds/three-character-30may09-en.pdf. With this new policy

> expansion will allow for more innovation, choice and change to the Internet's addressing system, now constrained by only 21 generic top-level domain names. In a world with 1.5 billion Internet users—and growing—diversity, choice and competition are key to the continued success and reach of the global network.

Id. See generally Mike Sachoff, *ICANN Approves Expansion of Domain Names*, WEBPRONEWS (June 26, 2008), http://www.webpronews.com/topnews/2008/06/26/icann-approves-expansion-of-domain-names ("New generic Top Level Domains . . . will open up the Internet and make it look as diverse as the people who use it.").

[53] *See* Beckstrom, *supra* note 45. Beckstrom shared that His Majesty King Goodwill Zwelithini kaBhekuzulu, the chief of the Zulu tribe, sent ICANN a letter declaring his interest to register the dot-zulu domain name. *Id.* His Majesty wrote that the dot-Zulu domain name could link the entire world Zulu community. *Id.* Beckstrom added that New York City and the city of Berlin have also inquired into registering their own domain names. *Id.*; *see also* Mike Rodenbaugh, *Abusive Domain Registrations: ICANN Policy Development Efforts (and Lack Thereof)*, 940 PLI/Pat 175, 182 (2008) ("It is expected there will be more than 100 applications early next year, and ICANN Staff has reported that there is no technical reason that the 'root zone' of the internet could not support more than 60 million new TLDs!").

[54] *See* Farley, *supra* note 51, at 627 ("[B]ecause the new gTLD policy imports certain concepts and doctrines from trademark law in an effort to address architecture issues, this policy would result in long-term problems both for domain names and for trademark law jurisprudence.").

[55] *See* Reinhardt Krause, *Control of Internet is at Issue ICANN Renewal Up Europe Doesn't Want the U.S. Commerce Dept. in Charge of Oversight Body*, INVESTOR'S BUSINESS DAILY, Sept.

deter, prevent, or address abusive domain name registrations in existing or future TLDs.[56] If the Internet does experience the projected increase in domain name registrations as a result of ICANN's new domain name policy, courts may be burdened with an increase of legal disputes stemming from the policy.[57] This new policy has resulted in a number of common domain name disputes entering courtrooms across the United States.[58]

E. Typical Domain Name Registration Disputes

Domain name disputes fall under a number of distinct categories, but they all have one commonality: they exploit the increasingly popular DNS and registration of a finite number of domain names.[59]

1. Cybersquatters

The most litigated and prevalent domain name registration dispute is known as cybersquatting.[60] A cybersquatter is one who knowingly

---

22, 2009, at A04 ("Many U.S. industry groups, though, are concerned about ICANN's plans to expand top-level domains and Web addresses. They fret about trademark protection, consumer fraud and other issues if a Wild West-like market is created for Web addresses."); Anick Jesdanun, *ICANN Mulls Database for Trademark Holders*, LAW.COM (July 17, 2009), http://www.law.com/jsp/cc/PubArticleFriendlyCC.jsp?id=1202432313887 ("[M]any companies fear that if ICANN suddenly adds 500 suffixes to the system, they'd have to register their brands in each domain. Administrative costs could balloon if those suffixes all have different rules for trademark claims."); Andrew Noyes, *ICANN's Domain Name Expansion Plans Draw Attention*, CONGRESS DAILY, Sept. 23, 2009, *available at* 2009 WLNR 18765545. Corporations such as

> Nike, Verizon and Marriott along with trade groups like the National Association of Manufacturers and U.S. Chamber of Commerce have built up opposition to the Internet Corporation for Assigned Names and Numbers plan, claiming that it could exacerbate cyber-squatting, fraud, and consumer confusion while forcing trademark owners to spend more money to defend their brands.

Id.; *see also* Carlton, *supra* note 39, at 8 ("[T]he Association of National Advertisers states that new gTLDs will generate higher 'costs of brand management and create new opportunities for others to infringe, phish, and engage in other deceptive practices. As a result, brand owners and consumers will be net losers.'"); *infra* Part II.E (discussing the typical domain name disputes prevalent today).

56 Rodenbaugh, *supra* note 53, at 184.

57 *See* Chatterjee, *supra* note 27, at 69 (focusing on the fact that as commerce on the Internet grows, courts will be forced to apply traditional legal tenets to a new medium).

58 *See generally* Adam Chase, Note, *A Primer on Recent Domain Name Disputes*, 3 VA. J.L. & TECH. 3 (Spring 1998), *available at* http://www.vjolt.net/vol3/issue/vol3_art3.pdf (detailing a number of influential domain name dispute cases).

59 *See* Chatterjee, *supra* note 27, at 70 (recognizing that as the Internet grows in volume there are less domain names available and thus disputes over domain names were inevitable).

registers a domain name using the trademark or name of a company strictly for the purpose of selling back that domain name to the legitimate owner for a price.[61] Cybersquatters attempt to profit through the bad faith use of a trademark in which they are not the rightful owners.[62]

One of the earliest cybersquatting cases, *Panavision International, L.P. v. Toeppen*, is illustrative of the unscrupulous nature of cybersquatters.[63] Panavision manufactured motion picture equipment and registered trademarks under the names "Panavision" and "Panaflex."[64] In December 1995, Panavision attempted to register the domain name Panavision.com, but could not do so.[65] An Illinois man, David Toeppen, already registered Panavision.com along with over two hundred other domain names for famous companies such as Delta Airlines, Neiman Marcus, Eddie Bauer, and Lufthansa.[66] The courts found that Mr.

---

[60] *See* Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 680 (9th Cir. 2005). The court explained that:

> [C]ybersquatting occurs when a person other than the trademark holder registers the domain name of a well known trademark and then attempts to profit from this by either ransoming the domain name back to the trademark holder or by using the domain name to divert business from the trademark holder to the domain name holder.

Id. (quoting DaimlerChrysler v. The Net Inc., 388 F.3d 201, 204 (6th Cir. 2004)); *see also* Lucas Nursery & Landscaping, Inc. v. Grosse, 359 F.3d 806, 809 (6th Cir. 2004). Cybersquatters are those who do as follows:

> (1) 'register well-known brand names as Internet domain names in order to extract payment from the rightful owners of the marks;' (2) 'register well-known marks as domain names and warehouse those marks with the hope of selling them to the highest bidder;' (3) 'register well-known marks to prey on consumer confusion by misusing the domain name to divert customers from the mark owner's site to the cybersquatter's own site;' (4) 'target distinctive marks to defraud consumers, including to engage in counterfeiting activities.'

Id. (quoting S. REP. NO. 106-140, at 5–6 (1999)).

[61] J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:77 (4th ed. 2009) (noting that most cybersquatters have no intention of using the domain name as an active website).

[62] *See* Harrods Ltd. v. Sixty Internet Domain Names, 110 F. Supp. 2d 420, 426 (E.D. Va. 2000). Cybersquatting is defined as the "registering, trafficking in, or using [domain names] similar to trademarks *with the bad-faith intent to profit* from the goodwill of the trademarks." *Id.* (citations and internal quotations omitted).

[63] 141 F.3d 1316 (9th Cir. 1998).

[64] *Id.* at 1319.

[65] *Id.*

[66] *Id.* Toeppen offered to settle the matter if Panavision would pay him $13,000 in exchange for the domain name. *Id.* Further, Toeppen offered to not register any other infringing domain names. *Id.*; *see also* Intermatic, Inc. v. Toeppen, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996) ("Toeppen has registered approximately 240 Internet domain names

Toeppen was a shrewd businessman operating as a cybersquatter.[67] The Ninth Circuit concurred with the lower court's ruling and held that Toeppen's actions violated a number of federal trademark laws.[68]

Similar types of cybersquatting still occur today.[69] Nevada gubernatorial candidate Rory Reid recently fell victim to a cybersquatter and chose to pay $10,000 to the cybersquatter for the Internet domain name roryreid.com.[70] Although cybersquatters may be shrewd entrepreneurs in their own eyes, Congress has enacted legislation to illegalize such conduct.[71] Additionally, cybersquatters are not the only predators causing havoc on the Internet and the DNS.[72]

---

without seeking the permission from any entity that has previously used the names he registered, because he contends that no permission was or is necessary.").

[67] *See Panavision Int'l, L.P.*, 141 F.3d at 1319 ("Toeppen then offered to 'settle the matter' if Panavision would pay him $13,000 in exchange for the domain name. . . . Toeppen has attempted to 'sell' domain names for other trademarks such as intermatic.com to Intermatic, Inc. for $10,000 and americanstandard.com to American Standard, Inc. for $15,000."); *Intermatic, Inc.*, 947 F. Supp. at 1230 ("One of Toeppen's business objectives is to profit by the resale or licensing of these domain names, presumably to the entities who conduct business under these names.").

[68] *Panavision Int'l, L.P.*, 141 F.3d at 1327 (affirming "the district court's summary judgment in favor of Panavision under the Federal Trademark Dilution Act, 15 U.S.C. § 1125(c)" and holding that "Toeppen made commercial use of Panavision's trademarks and his conduct diluted those marks"); *see also Intermatic, Inc.*, 947 F. Supp. at 1241. The court held the following:

> Pursuant to 15 U.S.C. § 1125(c) . . . Toeppen, and his officers, agents, servants, employees, and attorneys, and those persons in active concert or participation with them who receive actual notice of this final judgment and permanent injunction are hereby permanently enjoined from taking any action to prevent Intermatic from obtaining the Internet domain name, "intermatic.com", and are permanently enjoined from asserting any further interest in "intermatic.com" domain name . . . .

Id. (bulleted format omitted).

[69] *E.g.*, Frank Geary, *Reid's Online Site Up, in Race: Candidate Pays for Roryreid.com*, LAS VEGAS REVIEW-JOURNAL, Sept. 20, 2009, *available at* 2009 WLNR 18547790.

[70] *Id.* Reid chose to pay the cybersquatter's price because the $10,000 asking price was less than the cost of litigating the matter. *Id.* Also, Reid's legal team noted that any time a party enters into arbitration or litigation there is risk involved and Reid did not want to deal with that risk. *Id.*

[71] *See infra* Part II.F.1–3 (addressing Congress's attempts to criminalize cybersquatting).

[72] *See infra* Part II.E.2–6 (documenting the numerous other forms of domain name registration abuse besides cybersquatting).

2. Cyberparasites

Cyberparasites, like cybersquatters, expect to reap financial benefits from their actions.[73] However, unlike cybersquatters, cyberparasites anticipate their financial gain through the active use of a domain name.[74] There are two types of tactics employed by cyberparasites.[75] First, in some cases one party registers another competitor's famous name.[76] In the alternative, a party registers a mark that is remarkably similar to an official mark, or may register a commonly mistyped or misspelled version of a famous name.[77] The registration of domain names that closely resemble those of popular domain names but are mistyped or misspelled is generally known as typosquatting.[78] One emblematic example is 1800contacts.com, an online retailer of contact lenses. If the consumer enters 18oocontacts.com, 18000contacts.com, or 1888contacts.com the consumer arrives at a typosquatter domain site that is designed to lead him or her into buying lenses from a competing seller.[79] These typosquatting sites are known as ad parking sites, and typosquatters make advertising money when users, who intended to go to 1800contacts.com, click on sponsored links for other contact lens sellers.[80] Although these types of domain name disputes involve arguably deceptive means to profit, some domain name disputes arise out of legitimate name ownership disputes.

---

[73] Chatterjee, *supra* note 27, at 73 (positing that cyberparasites, like cybersquatters, plan to profit from their illegal activities).

[74] *Id.*

[75] *See* Comp. Exam'r Agency, Inc. v. Juris, Inc., No. 96-0213-WMB (CTx), 1996 WL 376600, at *1 (C.D. Cal. May 22, 1996).

[76] *Id.* In this case, Comp. Examiner Agency, Inc. illegally registered second level domain name juris.com, which happened to be a registered trademark belonging to Juris, Inc. *Id.* Comp. Examiner Agency, Inc. posted advertisements for their products and services on the illegally registered domain name site, which were in direct competition with Juris, Inc. *Id.*

[77] *See* Steve DelBianco & Braden Cox, *ICANN Internet Governance: Is It Working?*, 21 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 27, 33 (2008) (calculating that almost half of all Internet users choose to type the domain name of a website directly into their browser's address bar and as such misspellings are inevitable).

[78] *Id.* DelBianco and Cox explain that typosquatting is the registration of domain names that are spelled incorrectly but bear a resemblance to already established popular website. *Id.* If an Internet user does mistakenly misspell the domain name, they may end up at a typosquatter's website. *Id.* Usually at such a site Internet users will find advertisements for products or services that directly compete with the legitimate site. *Id.*

[79] *Id.* at 34. Sedo, the current leader in "parking" domain names, uses different variations of the 1800contacts.com domain name to generate their advertising revenue when users mistakenly click on their sponsored links leading them to other contact lens vendors. *Id.*

[80] *Id.*

3. Cyber Twins

When a domain name holder and the challenger have a legitimate claim to a domain name, they are known as cyber twins.[81] More often than not, cyber twin cases are the most difficult for courts to decide because in the absence of a domain name dispute, both parties would otherwise likely be able to enjoy concurrent use of the name under traditional trademark law.[82] In *Indian Farmers Fertiliser Cooperative Ltd. v. International Foodstuffs Co.*, the World Intellectual Property Organization ("WIPO") Arbitration and Mediation Center heard argument over the domain name iffco.com.[83] The defendant properly registered the iffco.com domain name, but the complainant had other domain names related to iffco.com and had a reasonable interest in that particular domain name.[84] Although the complainant alleged that the defendant was diverting Internet users to its own website, the Arbitration Center dismissed the case because the complainant failed to prove any "bad faith" on the part of the defendant, despite the fact that both parties had a legitimate interest in the domain name.[85]

4. Land-Grab

A parallel abuse of the domain name registration system, called a land-grab, may occur whenever a new TLD is released. Internet speculators, much akin to those who homesteaded the western United States during the mid- to late-nineteenth century, register hundreds or even thousands of names in the new domain in hopes of locking up

---

81 Chatterjee, *supra* note 27, at 74.

82 *Id.* "The cases involving cyber twins are the most difficult ones, because, but for the domain name dispute, the law of trade mark and unfair competition might otherwise allow each party to enjoy concurrent use of the name." *Id.*; *see also* Sun Microsystems, Inc. v. Astro-Med, Inc., No. C-95-20602-JW, 1996 WL 369100, at *1 (N.D. Cal. Apr. 1, 1996) (exhibiting a fight over the trademarked name "SUNDANCE" in which both parties have a legitimate claim to such a use).

83 Indian Farmers Fertiliser Coop. Ltd. v. Int'l Foodstuffs Co., WIPO Case No. D2001-1110, § 2 (WIPO Jan. 4, 2002), http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-1110.html.

84 *Id.* at § 4; Chatterjee, *supra* note 27, at 74. The Arbitration Center held that "[t]he defendants had registered the domain name ‹ iffco.com› [sic] and had been using it with good faith." *Id.*

85 Chatterjee, *supra* note 27, at 74. The case was dismissed "as both the parties had legitimate interest in the domain name and the complainant had failed to prove 'bad faith' on the part of the defendant." *Id.*

names similar to those of legitimate businesses and organizations.[86] Then, for financial gain, the speculators hold the domain names ransom from the legitimate owner of the names or use them for typosquatting and ad parking.[87]

The most recent occurrence of a land-grab occurred when the .eu top-level domain name was created for Europe.[88] Opportunistic registrants quickly registered names that legitimate businesses and organizations already held in other top-level domains.[89] In response EURid, the non-profit organization in charge of operating the .eu registry, suspended 74,000 .eu domain names and sued four hundred registrars for breach of contract.[90]

5. Domain Sharking/Tasting/Kiting

Domain name sharking, tasting, or kiting are all synonymous with a certain type of domain name registration abuse. Under these tactics, speculators look for sites where they can place or "park" ads to take advantage of the five-day grace period between the time a new domain name is initially registered and the time when the registration fee must be paid.[91]

In May 2006, out of thirty five million domain name registrations, approximately 2.7 million, or 7.7%, of registered names were purchased.[92] Domain name speculators register huge numbers of

---

[86] *See* DelBianco & Cox, *supra* note 77, at 35 (instructing that in a typical land-grab scenario violators will register thousands of new names in the new domain in the hopes of locking up sites similar to those of functioning businesses and organizations).

[87] *Id.* (detailing how domain name speculators demand a ransom or use the domain names for typesquatting and ad parking).

[88] *Id.*

[89] *Id.*; *see also* GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF THE INTERNET § 8.02 (Aspen 2010) (stating that there have been substantial difficulties with Internet speculators and misunderstandings of the registration process surrounding the unveiling of the .eu top-level domain).

[90] Roland Buck, *EURid Accuses Registrars of Stockpiling 74,000 .eu Domain Names*, DOMAIN NEWS (June 18, 2008), http://www.domainnews.com/en/eurid-accuses-registrars-of-stockpiling-74000-.eu-domain-names.html. EURid accused "400 US based registrars of stockpiling over 74,000 .eu domain names . . . . [and] registering them speculatively for resale." *Id*.

[91] DelBianco & Cox, *supra* note 77, at 35 (detailing the typical ad parking procedure conducted by Internet speculators).

[92] Bob Parsons, *35 Million Names Registered in May. Only 8% of Registrations Were Paid. 32 Million Were Part of a Scam. It's Called "Domain Kiting."*, BOBPARSONS.ME (June 21, 2006), http://www.bobparsons.me/118/35-million-names-registered-only-registrations-paid-32-part-scam-called-domain-kitinG.html. Internet statistics show that

> [j]ust over 35 million names were registered for the month of May. Of those just over 2.7 million were permanent registrations. That means

domain names that they believe may be profitable and then statistically track how many accidental visits each site receives.[93] If a site generates little traffic during the grace period, the speculator lets the domain name lapse without paying the registration fee.[94] Recently, ICANN passed a resolution to eliminate domain tasting, but no further action has been pursued beyond that.[95]

6. Reverse Domain Name Hijacking

The final notable domain name registration dispute is known as "reverse domain name hijacking." This occurs in cases where the complainant attempts to overextend the scope of their famous name by using one of the domain dispute resolution remedies in bad faith.[96] Ultimately, the existence of a cause of action for reverse domain name hijacking requires trademark owners to exercise caution to avoid filing frivolous claims in their domain name registration disputes.[97] As

---

> that 92.3% of all domain names registered were part of a scam now known as domain kiting. These names were kept off of the market, they were used to generate search engine revenue—AND BECAUSE OF A LOOPHOLE ICANN REFUSES TO ELIMINATE—those 32.3 million names were used without being paid for.

Id.

93 *See* DelBianco & Cox, *supra* note 77, at 35 (noting that of the 35 million domain name registrations in April 2006, only 2 million were permanently purchased and that a large portion of the remaining 33 million were part of a sharking scheme); Elizabeth M. Flanagan, Note, *No Free Parking: Obtaining Relief from Trademark-Infringing Domain Name Parking*, 98 TRADEMARK REP. 1160, 1166 (Sept.–Oct. 2008) (expressing that Internet users typically reach ad parked websites by either incorrectly guessing a domain name or because they commit typographical errors).

94 DelBianco & Cox, *supra* note 77, at 35. Alternatively, if the site generates a lot of traffic, the speculator may use it to park ads to generate revenue without having to expend any effort. *Id.* at 35–36.

95 Sachoff, *supra* note 52 (detailing ICANN's resolution seeking to eliminate domain tasting and prevent speculators from using the loophole of registration grace periods to see what names will be the most profitable).

96 Chatterjee, *supra* note 27, at 74 (articulating that the complainant in some cases will overextend their famous name); Ian L. Stewart, Note, *The Best Laid Plans: How Unrestrained Arbitration Decisions Have Corrupted the Uniform Domain Name Dispute Resolution Policy*, 53 FED. COMM. L.J. 509, 513 (2001). Reverse domain name hijacking is defined as the "bad faith . . . attempt to deprive a registered domain-name holder of a domain name." Stewart, *supra* (citation omitted). ICANN defined reverse domain name hijacking as "using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name." *Rules for Uniform Domain Name Dispute Resolution Policy*, ICANN, para. 1, 15(e), http://www.icann.org/en/udrp/udrp-rules-24oct99.htm (last visited Mar. 3, 2010) [hereinafter ICANN Rules].

97 *See* Hawes v. Network Solutions, Inc., 337 F.3d 377, 384 (4th Cir. 2003) (reasoning that the ACPA provides a very limited registrar liability that nullifies most suits against registrars); Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617,

suggested by the variety of domain name registration disputes and their increasing pervasiveness, Internet stakeholders enacted remedial measures to ensure the continued success and integrity of the DNS.[98]

F. Remedial Responses to Domain Name Disputes

During the early stages of the Internet and well before it became ubiquitous, courts simply applied traditional trademark law to this new technology.[99] However, traditional trademark law and its two underlying principles—(1) to prevent confusion in the public and (2) to protect the owner's investment in the mark—proved to be unwieldy and limiting in Internet domain name cases.[100] As a result, in 1995, the United States Congress amended the Lanham Act and passed the first federal statute addressing the intersection of trademark and Internet issues.[101] Subsequently, a number of remedial legislative measures have been enacted and applied in domain name disputes.[102]

---

625 (4th Cir. 2003) (stating that the reverse domain name hijacking provision of the ACPA protects domain name registrants from overreaching trademark owners); *see also* KENT D. STUCKEY ET AL., INTERNET AND ONLINE LAW § 7.07, ¶ [1][c], (2009) (cautioning trademark owners to prudently employ the ACPA because under certain circumstances domain name registrants can counter with a reverse domain name hijacking suit).

98 *See* Kathrun Miller Goldman & Cynthia Blake Sanders, *Intellectual Property Issues for You and Your Small Business*, 1 ANN.2001 ATLA-CLE 1025 (2001) (providing that besides traditional trademark actions, two additional remedies were created to allow a trademark owner protection against persons who register a domain name using the trademark).

99 Howard, *supra* note 39, at 647 (noting how courts have toiled in dealing with trademark abuses in domain names, first by applying traditional trademark infringement and dilution law).

100 *See* Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 871 (9th Cir. 1999) ("We are the third panel of this court in just over a year faced with the challenging task of applying centuries-old trademark law to the newest medium of communication—the Internet."); *see also* Block, *supra* note 27, at 438 (explaining that there was no federal anti-dilution law prior to 1996 so trademark owners attempted to combat dilution through a variety of state laws); Howard, *supra* note 39, at 637–38 (analyzing that in early cases courts used traditional trademark law, like trademark infringement and later trademark dilution, to provide redress to mark owners).

101 Federal Trademark Dilution Act of 1995, Pub. L. No. 104-98, 109 Stat. 985 (1996) (codified as amended at 15 U.S.C. § 1051 et seq. (2002)); *see also* Elizabeth D. Lauzon, Annotation, *Validity, Construction, and Application of Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)*, 177 A.L.R. FED. 1, 1 (2002) (noting that the Amendment to the Lanham Act provided stronger remedies against cybersquatters).

102 *See infra* Part II.F. (detailing the passage and implementation of the FTDA, TDRA, ACPA, and the UDRP).

1. Federal Trademark Dilution Act

The Federal Trademark Dilution Act ("FTDA"), enacted January 16, 1996, created a federal cause of action for trademark dilution.[103] Congress specifically promulgated the FTDA to address Internet domain name registration issues.[104] Congress, however, failed to offer any notion of how trademark owners could prove dilution, which granted courts a huge amount of discretion in their decision making.[105] A plaintiff must prove four distinct factors for a court to find a violation of the FTDA: "(1) the mark is famous; (2) the defendant makes a commercial use of the mark in commerce; (3) the defendant's use began after the mark became

---

[103] Lanham Act § 43(c)(1), 15 U.S.C. § 1125(c)(1) (2006). The statute states the following:

> Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

Id. The statute then lays out the factors that courts should use to determine if a mark is distinctive and famous:

> (i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.
> (ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.
> (iii) The extent of actual recognition of the mark.
> (iv) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

Id. § 1125(c)(2)(A) (bulleted format modified); *see also* Acad. of Motion Picture Arts & Scis. v. Network Solutions, Inc., 989 F. Supp. 1276, 1279 (C.D. Cal. 1997) (noting that domain names must be affiliated to some commercialized goods or services of the registrant); Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1238 (N.D. Ill. 1996) (reiterating the statutory definition of dilution, which is "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion, mistake, or deception" (quoting Lanham Act § 45, 15 U.S.C. § 1127 (1999))).

[104] *See* 104 CONG. REC. S19312 (daily ed. Dec. 29, 1995) (statement of Sen. Patrick J. Leahy). Senator Patrick J. Leahy (D-Vt.) stated that the legislative history of the Act indicated that it was created to deal with domain name conflicts. *Id.* Senator Leahy declared "it is my hope that this antidilution statute can help stem the use of deceptive Internet addresses taken by those who are choosing marks that are associated with the products and reputations of others." *Id.*

[105] *See* Matthew S. Voss, *Ringling Bros.-Barnum & Bailey Combined Shows, Inc. v. Utah Division of Travel Development & Nabisco, Inc. v. PF Brands, Inc.*, 15 BERKELEY TECH. L.J. 265, 266 (2000) (commenting that the language of the Dilution Act may have provided guidance on how to determine if a trademark is sufficiently famous to deserve protection but remains silent on how to actually prove dilution).

famous; and (4) the defendant's use of the mark dilutes its quality by diminishing its capacity to identify and distinguish goods and services."[106]

One of the early cases in which a plaintiff claimed an FTDA violation occurred in *ActMedia, Inc. v. Active Media International Inc.*[107] The defendant's registration of the name "actmedia.com" without the authorization of the plaintiff, who conducted business under the name Actmedia since 1972 and registered the trademark, was ruled to be a violation of the FTDA.[108] Judging the application of the FTDA in cases like *ActMedia*, many courts and legal scholars saw the FTDA as an adequate first attempt to legally address domain name registration disputes.[109] However, scholars ultimately determined that the FTDA missed its intended mark because it failed to adequately protect trademark owners.[110] Therefore, further legislation was needed to adequately preserve the domain name registration system.

2. Trademark Dilution Revision Act of 2006

Congress revised the prior FTDA in 2006 with the enactment of the Trademark Dilution Revision Act of 2006 ("TDRA").[111] This revision eliminated the requirement that a plaintiff must establish actual dilution to succeed in its claim and created instead the new "likelihood of

---

106 Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1324 (9th Cir. 1998).

107 No. 96C3448, 1996 WL 466357, at *1 (N.D. Ill. July 17, 1996).

108 *Id.* at *1–2 (holding that the defendant's reservation of the domain name violated 15 U.S.C. § 1125 because it was an unauthorized use and misappropriation of the plaintiff's trademark and also because the use of the mark constituted "false designation of origin").

109 Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1237–38 (N.D. Ill. 1996). The court reasoned that the new law "benefits only 'famous' trademarks." *Id.* at 1237. Furthermore,

> [u]nder the Act, the owner of a famous mark is only entitled to injunctive relief unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. The Act does not preempt state dilution claims. The Act specifically provides that noncommercial use of the mark is not actionable.

Id. at 1238 (citing 15 U.S.C. § 1125(c)(4)(B) (1994)).

110 *See* Howard, *supra* note 39, at 638, 643. Howard concluded that the FTDA had a major limitation. *Id.* at 638. Trademark infringement and dilution did not provide proper legal redress for the trademark owner. *Id.* As a result courts stretched the original intent of the law to try and incorporate domain names into traditional trademark law in the name of equity and justice. *Id.*

111 Trademark Dilution Revision Act of 2006, Pub. L. No. 109-312, 120 Stat. 1730 (2006); Perla M. Kuhn, *Trademarks as Competitive Tools-Obtaining and Protecting Them*, ASPATORE, at 1, 8, *available at* 2009 WL 534745.

dilution" standard.[112] To establish a prima facie case of dilution under the TDRA, a plaintiff must show that: "(1) the plaintiff is the owner of a mark that qualifies as a famous mark, (2) the mark is distinctive, (3) the defendant is making commercial use of the mark in interstate commerce, (4) defendant's use began after plaintiff's mark became famous, and (5) there is a likelihood of dilution."[113] However, federal courts interpreting this new standard have made it extremely challenging for plaintiffs to prove a likelihood of dilution.[114] Dilution can occur in two distinct ways, by "blurring" or by "tarnishment."[115] Presently, limited case law employing the likelihood of dilution standard exists; thus, the law continues to change and develop.[116]

3. Anticybersquatting Consumer Protection Act ("ACPA")

Congress also addressed the DNS issue when it passed the ACPA in 1999 as another amendment to the Lanham Act.[117] Courts read the ACPA to reach outside of what the FTDA and Lanham Act previously

---

[112] *See* Melvyn J. Simburg et al., *International Intellectual Property Law*, 41 INT'L LAW. 379, 386 (2007). The authors explained that the FTDA

> was a response to, and overrules, the Supreme Court's widely criticized holding in *Moseley v. V Secret Catalogue, Inc*., in which the Court, addressing the split among the lower courts over the more subjective "likelihood of dilution" standard, held that actual dilution was required in order for famous marks to qualify for injunctive relief under the FTDA.

Id. (citing Moseley v. V Secret Catalogue, Inc., 537 U.S. 418 (2003)); *see also* Jeremy M. Roe, Note, *The Current State of Antidilution Law: The Trademark Dilution Revision Act and the Identical Mark Presumption*, 57 DEPAUL L. REV. 571, 589 (2008) (claiming that the open-ended likelihood to dilute standard is open to judicial interpretation).

[113] 98 AM. JUR. PROOF OF FACTS 3D *Proof of Dilution of a Trademark* § 5 (2007).

[114] *See* Kuhn, *supra* note 111, at 20–21 (noting that courts interpreting the TDRA have yet to answer a number of questions including how much of a burden the plaintiff must bear in demonstrating the level of fame of its mark and the necessary degree of similarity between the plaintiff's mark and the diluting mark).

[115] *See* Simburg et al., *supra* note 112, at 387 (commenting that the TDRA provides greater certainty in determining when dilution has occurred by defining and differentiating between "blurring" and "tarnishment"). Dilution by blurring is defined as an "association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark." *Id.* (citation omitted). The definition of tarnishment is an "'association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.'" Roe, *supra* note 112, at 583 (citation omitted).

[116] *See generally Moseley*, 537 U.S. 418 (failing to answer how a plaintiff successfully proves a likelihood of dilution by blurring); Louis Vuitton Malletier S.A. v. Haute Diggity Dog, L.L.C., 507 F.3d 252, 267–68 (4th Cir. 2007) (ruling impliedly that the more famous the mark, the less likely that dilution by blurring will be determined); Kuhn, *supra* note 111, at 20 (proclaiming that the application of the TDRA is new and still evolving).

[117] Anticybersquatting Consumer Protection Act, 15 U.S.C. §§ 1114–1117, § 1125(d) (2006).

addressed.[118] Specifically, the ACPA provided two additional weapons for trademark owners to protect their trademarks that were previously unavailable: jurisdiction and statutory damages.[119] To present a successful claim under the ACPA, the complainant must plead that the violator had a bad faith intent to profit.[120] Further, the statute has nine

---

[118] *See* Porsche Cars N. Am., Inc. v. Porsche.Net, 302 F.3d 248, 260–61 (4th Cir. 2002). The court concluded that the promulgation of the ACPA

> eliminated any need to force trademark-dilution law beyond its traditional bounds in order to fill a past hole, now otherwise plugged, in protection of trademark rights.
>
> As the Second Circuit recently remarked, the ACPA "was adopted specifically to provide courts with a preferable alternative to stretching federal dilution law when dealing with cybersquatting cases."

Id. at 261–62 (quoting Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489, 497 (2d Cir. 2000)); *see also* Harrods Ltd. v. Sixty Internet Domain Names, 110 F. Supp. 2d 420, 426 (E.D. Va. 2000). The court claimed that the ACPA was not

> designed to combat domain name registrants utterly ignorant of certain existing trademarks, or those registrants with a good faith reason to believe that they have the right to register certain domain names. On the contrary, as its title reflects, the AntiCybersquatting Consumer Protection Act was designed to combat "cybersquatting" or "cyberpiracy," defined as "registering, trafficking in, or using similar to trademarks *with the bad-faith intent to profit* from the goodwill of the trademarks."

Id. (quoting H.R. REP. NO. 106-412 (1999) and citing S. REP. NO. 106-140 (1999)); *see also* S. REP. NO. 106-140, at 4, 17 (1999). The report provides that the legislative purpose of the ACPA was

> to protect consumers and American businesses, to promote the growth of online commerce, and to provide clarity in the law for trademark owners 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—a practice commonly referred to as "cybersquatting."

Id. at 4. "This section [was intended] to encourage domain name registrars and registries to work with trademark owners to prevent cybersquatting." *Id*. at 17.

[119] *See* Gore, *supra* note 29, at 203. Benefits of the ACPA include the following:

> First, the ACPA provides for *in rem* jurisdiction against the domain name itself, which alleviates trademark owners' difficulties in locating the domain name's registrant, since many cybersquatters register domain names under aliases and use false information to avoid being identified. Second, in regards to remedies, the ACPA allows a court to award injunctive relief barring the defendant's further use of the domain name, cancellation or transference of the domain name to the plaintiff, actual damages and profits, attorneys' fees, and statutory damages in an amount between $1,000 and $100,000 per domain name.

Id. (internal citations omitted); *see also* Brenda R. Sharton, *Domain Name Disputes: To Sue or Not to Sue*, 44 B. B.J., Sept./Oct. 2000, at 10, 11.

[120] 15 U.S.C. § 1125(d)(1)(A)(i) (2006) ("A person shall be liable in a civil action . . . if . . . that person . . . has a bad faith intent to profit from that mark . . . .").

non-exclusive factors for determining a person's bad faith intent to profit.[121]

In *Lockheed Martin Corp. v. Network Solutions, Inc.*,[122] Lockheed Martin brought claims of trademark infringement and dilution under the ACPA against a domain name registrar for failure to protect trademarks and prevent the registration of a number of domains using the trademark names owned by Lockheed Martin.[123] The district court held that the registrar did not incur cybersquatting liability by registering and maintaining domain names that allegedly infringed the owner's trademarks.[124] Due to these problems, ICANN developed its own

---

121 *Id.* § 1125(d)(1)(B)(i). The nine non-exclusive factors considered are:

> (I) the trademark or other intellectual property rights of the person, if any, in the domain name;
>
> (II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
>
> (III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
>
> (IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
>
> (V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, 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;
>
> (VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;
>
> (VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;
>
> (VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and
>
> (IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c)(1) of this section.

Id.

122 141 F. Supp. 2d 648 (N.D. Tex. 2001).

123 *Id.* at 649–50.

124 *Id.* at 655. In its opinion the court stated the following:

remedial system in addition to Congress's efforts to create legislation to improve the domain name system and to minimize domain name disputes.[125]

4. Uniform Domain Name Dispute Resolution Policy

ICANN adopted the Uniform Domain Name Dispute Resolution Policy ("UDRP") on October 24, 1999.[126] The UDRP provides for electronic arbitration of domain name disputes between trademark owners and domain name registrants.[127] The UDRP exists as a "fast-track" alternative to traditional court proceedings.[128] One benefit of the UDRP is that in order to register a domain name, the registrant has to agree to comply with the UDRP, which provides some redress for disputes that may arise.[129] However, the UDRP is limited in that it only

> It is quite understandable that Congress did not cause defendant as a domain name registrar, or as keeper of the registry, to be subject to civil liability under § 1125(d). . . . Defendant simply could not function as a registrar, or as keeper of the registry, if it had to become entangled in, and bear the expense of, disputes regarding the right of a registrant to use a particular domain name.

Id.

125 *See* Rohrer, *supra* note 26, at 573 (outlining ICANN's adoption of the Uniform Domain Name Dispute Resolution Policy as a mandatory administrative proceeding that governs all domain name registrants).

126 *Id*.

127 *See* Brett R. Harris et al., *PIERCING THE REGISTRANT'S VEIL: Trademark Infringement on the Internet, Identifying and Pursuing Infringers, and the Pros and Cons of Proxy Domain Name Registration*, N.J. LAW., June 2009, at 46, 47 (explaining that ICANN provides the UDRP as an arbitration proceeding to resolve a trademark infringement based on the domain name itself and not the content found when one visits the website connected to the domain name); *see also* Goldman & Sanders, *supra* note 98, at II; *Uniform Domain Name Dispute Resolution Policy*, ICANN, ¶ 1, http://www.icann.org/en/udrp/udrp-policy-24oct99.htm (last visited Mar. 3, 2010) [hereinafter ICANN Policy]. ICANN incorporates the UDRP into the domain name Registration Agreement. ICANN Policy, *supra*, ¶ 1. Within that agreement there are terms and conditions that dictate any disputes over domain name registrations. *Id.*

128 Rodenbaugh, *supra* note 53, at 179 (elucidating that ICANN privately formulated the UDRP as a fast-track remedy for trademark cybersquatting that avoided court actions to recover misappropriated names); Nicole K. McLaughlin, *A Warning to Overreaching Trademark Owners: ACPA Gives Domain Name Registrants Cause of Action*, THE L. INTELLIGENCER, Jan. 3, 2002, at 5, *available at* 2002 WLNR 15048896 (expounding that the UDRP maintains authority in disputes between potential cybersquatters and third-party trademark owners); *see also* Geary, *supra* note 69 (stating that, typically, a UDRP proceeding resolves such disputes within two to three months).

129 *See* Chatterjee, *supra* note 27, at 77 (noting that domain name registrants are required to avail themselves to a mandatory administrative proceeding in the event of any domain name disputes). The ICANN approved resolution providers are the World Intellectual Property Organisation (WIPO), National Arbitration Forum (NAF), Centre for Public Resources Institute for Dispute Resolution (CPRIDR), eResolution Consortium (eRes), and

addresses the .com, .net, and .org TLDs.[130] Furthermore, the UDRP only covers claims that the registrant's domain name infringes on a trademark.[131]

To prevail under the UDRP, the complainant must prove that the domain name is: (1) identical or confusingly similar to the complainant's trademark; (2) that the domain name registrant has no legitimate interests in the domain name; and (3) that the domain name has been registered and is being used in bad faith.[132] The UDRP formula for determining bad faith appears to be a close relative to the nine factor bad faith test set forth in the ACPA.[133] A panel of one or three decision-makers hears an UDRP proceeding, and then submits a written decision as to the registration of the disputed domain name.[134] The panel members employ the rules of procedure established by ICANN and operate under any principles of law deemed necessary.[135] According to

---

the Asian Domain Name Dispute Resolution Centre (ADNDRC). *Id.*; s*ee also* ICANN Policy, *supra* note 127, ¶ 4 (explaining that all domain registrants automatically avail themselves to UDRP proceedings to resolve any domain name disputes). *See generally* ICANN Rules, *supra* note 96 (outlining the rules of the UDRP proceedings).

130 *See* Wal-Mart Stores, Inc. v. wallmartcanadasucks.com, WIPO Case No. D2000-1104 (WIPO Nov. 23, 2005), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1104.html (ruling that the UDRP has a small scope); *see also* Goldman & Sanders, *supra* note 98, at II.

131 *See* Stephen J. Ware, *Domain-Name Arbitration in The Arbitration-Law Context: Consent to, and Fairness in, the UDRP*, 6 J. SMALL & EMERGING BUS. L. 129, 146 (2002) (explaining that UDRP proceedings only cover claims that a registrant's name infringes upon a trademark or a servicemark).

132 Goldman & Sanders, *supra* note 98, at II (satisfying these three elements of the UDRP allows a rightful domain name owner to reclaim or cancel an infringing name).

133 *See* Cnty. Bookshops Ltd. v. Guy Loveday, WIPO Case No. D2000-0655, at 4 (WIPO Sept. 22, 2000), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0655.html (analyzing a dispute by determining whether the domain name at issue is identical or confusingly similar to a trademark or servicemark in which the complainant has rights); *see also* Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 359, 379 (2003) (explicating that although the U.S. Government wandered from the exact UDRP formula with the passage of the ACPA, overall the ACPA's bad faith test parallels the terms in the UDRP that should trigger a domain name transfer). *Compare* 15 U.S.C. § 1125(d)(1)(B)(i) (2006) (detailing the ACPA's nine factor bad faith test), *with* ICANN Policy, *supra* note 127, ¶ 4(a)–(b) (laying out the criteria for determining when a valid dispute exists and when bad faith registration has occurred).

134 Lockheed Martin Corp. v. Network Solutions, Inc., 141 F. Supp. 2d 648, 651–52 (N.D. Tex. 2001); *see also* Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745, 747 (E.D. Va. 2001) (stating that the panel may consist of either one or three members to conduct the inquiry).

135 *See* Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 624 (4th Cir. 2003) ("The UDRP is intended to provide a quick process for resolving domain name disputes by submitting them to authorized panels or panel members operating under rules of procedure established by ICANN and under 'any rules and principles of law that [the panel] deems applicable.'") (quoting ICANN Policy, *supra* note 127, ¶ 15(a)).

ICANN's most recently released statistics, over 7700 UDRP disputes were resolved in the less than five years of UDRP proceedings.[136]

In March 2009, ICANN formed the Implementation Recommendation Team ("IRT") to seek solutions to any potential risks to trademark holders upon the release of the new gTLD policy.[137] In its work, the IRT analyzed current trademark protections and responded with new proposals to aid current trademark holders.[138] The proposal of these new measures demonstrated the divide between existing remedial measures and the risk for future abuses with the lifting of restrictions on domain name registrations. Following the advent of the Internet and its ubiquitous rise, a disconnect developed between trademark law and domain name policy.[139]

III. ANALYSIS

In the next Part of this Note, Part III.A will first review the successes and shortcomings of the remedial measures for domain name disputes provided for by the FTDA, TDRA, ACPA, and UDRP. Next, Part III.B analyzes ICANN's five primary proposed solutions to limit domain name problems that may accompany the release of the new gTLD policy.

A. Lackluster Remedial Measures for Domain Name Disputes

As discussed in Part II.F of this Note, four major remedial measures currently govern domain name disputes: the FTDA, TDRA, ACPA, and

---

136 *See* Laurence R. Helfer, *Whither the UDRP: Autonomous, Americanized, or Cosmopolitan?*, 12 CARDOZO J. INT'L & COMP. L. 493, 494–95 (2004) (recognizing that since the UDRP's inception more than 7000 disputes have been decided while only a few hundred have been formally adjudicated in national courts in the same period); *see also Archived Statistical Summary of Proceedings Under Uniform Domain Name Dispute Resolution Policy*, ICANN (May 10, 2004), http://www.icann.org/en/udrp/proceedings-stat.htm (expounding upon the graphical analysis shows that as of May 10, 2004, 7790 UDRP proceedings were disposed by decision).

137 *See Introduction: Implementation Recommendation Team (IRT)*, ICANN, 1 (Apr. 24, 2009), http://www.icann.org/en/topics/new-gtlds/irt-draft-report-trademark-protection-24apr09-en.pdf (indicating that the IRT was formed March 6, 2009, by ICANN Board resolution to assess risks of the new gTLD policy).

138 *Id.* at 2–3 ("[T]he IRT was constrained to prioritize the list of proposals . . . which are hoped may make available solutions to address some of the immediate concerns of the stakeholders . . . ."); *see An Open Letter from the IRT Introducing Our Work*, ICANN, 2 (May 29, 2009), http://www.icann.org/en/topics/new-gtlds/irt-final-report-trademark-protection-29may09-en.pdf [hereinafter IRT Letter] (reporting the IRT's goal "to provide . . . 'a tapestry of globally-effective solutions' which . . . will help reduce the incidence and severity of trademark abuse in the new gTLDs").

139 *See* Farley, *supra* note 51, at 632 (noting that although law and technology have grown closer through time, trademark law and domain names remain incongruent).

the UDRP.[140] Each measure provides some sort of redress to victims of domain name registration abuse.

1. FTDA[141]

The federal government, in an initial attempt to address domain name registration disputes, passed the FTDA to prohibit the dilution of commercially used and famous trademarks.[142] For a plaintiff to prevail, the statutory language states that the trademark must be "famous;" however, in practice, proving a mark to be "famous" is a rather difficult task.[143] Numerous courts have concluded that to be "famous" under the traditional dilution standard, a trademark must be eminent and well known.[144] In addition to the lofty famous standard, courts have criticized the statutory requirement that any infringing use must be "commercial."[145] Under the commercial use umbrella, proof of an FTDA violation requires that the domain names must be attached to some

---

[140] *See supra* Part II.F (addressing the four major remedial measures governing domain name disputes).

[141] *See supra* Part II.F.1 (detailing the promulgation of the FTDA and some of the documented violations of the Act).

[142] *See supra* note 103 and accompanying text (covering the factors used in determining dilution of a trademark).

[143] *See supra* note 103 (outlining the high mark that a plaintiff must reach to warrant the "famous" standard); *see also* Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 875 (9th Cir. 1999) (interpreting the high standard of famousness as being "invented and reserved for a select class of marks—those marks with such powerful consumer associations that even non-competing uses can impinge on their value"); Howard, *supra* note 39, at 647 (noting that the first requirement, that the mark be famous, is a very subjective and high standard to meet).

[144] *See Avery Dennison Corp.*, 189 F.3d at 875 (noting that a mark must be both prominent and renowned to be judged as famous under trademark dilution) (citing I.P. Lund Trading ApS v. Kohler Co., 163 F.3d 27, 46 (1st Cir. 1998)) (quoting 3 J. Thomas McCarthy, TRADEMARKS & UNFAIR COMPETITION § 24.91 (2d ed. 1984)).

[145] *See* 15 U.S.C. § 1127 (2006). The statute synonymously defines commercial or use in commerce as "the bona fide use of a mark in the ordinary course of trade." *Id.* A mark is deemed to be in use in commerce

> (1) on goods when—
>
> (A) it is placed in any manner on the goods or their containers or the displays associated therewith or on the tags or labels affixed thereto, or if the nature of the goods makes such placement impracticable, then on documents associated with the goods or their sale, and
>
> (B) the goods are sold or transported in commerce, and
>
> (2) on services when it is used or displayed in the sale or advertising of services and the services are rendered in commerce . . . .

Id.; *see also Avery Dennison Corp.*, 189 F.3d at 880 ("Commercial use under the Federal Trademark Dilution Act requires the defendant to be using the trademark as a trademark, capitalizing on its trademark status.").

commercial goods or services of the domain name registrant.[146] Courts quickly recognized the possible injustice of not holding the registration of a domain name itself as a commercial use and consequently began to stretch the original intent of the statute.[147] This extrapolation beyond the statutory language demonstrated that traditional trademark law of infringement and dilution had important limitations.[148] Due to the FTDA's shortcomings in regard to these Internet domain name issues, Congress proactively made subsequent legislative attempts and enacted the ACPA in 1999 and the TDRA in 2006.

2. TDRA[149]

Congress's revision of the FTDA in the form of the TDRA strengthened the protection afforded to famous trademarks.[150] The TDRA changed the standard of proof necessary to succeed on a dilution claim to the newly articulated "likelihood of dilution" standard, which differed from the former "actual dilution" standard under the FTDA.[151] Additionally, the TDRA provides trademark holders with a more definitive idea of when dilution has actually occurred due to the clearly

---

146 *See* Acad. of Motion Picture Arts & Scis. v. Network Solutions, Inc., 989 F. Supp. 1276, 1279 (C.D. Cal. 1997) (ruling that simply registering a domain name does not equate to a commercial use).

147 *See* Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1326 (9th Cir. 1998). In its ruling the court stretched the original intent of the statute to find dilution by stating that it did not have to rely solely "on the traditional definitions" of "blurring" and "tarnishment." *Id*. Instead, the court found dilution happened because "[p]rospective users of plaintiff's services who mistakenly access defendant's web site may fail to continue to search for plaintiff's own home page." *Id*. at 1327. Ultimately, following a review of the trial court's factual findings, the court found that "Toeppen's 'business' [was] to register trademarks as domain names and then sell them to the rightful trademark owners," and further that he acted as a "spoiler," and "prevent[ed] Panavision and others from doing business on the Internet under their trademarked names unless they pay his fee.'" *Id*. at 1325 (citation omitted); *see also* Howard, *supra* note 39, at 650 (discussing that courts attempted to stretch the statute to find commercial use and dilution in cases where the violators sold no goods or placed no advertisements on the site).

148 *See Avery Dennison Corp*., 189 F.3d at 871 (noting that traditional trademark law does not mesh well with the modern Internet).

149 *See supra* Part II.F.2 (explaining the enactment of the TDRA and the changes it implemented to bolster the FTDA).

150 *See* Simburg et al., *supra* note 112, at 386 (clarifying that the TDRA promulgation in fact boosted the protection afforded famous marks and also addressed any uncertainty within the federal courts in their respective applications of the FTDA).

151 *See* Moseley v. V Secret Catalogue, Inc., 537 U.S. 418, 434 (2003). The majority opinion stated that "direct evidence of dilution such as consumer surveys will not be necessary if actual dilution can reliably be proved through circumstantial evidence—the obvious case is one where the junior and senior marks are identical." *Id*.

proscribed definitions of blurring and tarnishment.[152] Overall, the TDRA was a positive step forward for antidilution law and protection of trademark holders.[153] However, the TDRA fell short by failing to specifically articulate the requirements to meet the new "likelihood of dilution" standard.[154]

3. ACPA[155]

The passage of the ACPA eliminated the need to overextend trademark dilution law beyond its intended limit under the original FTDA.[156] The two most profound additions that the ACPA brought to domain name dispute resolution were in rem jurisdiction and actual and statutory damage awards between $1000 and $100,000 per violating domain name.[157] Before passage of the ACPA, in personam personal jurisdiction was the only available tool, which accordingly allowed many anonymous or foreign defendants to escape personal jurisdiction because no alternative cause of action existed for plaintiffs.[158] Furthermore, the ACPA replaced the FTDA's arbitrary famous and

---

[152] *See* Simburg et al., *supra* note 112, at 387 (stating that the TDRA extends trademark owners concrete definitions of blurring and tarnishment as well as allowing a better understanding of when another mark is dilutive).

[153] *See* Roe, *supra* note 112, at 605 (evaluating the TDRA as an effective addition to the FTDA because the TDRA recognized and addressed the FTDA's major shortcomings).

[154] *See* Kuhn, *supra* note 111, at 20–21. Courts interpreting the TDRA have failed to answer "the burden a plaintiff must bear in demonstrating the fame of its mark . . . and what plaintiff needs to show to establish dilution by blurring beyond a mental association between the famous and dilutive marks." *Id*.

[155] *See supra* Part II.F.3 (detailing the enacting of the ACPA and some of the documented violations of the Act).

[156] *See* Porsche Cars N. Am., Inc. v. Porsche.Net, 302 F.3d 248, 261–62 (4th Cir. 2002). The court concluded that the promulgation of the ACPA

> eliminated any need to force trademark-dilution law beyond its traditional bounds in order to fill a past hole, now otherwise plugged, in protection of trademark rights.
>
> As the Second Circuit recently remarked, the ACPA "was adopted specifically to provide courts with a preferable alternative to stretching federal dilution law when dealing with cybersquatting cases."

Id. (quoting Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489, 497 (2d Cir. 2000)).

[157] *See* Gore, *supra* note 29, at 203. The ACPA provides for in rem jurisdiction against the domain name itself. *Id*. Thus, parties that have a legitimate interest in a domain name no longer have to locate the infringing wrongful registrants. *Id*. Additionally, the ACPA permits courts to award damages, attorneys' fees, and statutory damages ranging from $1000 to $100,000 per domain name. *Id*. *Compare* 15 U.S.C. § 1125(d)(2) (2006) (creating in rem jurisdiction), *with* Lauzon, *supra* note 101, §§ 6–8 (stating that in rem actions cannot be concurrent with in personam jurisdiction).

[158] Lauzon, *supra* note 101, § 21(b) (highlighting the ACPA's addition of in rem jurisdiction as an additional weapon to fight domain name cybersquatting).

commercial standards with a more workable and exhaustive list of nine factors that courts could use to determine a bad faith intent to profit in violation of the ACPA.[159] However, even the nine factor bad faith test has drawn criticism, with claims that it is ambiguous and unwieldy.[160]

Despite the improvements that the ACPA made to legally address domain name disputes following in the footsteps of the FTDA, the ACPA has been consistently criticized for being too narrow in scope.[161] Due to that narrow scope, the ACPA's in rem personal jurisdiction has become less forceful and functional to American plaintiffs because it has become increasingly easy to avoid by using domain name registrars outside of the United States when obtaining a domain name.[162] Consequently, ICANN's new gTLD policy that will dramatically increase the number of domain names registered across the globe will also create more domain names capable of circumventing the ACPA's in rem personal jurisdiction and will do so on a much larger scale.[163]

Besides the jurisdictional changes, the ACPA granted domain name registrars safe harbor from liability for registering an infringing domain name.[164] Specifically, the ACPA limits the liability of a registrar or

---

159 *See* 15 U.S.C. § 1125 (2006); *supra* note 121 (laying out the nine factors that are considered for determining a bad faith intent to profit).

160 *See, e.g.*, Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214, 234 (4th Cir. 2002) (explaining that there is no set approach to formulate and weigh the factors). Courts do not tally which party has more factors in its favor and then rule accordingly. *Id.* The ACPA's legislative history explicitly states that the presence or absence of any of the nine factors is not necessarily outcome determinative in the dispute. *Id*.

161 *See* Harrods Ltd. v. Sixty Internet Domain Names, 110 F. Supp. 2d 420, 426 (E.D. Va. 2000) (explaining that the court's interpretation adheres to the legislative history of the ACPA, which clearly states that the statute is narrow in scope); *see also* Solid Host, N.L. v. Namecheap, Inc., 652 F. Supp. 2d 1092, 1102 (C.D. Cal. 2009) ("[The] ACPA was enacted to counter cybersquatting, a narrow class of wrongdoing . . . .").

162 Magier, *supra* note 30, at 444–45. It would be quite easy for a cybersquatter to register their chosen domain name with any of the number of registrars located outside of the United States. *Id*. Doing so would allow the cybersquatter to avoid any basis for in rem jurisdiction under the provisions of the ACPA. *Id.*

163 *Id.* at 447. The author reflects that the increasing complexity of the Internet

> will spur the creation of more TLDs and more registries in many different countries. As the need for more TLDs increases, therefore, registries will follow the same pattern of internationalization seen in the registrar industry. Consequently, the ACPA's in rem personal jurisdiction provision will be further undermined and of less and less use to American plaintiffs in taking action against cybersquatters.

Id.

164 *See* 15 U.S.C. § 1125(D)(ii) (declaring that "[t]he domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order"); *see also* Lockheed Martin Corp. v. Network

registry in regard to registering, transferring, disabling, or cancelling a domain name, even if that domain name is ultimately determined to be dilutive or infringing upon a trademark.[165] Subsequently, courts have enforced the limited liability of domain name registrars under the ACPA to protect both the efficiency of the domain name registration system as a whole and also the functionality of the alternate domain name dispute resolution avenue, the UDRP.[166] The ACPA recognizes the UDRP only insofar as it forms part of the general contractually accepted policy that registrars abide by in administering domain names.[167] Beyond that, the UDRP's relevance to actions brought under the ACPA exists under two specific contexts: (1) limiting the liability of a domain name registration that is done by a reasonable policy (including the UDRP); and (2) the ability to bring an ACPA suit for a victim of domain name transfer under that reasonable policy (again including the UDRP).[168] Although courts

---

Solutions, Inc., 141 F. Supp. 2d 648, 655 (N.D. Tex. 2001) (noting that domain registrars are immune from liability when acting in their normal capacities as registrars).

[165] 15 U.S.C. § 1114(2)(D)(ii)(II). The ACPA states that a registrar or registry will not be held liable for injunctive or monetary relief of a domain name registration if it is done "in the implementation of a reasonable policy by such registrar, registry, or authority prohibiting the registration of a domain name that is identical to, confusingly similar to, or dilutive of another's mark." *Id.*

[166] *See Lockheed Martin Corp.*, 141 F. Supp. 2d at 655. The court posited that if it were to allow for registrar liability

> [the] Defendant simply could not function as a registrar, or as keeper of the registry, if it had to become entangled in, and bear the expense of, disputes regarding the right of a registrant to use a particular domain name. . . . The reason the UDRP was developed was to provide the mechanism to resolve these disputes. Not only would imposing plaintiff's scheme render the UDRP nugatory, it would cause the domain name registration system in its entirety not to be feasible.

Id.

[167] *See* Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 625 (4th Cir. 2003) (recognizing the UDRP only as it represents part of a policy followed by domain name registrars).

[168] *Id.* The court states that the UDRP is relevant to actions brought under the ACPA in two contexts:

> First, the ACPA limits the liability of a registrar in respect to registering, transferring, disabling, or cancelling a domain name if it is done in the "implementation of a *reasonable policy*" (including the UDRP) that prohibits registration of a domain name "identical to, confusingly similar to, or dilutive of another's mark." Second, the ACPA authorizes a suit by a domain name registrant whose domain name has been suspended, disabled, or transferred *under that reasonable policy* (including the UDRP) to seek a declaration that the registrant's registration and use of the domain name involves no violation of the Lanham Act as well as an injunction returning the domain name.

Id. (quoting 15 U.S.C. § 1114(2)(D)(ii)(II) (2000)) (internal citation omitted).

interpreting ACPA cases may recognize the UDRP in a limited capacity, the UDRP does play a valuable role in resolving domain name disputes.

4. UDRP[169]

The UDRP plays a unique role, in addition to the existing legal remedies granted by the FTDA and the ACPA, in privatized dispute resolution.[170] The system has garnered praise for its contribution to domain name dispute resolution and also for its speed and efficiency.[171] However, like the FTDA and the ACPA, the UDRP has its fair share of criticism beginning with its narrow scope.[172] For example, the UDRP covers only a limited category of domain name disputes.[173] Further, the UDRP applies differently to different parties involved in domain name disputes.[174]

In addition to the UDRP's narrow scope, UDRP decisions have been rendered virtually null and void.[175] The proverbial deathblow of the UDRP came in *Sallen v. Corinthians Licenciamentos LTDA*.[176] The First Circuit in *Sallen* effectively ruled that the ACPA trumps any UDRP decision.[177] This holding undermined the function and purpose of

---

169 *See supra* Part II.F.4 (detailing the implementation of the UDRP).

170 *See* Carlton, *supra* note 39, at 33–34 (reasoning that the ICANN established procedures allow owners to protect their marks and to reduce the need for defensive domain name registrations).

171 *See* Helfer, *supra* note 136, at 494 (opining that the UDRP is a cost-effective and speedy method to address domain name disputes, but that in no fashion did the UDRP supplant cybersquatting litigation).

172 *See* Wal-Mart Stores, Inc. v. wallmartcanadasucks.com, WIPO Case No. D2000-1104 (WIPO Nov. 23, 2005), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1104.html (ruling that the UDRP is narrow in scope and is not designed to be a general remedy for all domain name misconduct).

173 *See* Ware, *supra* note 131, at 146 (expositing that the UDRP only covers claims that the registrant's domain name infringes on a trademark or servicemark). The UDRP applies only to registrars in the .com, .net, and .org top-level domains. ICANN Policy, *supra* note 127, ¶ 1.

174 *See* Parisi v. Netlearning, Inc., 139 F. Supp. 2d 745, 751 (E.D. Va. 2001). Participation in UDRP proceedings is mandatory for domain name registrants, but optional for trademark owners. *Id*. Trademark owners are not bound by contracts with domain name registrars; thus, they may choose to take their trademark claims directly to court. *Id*.

175 *See* Cnty. Bookshops Ltd. v. Guy Loveday, WIPO Case No. D2000-0655, at 4 (WIPO Sept. 22, 2000), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0655.html. UDRP decisions are not binding. *Id*. A losing domain name registrant can block implementation of a cancellation or transfer order by filing a law suit following the decision, and a losing trademark owner can exhume its claim by filing suit or merely by filing a second UDRP complaint. *Id*.

176 273 F.3d 14 (1st Cir. 2001).

177 *Id*. at 18 ("Section 1114(2)(D)(v) grants domain name registrants who have lost domain names under administrative panel decisions applying the UDRP an affirmative cause of

ICANN's UDRP, removed any urgency to reform the shortcomings of the current UDRP proceedings, caused federal courts to lose a valuable alternative resource, and turned the domain name dispute resolution process into a burden on domain name registrants.[178] This line of judicial reasoning has been extended, further weakening the UDRP's legitimacy.[179]

Legal scholars hypothesize that part of the reason that courts have chosen to give less deference to UDRP decisions is either that panels have stretched the role of the UDRP beyond its initial scope, or that they have simply acted incorrectly.[180] Ultimately, ICANN's major objective of eliminating both multiple jurisdictions and laws that decide domain name disputes is circumvented when the ACPA overrides UDRP panel decisions.[181]

Besides the effective undermining of the UDRP by the ACPA, another major criticism of the UDRP is that there are no uniform rules in place for arbitration panels to follow during their decision-making.[182] The very language of ICANN's Rules for the UDRP grants panel members great discretion to use "any rules and principles of law it deems applicable."[183] In early cases a lack of uniform rules may not have been a major problem; however, with the increase in the volume, speed, and intellect of modern cybersquatters, the UDRP has become

---

action in federal court for a declaration of nonviolation of the ACPA and for the return of the wrongfully transferred domain names."); *see also* McLaughlin, *supra* note 128, at 4–5 (commenting that the overlap between the ACPA and the UDRP could limit the effectiveness of the UDRP in cases that the dispute appears to allow for some federal cybersquatting action).

178 *See* Rohrer, *supra* note 26, at 564 (identifying that because federal courts give no deference to UDRP proceedings, they may lose a useful resource in resolving domain name disputes and the process could become a burden for domain name registrants).

179 *See* Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 625–26 (4th Cir. 2003) (ruling that any UDRP panel decision receives no deference under the ACPA).

180 *See* Stewart, *supra* note 96, at 515 (commenting that the creative decision-making employed in some UDRP cases is improper because the process relies on standard procedures to achieve fast and inexpensive results).

181 *See* Rohrer, *supra* note 26, at 584–85 (noting that a party to a UDRP proceeding can ignore the administrative decision and head to court where an entire new body of laws will govern the case).

182 *See generally* Jo Saxe Levy, *Precedent and Other Problems with ICANN's UDRP Procedure*, CYBERSPACE LAW., Apr. 2001, at 20. UDRP Rule 15(a) provides little guidance in that "the Panel shall decide the matter 'in accordance with this Policy, these Rules and any rules and principles of law that it deems applicable.'" *Id.* (quoting ICANN Rules, *supra* note 96, at 15(a)). Such open-ended rules grant each panel great discretion in making decisions. *Id.*

183 ICANN Rules, *supra* note 96, at 15(a).

ineffective.[184] ICANN's original framers of the UDRP never anticipated the advanced contemporary forms of cybersquatting, much less the introduction of new TLDs.[185] In addition to the expansive rules under the UDRP, the cost of filing a UDRP action can range from two hundred to two thousand times greater than the cost of registering a .com domain name, thus allowing cybersquatters to register millions of violating domain names.[186]

Currently, ICANN has no official policy in place to deter, prevent, or address abusive domain name registrations.[187] However, in the planning stages of the new gTLD policy, ICANN commenced a process to evaluate the concerns of trademark holders by seeking comments for improving the mechanisms used to limit the unauthorized use of trademarks in domain names.[188] Fortunately, following the trademark owners' comments, ICANN focused intensely on this issue in regard to the development of the new gTLD policy, and proactively proposed a number of its own recommendations.[189] These recommendations sought to address possible problems that may arise in applying traditional trademark law concepts to Internet governance.[190]

B. ICANN's New gTLD Policy and Accompanying Proposed Proactive Measures

ICANN's new gTLD policy has been applauded as an avenue to bring new services to consumers and to mitigate the market power of the .com gTLD.[191] ICANN's IRT formulated five proposed solutions to accompany the new policy lifting restrictions on gTLDs, specifically to address potential problems like cybersquatting.[192] First, ICANN plans to

---

184 *See* Rodenbaugh, *supra* note 53, at 184 (explaining that the current UDRP has been rendered ineffective with the increasing sophistication of trademark cybersquatters).

185 *Id.* (stating that the UDRP was not designed to deal with phishers and drive-by downloaders and is even less equipped to handle any new TLDs).

186 *See id.* at 179 (highlighting a recent report by MarkMonitor that discovered 380,000 cybersquatted domains that were related to just thirty brands).

187 *Id.* at 184.

188 Carlton, *supra* note 39, at 23 (developing this process was a direct attempt to prevent non-trademark holders from obtaining domain names of rightful trademark owners).

189 *See* Farley, *supra* note 51, at 627 (indicating that ICANN's Final Draft Proposal contained twenty recommendations to curtail long-term domain name registration problems).

190 *Id.*

191 Carlton, *supra* note 39, at 10 (explaining that ICANN's new gTLD plan will likely benefit consumers by offering new services and increasing innovation while at the same time mitigating the market power associated with the .com TLD).

192 *See Draft Final Report – Introduction of the GNSO New Generic Top-Level Domains*, ICANN (Mar. 16, 2007), http://gnso.icann.org/drafts/pdp-dec05-draft-fr.htm#recom; *see also* Beckstrom, *supra* note 45 (recognizing that with the domain expansion there is a

implement a new top-level, objection-based process to handle domain name dispute resolution.[193] This proposed objection-based process will conduct an initial evaluation of both the merits of the applicants and their disputed domain names.[194] During the name portion of the initial evaluation the IRT has proposed that during the name portion of the initial evaluation an algorithm should be used to determine which names require further analysis.[195] Legal scholars criticize this proposed solution for its potentially unscientific grounds for objecting to domain names. Further, scholars claim that this solution illustrates the disconnect between trademark law and domain name registration policy.[196]

---

possibility that some concerns and problems may arise). In order to ensure a smooth transition, ICANN opened dialogues with various Internet stakeholders for recommendations on how to handle the new TLDs. *Id*. These open dialogues have mainly addressed intellectual property rights. ICANN, in collaboration with intellectual property scholars, has begun to formulate solutions to any potential problems. *Id*.

193 *See* ICANN FAQs, *supra* note 38, at 3.15. This objection based process would allow rights holders to assert that proposed gTLD domain names would infringe their legal rights based on generally accepted and internationally recognized principles of law. *Id*. This process would take into account that it is not unusual to have a trademark in the same word or phrase for different products or services registered in different jurisdictions. *Id*.; *see also* Carlton, *supra* note 39, at 7. The objection process to new gTLD applications would include existing TLD registries, other applicants, holders of intellectual property rights and others. Carlton, *supra* note 39, at 7. However, these objections can be filed on a limited number of grounds including string confusion, trademark infringement, morality, public order, and community objection. *Id*.

194 *See Draft Applicant Guidebook, supra* note 51, at 2-1 to 2-11. The Initial Evaluation will assess domain names for their string similarity, if they are an already reserved name, if they affect the stability of the DNS, and if they impose on established geographic domain names. *Id*. Applicants will be judged upon their ability to demonstrate adequate technical and operational capacity, sufficient finances, and an implemented registry service review process for any DNS issues that may arise. *Id*. at 2-2, 2-14 to 2-18. Applicants who do not pass all Initial Evaluation criteria will be subject to an Extended Evaluation. *Id*. at 2-18. The Extended Evaluation maintains the same criteria as the Initial Evaluation but allows applicants to remedy any initial shortcomings in their Initial Evaluation. *Id*.

195 *See* IRT Letter, *supra* note 138, at 46 (specifying that the IRT recommends that the algorithm should only be used to determine possibly infringing domain names that would then require further analysis).

196 Farley, *supra* note 51, at 631. Professor Farley exposits that

> [t]rademark law is territorial in nature, therefore legal standards reflect the consumer perspectives of the particular state. . . . Trademark content restrictions are similar in approach. For instance, under U.S. trademark law, a mark will be refused registration if it is deemed to be scandalous or immoral when considered from the perspective of "a substantial composite of the general public." The "public" is understood to mean the U.S. public. To extend this legal standard to domain names it is necessary to consider a substantial composite of the general public of the entire world, not just the United States. This is obviously an unworkable standard. Even if it were a workable

The ICANN IRT's second major proposal is to create an Intellectual Property Clearinghouse in concert with a Globally Protected Marks List ("GPML").[197] This proposed solution calls for the IP Clearinghouse to act: (1) as the neutral central body with which all new gTLD registries, and possibly registrars, interact in relation to the GPML; and (2) also as a central information and database performing specific information collection and data validation.[198] The IP Clearinghouse would employ the GPML as a tool to prevent third parties from registering TLDs that match or are confusingly similar to trademarks on the list as well as second-level domains that match trademarks on the list.[199] Similar to other previously mentioned proposed measures, this proposed solution has been bombarded because of the incongruence between the domain name registration process and traditional trademark law.[200]

The third major proposal of the IRT is the implementation of the Uniform Rapid Suspension ("URS") for cases in which there is no genuine contestable issue as to the blatant and obvious domain name abuse that is taking place.[201] The IRT recognized that since the inception of the UDRP, circumstances and technology have changed, and as such,

---

> standard, it results in the lowest common denominator analysis much like obscenity analysis over the Internet. Thus, for example, .democracy, .gayrights, and .jesus, may all be refused as being morally offensive to the least tolerant society.

Id. (citations omitted).

197 *See* IRT Letter, *supra* note 138, at 5 (outlining the IRT's draft recommendation for the IP Clearinghouse, the Globally Protected Marks List and associated Rights Protection Mechanisms ("RPMs"), and standardized pre-launch rights protection mechanisms).

198 *Id*. at 13.

199 *See id*. at 15 ("A Globally Protected Marks List of trademarks satisfying the strict requirements recommended herein that has the effect of limiting third-party applications for (a) top-level domains that match or are confusingly similar to trademarks on the list; and (b) second-level domains that match trademarks on the list . . . .") (emphasis omitted).

200 Farley, *supra* note 51, at 628. Professor Farley states the following:

> This policy proposes comparing existing second level domains with proposed dot generics. Consider www.amazon.com versus an application for .amazon, where .amazon might be a top-level domain dedicated to the study of all things having to do with the Amazon. These two applications are certainly confusingly similar. They are identical words, therefore they would fail the test provided by this ICANN proposal. . . .
>
> A related problem with this recommendation is that it equates domain names with trademarks as legally protectable properties. They are not. Trademarks are legally protected intellectual property because the commercial use of a mark by another that is likely to cause confusion would injure consumers.

Id.

201 *See* IRT Letter, *supra* note 138, at 25 (clarifying that the URS will not be used to address cases of alleged infringement, for anti-competition purposes, or to prevent free speech).

trademark holders and Internet users face more domain name abuse and infringement daily.[202] The URS would supplement the UDRP by providing a faster means to stop the operation of an abusive Internet domain in a separate proceeding.[203] The URS would provide a cheaper and faster means for removing infringing domain name registrations, while allowing the possibility for appeal by the registrant.[204] Presently, there is little scholarly analysis of this proposed solution, but judging from the criticism addressing the UDRP, any change would be welcome.[205]

The IRT's fourth proposed solution calls for a Post-Delegation Dispute Mechanism to inhibit any registry misconduct.[206] The Post-Delegation Dispute Mechanism would allow a trademark holder to initiate a post-domain name delegation dispute by submitting a complaint to ICANN.[207] Following ICANN's investigation, the Post-Delegation Dispute Mechanism could enforce sanctions, suspensions, or find group liability that would warrant the cancellation of the registry's or registrar's agreement with ICANN.[208] Similar to the other proposed

---

[202] *See id.* at 25–26. The IRT suggested that "times and circumstances have changed since the UDRP was implemented and brand owners and Internet users find themselves facing unprecedented levels of abuse and infringement, which undermines trust in, and thereby negatively impacts the stability and security of the Internet." *Id.* Furthermore, "[t]he purpose of the URS is to address a cybersquatting problem for brand owners that is already insidious and enormous in scale, and which will continue to spiral out of control with the introduction of an unlimited number of new gTLDs unless addressed." *Id.*

[203] *Id.* at 25. The URS proceeding would only supplement the UDRP and not supplant it. *Id.* When any genuine contestable issue as to whether a domain name is an abusive use of a trademark, the complaint would not be heard in a URS proceeding but in a UDRP or court proceeding. *Id.*

[204] *Id.* at 26.

[205] *See supra* Part III.A.4 (recognizing that some legal scholars have documented their displeasure with the current domain name dispute resolution model).

[206] *See* IRT Letter, *supra* note 138, at 39. The Post-Delegation Dispute Mechanism was designed to combat the following:

> (i) Registry Operators that operate a TLD in a manner that is inconsistent with the representations and warranties contained within its Registry Agreement, or (ii) Registry Operations that have a bad faith intent to profit from the systematic registration of infringing domain names (or systematic cybersquatting) in the Registry Operator's TLD.

Id.

[207] *See id.* at 40 (noting that following the submission of the complaint and a refundable deposit ICANN must investigate whether the Registry Operator is in material breach of its contractual obligations).

[208] *Id.* at 25. The IRT proposes that the following enforcement tools be available:

> 2.4.1 Sanctions & Suspension—Providing for escalated compliance enforcement tools such as monetary sanctions

solutions, the Post-Delegation Dispute Mechanism would supplement the UDRP, not supplant it; and if either ICANN or the Registry Operator chose to have a UDRP proceeding, or a court action in the appropriate jurisdiction, it would be permitted.[209]

The fifth and final major proposed solution by the IRT calls for all new TLDs to provide WHOIS under the "Thick" or Registry level WHOIS Model.[210] The WHOIS database is a central publicly accessible list that contains all of the domain name registration information submitted by domain name registrars.[211] The IRT believes the "Thick" WHOIS Model is essential to the cost-effective protection of consumers and intellectual property owners.[212] The IRT bases its decision on the fact that for many years newer gTLDs such as .biz and .info have employed a "Thick" Registry WHOIS model without any evidence of

---

> the suspension of accepting new domain name registrations in the TLD until such time as the violation(s) . . . is cured.
>
> 2.4.2 Group Liability—Preventing "serial misconduct" by registries when another affiliated (by common control) registry's or registrar's agreement with ICANN is terminated, provided that such affiliated registry or registrar has also been involved in the [violating] activities . . . .
>
> 2.4.3 Termination of Contract—Providing for the termination of a registry agreement should a Registry Operator be found by three (3) separate Panels, arising out of 3 separate and distinct incidents, to have violated its contract . . . within any eighteen (18)-month period.

Id at 43.

[209] *Id.* at 44. The system is set up so that

> [t]he mandatory administrative proceeding requirements . . . shall not prevent Registry Operator or ICANN from submitting the dispute to an administrative panel in accordance with its applicable Registry Agreement or to a court of competent jurisdiction for independent resolution *before* such mandatory Post-Delegation Dispute proceeding is commenced or *after* such proceeding is concluded.

Id.

[210] *See* Froomkin, *supra* note 27, at 99 n.356 (explaining WHOIS). The preferred Thick WHOIS model would be "the central, registry-level provision of WHOIS information for all domain names registered within the registry. This model is in contrast to the 'Thin WHOIS' model whereby the registry-level information is very limited and Internet users must rely on the registrar-level for the submission of robust WHOIS data." IRT Letter, *supra* note 138, at 45.

[211] *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 395 (2d Cir. 2004) (noting that the registration of a domain name requires one to submit the applicant's name, telephone number, postal address, and e-mail address, and further noting that this information is known as the WHOIS information according to the ICANN Agreement and that it must be publicly accessible and updated daily by the registrars).

[212] IRT Letter, *supra* note 138, at 45.

legal repercussions.[213] Adopting such a policy would allow Internet users and domain name registrants to monitor all the names that are registered in their registry including those that may be infringing upon their trademark.[214]

Surveying the current landscape of domain name dispute resolution, both through governmental legislation and private arbitration, it is clear that some sort of change is in order.[215] Although ICANN is far from a perfect manager of the domain name registration system, it is extremely successful in separating the technical operations of the Internet from overreaching governments.[216] Furthermore, throughout the implementation of the new gTLD policy, ICANN has remained open to enacting additional mechanisms to protect against potential abuse of existing trademarks, which demonstrates ICANN's ultimate goal of minimizing domain name abuse.[217] Unfortunately, ICANN's five proposed solutions to accompany the new policy lifting the restrictions on gTLDs are idealistic and lack the legal power to be enough to protect legitimate trademark holders and domain name registrants.[218] ICANN acts as little more than a gatekeeper to those who wish to register domain names. Further, any decision that a UDRP panel hands down

---

[213] *Id*. The IRT recognizes that some comments raised in the public comment session raised privacy concerns about this recommendation. *Id*. at 45 n.50. However, it notes that the Thick registry WHOIS model has been used in many new gTLDs without any adverse legal consequences. *Id*.

[214] *See* Harris, *supra* note 127, at 48. The authors explain that the

> WHOIS databases provide a crucial tool for businesses, the Federal Trade Commission, and other law enforcement agencies to track down brand infringement, online fraud, identity theft, and other online illegal activity, but are often hindered in their pursuit because the person responsible is hiding behind the anonymity of false registration information.

Id. (quoting S. Res. 564, 110th Cong. § 2(15) (as introduced Feb. 25, 2008)).

[215] *See supra* Part III.A (documenting the successes and shortcomings of the current remedial measures for domain name disputes).

[216] *See* DelBianco & Cox, *supra* note 77, at 39 (noting that ICANN's thorough and continued management of the technical functions of the Internet is the best way to maintain its independence and democracy and at the same time fend off interfering governments).

[217] *See* Carlton, *supra* note 39, at 33. If ICANN deems it necessary

> various additional mechanisms could be created by ICANN to protect against abuse of existing trademarks. The draconian remedy of precluding entry a as [sic] means of preventing the possibility of a need for defensive registrations is unlikely to be an efficient mechanism for dealing with these costs because it deprives consumers of the benefits of entry.

Id.

[218] *See* Cnty. Bookshops Ltd. v. Guy Loveday, WIPO Case No. D2000-0655, at 4 (WIPO Sept. 22, 2000), *available at* http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0655.html (recognizing that UDRP decisions are not binding on federal courts).

can be abrogated by a federal court proceeding.[219] The lack of a final say in domain name disputes makes any ICANN remedial measure a truly hollow solution. Reviewing the current landscape, there is no doubt that the likelihood of confusion test is beneficial in limited circumstances as is the ACPA. However, there remains a huge hole that can be filled by a likelihood of dilution test. The task at hand now is to determine which proposed solutions to integrate to ensure a smooth and efficient transition into a more expansive TLD name system.

IV. CONTRIBUTION

Lifting restrictions and allowing the open registration of new gTLDs will flood both federal courts and UDRP proceedings with an increased caseload of domain name disputes.[220] Ideally, a new federal cybersquatting law designed specifically to address these potentially new domain name disputes would be the best solution. Unfortunately, the time that it would take Congress to conduct congressional hearings, engage committees, and then approve any legislation, makes new legislation an impractical solution with the domain registration restrictions having been lifted in 2010. Consequently, any effective solution must incorporate the currently established and utilized remedial measures.[221]

The common thread among the currently established remedial measures is the fact that both trademark and legitimate domain name registrants bear the responsibility of monitoring the market for any infringement.[222] Convoluting the situation, ICANN's lifting of TLD name registration restrictions will likely lead to some cybersquatting or damage to those famous domain names and trademarks.[223] However, a solution does exist that would not only give legitimate domain name owners redress but also clarify some current uncertainty in trademark law.

---

[219] *See* Barcelona.com, Inc. v. Excelentisimo Ayuntamiento De Barcelona, 330 F.3d 617, 625–26 (4th Cir. 2003) (reiterating that federal courts give no deference to UDRP panel decisions).

[220] *See supra* notes 54–56 and accompanying text (noting that a number of possible trademark issues exist and that many influential American corporations have expressed concerns with possible increased domain name litigation).

[221] *See supra* Part III.A (analyzing the currently available remedial measures: the FTDA, TDRA, ACPA, and UDRP).

[222] Whether a plaintiff chooses to use the FTDA, TDRA, ACPA, or UDRP the burden of monitoring the market for infringing uses on a rightful owner's trademark falls on that owner.

[223] *See supra* Part II.D (recognizing the potential problems that could accompany the expansion of top-level domain name registrations).

A. Killing Two Birds with One Stone: The TDRA and a Likelihood of Dilution Test

Implementing an articulated likelihood of dilution test that would be used by courts to accompany the TDRA would protect both domain name registrants from cybersquatters and also trademark owners from infringing use of their respective marks. The TDRA provides the best solution for a number of reasons. First, the TDRA provides an intact, fast, and furious remedy to litigate both domain name abuses and trademark dilution.[224] Second, common domain name abuses fall within the realm of dilution protected under the TDRA.[225] Third, the TDRA is recent legislation that is still open for judicial interpretation using the new likelihood of dilution standard.[226] Fourth, by simply adding an articulated likelihood of dilution test, federal courts would have a uniform standard to use in reviewing claims of trademark dilution and domain name abuses. Fifth, domain name registrants and trademark holders would have a clear indication of what constitutes infringing use, thus limiting the number of frivolous claims. These five reasons demonstrate that implementing a likelihood of dilution test would benefit legitimate domain name holders, trademark holders, federal courts, and trademark law in general.

B. The Likelihood of Dilution Test

Initially, it is important to note that this proposed likelihood of dilution test would be distinct and insular from the currently employed test that governs FTDA analysis. The proposed test would only amend the test for "dilution by blurring," which in no way affects the separate "dilution by tarnishment" test or any trademark infringement based on the "likelihood of confusion analysis." That being said, to implement the most effective and impactful test, three carefully selected factors have been compiled: the similarity of the marks, the relatedness of the goods or services, and the contemporaneous use of the Internet as a marketing channel. Unlike most trademark tests that weigh the totality of the circumstances or act as a balancing test, the proposed test navigates a step by step procedure in which dilution by blurring can be found at any

---

224 *See supra* Part II.F.2 (detailing the intricacies of the TDRA).

225 *See* Roe, *supra* note 112, at 602 (recognizing that courts may find a use to be close enough to constitute "identical" under the TDRA to find dilution, even though the use of domain names was not precisely identical).

226 *See id*. at 589 (claiming that the open-ended likelihood of dilution standard allows for judicial interpretation); Kuhn, *supra* note 111, at 9 (stating that federal courts have yet to set concrete standards to determine dilution under the TDRA).

step without requiring further analysis of the remaining factors. The first and primary factor in determining dilution should be the similarity of the marks.[227] Infringing marks that are remarkably similar to famous and legitimate trademarks would generate a presumption of dilution under the proposed test. Marks that are identical or nearly identical would need no further factor analysis beyond the first factor because dilution would already exist.[228]

The same analysis would apply to domain name abuses. An example would be illustrative. Imagine if a cybersquatter were to acquire the .ford TLD name following ICANN's lifting of gTLD restrictions and the Ford Motor Company brought suit under the TDRA. Following the proposed likelihood of dilution test and its primary factor, the similarity of the marks, the cybersquatter would be diluting Ford's legitimate trademark.[229] Clearly, implementing similarity of the marks as the first factor would catch many egregious and obvious infringements and abuses without requiring further analysis.[230]

Nonetheless, to augment the likelihood of dilution test in a case where the similarity of the marks is ruled inconsequential, the second factor would be the relatedness of the goods or services. Marks or domain names that may have passing similarities may not be fatal in similarity, but if they are competitors in business, dilution may be found. Implementing this as the second factor would have found dilution by both blurring and tarnishment in *Moseley v. V Secret Catalogue, Inc*.[231] Although the Supreme Court found dilution by tarnishment, they did not find dilution by blurring.[232] Under the relatedness of goods or services factor of the proposed likelihood of dilution test, dilution by blurring would be found. Both companies were in the business of selling women's lingerie and other novelty items.[233] In such a case, dilution

---

227 *See* Moseley v. V Secret Catalogue, Inc., 537 U.S. 418, 434 (2003) (holding that "direct evidence of dilution such as consumer surveys will not be necessary if actual dilution can reliably be proved through circumstantial evidence—the obvious case is one where the junior and senior marks are identical").

228 *Id*.

229 *See* Simburg et al., *supra* note 112, at 387. The TDRA provides greater certainty in determining when dilution has occurred by defining blurring as the "association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark." *Id*. (citation omitted).

230 *See Moseley*, 537 U.S. at 434 (reasoning that dilution can be proven easily in the cases where the true mark and the infringing mark are identical).

231 *Id*.

232 *Id*.; *see also* Kuhn, *supra* note 111, at 21 (relaying that the court found dilution by tarnishment but not by blurring, thus leaving the question of how one proves a likelihood of dilution unanswered).

233 *Moseley*, 537 U.S. at 423 (noting that besides lingerie, the store sold romantic lighting, lycra dresses, adult novelty items, and pagers).

would likely be found because a legitimate trademark was being infringed upon by a direct competitor in business.

The third and least weighted factor of the proposed likelihood of dilution test is the contemporaneous use of the Internet as a marketing channel. TDRA cases that do not find dilution by the first two factors of the proposed test would then look to the contemporaneous use of the Internet as a marketing tool. Courts would look to where the competing marks advertise and market their respective businesses. For example, if two companies with somewhat similar marks compete in related or similar goods or services, but market on different Internet sites, it is possible that dilution may not be found. Conversely, if two companies with somewhat similar marks compete in related or similar goods or services, and then one company begins to encroach and advertise on all the same sites as another, dilution may be found.

Overall, the framework of the proposed likelihood of dilution test may not appear to be concrete. However, given the sophistication of federal courts, a uniform factored test would heed consistent rulings. That being the case, both legitimate trademark holders and domain name registrants would benefit because there would be a more indicative body of case law as to what constitutes a likelihood of dilution. Critics may argue that such a proposed test is only a solution for marks that are already in existence. Nonetheless, trademark holders and domain name registrants would have a clearer idea of when their trademarks or domain names were being violated. Ultimately, this federal claim provides a more powerful and far reaching course of action for trademark holders and domain name registrants than any other remedy currently in existence.

V. CONCLUSION

As mentioned in the introduction to this Note, history has a way of repeating itself. Although the Homestead Act of 1862 proved to be an unsuccessful attempt at physical expansion, ICANN and federal courts can learn something in their technological land-grab. Under the already implemented TDRA, federal courts can adopt a simple, three-factor likelihood of dilution test that can solve both trademark issues and domain name disputes.

This Note proposes a likelihood of dilution test under the TDRA that can apply both to trademark law issues and domain name disputes. Critics may question the efficacy of a simple three-factor test. However, if federal courts simply employ the suggested likelihood of dilution test, their courtrooms will run more efficiently, trademark and domain name owners will recognize dilution and abuses with more ease, and

trademark law as a whole will gain some needed clarity. Successful implementation of the new gTLD registration policy will spur innovation, creativity, and business expansion in cyberspace. On the other hand, failure to implement a new policy will lead to a flood of lawsuits, trademark violations, and finger pointing. With the proposed likelihood of dilution test under the TDRA, federal courts can avoid a mountain of problems that would result if the gTLD expansion occurred today.

Brian W. Borchert[*]

[*] J.D. Candidate, Valparaiso University School of Law (2011); B.A. Spanish Studies and B.S. Sport Studies, University of Minnesota-Twin Cities (2006). I would like to thank my parents, James and Wendy, for their lifelong support, encouragement, and inspiration. I am also grateful to have two amazing siblings, Karin and Christopher, who have always been there for me.