An End to an Era of Cyber-Squatters: Connecting the Domain Name Registration Process to the World Intellectual Property Organization to End Bad Faith Registration.

Nicole Camuti
An End to an Era of Cyber-Squatters: Connecting the Domain Name Registration Process to the World Intellectual Property Organization to End Bad Faith Registration.

Nicole C. Camuti-Popovski*

I. INTRODUCTION

As early as 1962, the concept of a “Galactic Network” was envisioned by J.C.R Licklider in a series of memos in which he discussed his visions of a global interconnecting set of computers where every person could access a wide variety of data and programs from any site at any time.¹ The idea behind every famous developer who assisted in the creation of the Internet was to create a link which could extend around the world, ultimately giving rise to a global connection. It seems strange then that while the conceptual thinkers dating back to the 1960’s imagined this global connection, the mainstream problem of the abusive registration of domain names stems from the very lack of a worldwide connection between the registry system of domain names and trademarks.

This article discusses the increased efforts to provide an effective and efficient resolution mechanism for trademark holders who have been subject to attack by cyber-squatters through the use of domain names which are either identical or confusingly similar to their marks. The increase in cases brought before the dispute resolution body providers shows that individuals are able to effectively seek relief when faced with a domain name conflict. At the same time, this article will discuss the lack of connection between the registration processes in applying for a domain name against the registration process for trademarks.

---

*J.D. Candidate 2013, Albany Law School; B.S. in Engineering and Business, New York Institute of Technology.
Part II of this article provides an overview of the creation and development of the World Intellectual Property Organization ("WIPO") including the goals set forth when the organization was originally created as well as membership criteria, the different organs of the organization and their functions. It also discusses the creation and development of the WIPO Arbitration and Mediation Center with primary focus on its dispute resolution mechanism and how it has played a key role in the international growth of Intellectual Property.

Part III of this article discusses the abusive registration of a domain name which is identical or confusingly similar to that of a trademark which an individual or entity has rights to. This part examines the various types of cyber-squatters and the methods that they use to either profit from the trademark owner’s reputation or attempt to confuse the public into thinking it is accessing the actual trademark owner’s website and products on-line. In addition, Part III will discuss the important steps the United States has taken to provide for a legally binding resolution for trademark holders.

Part IV of this article examines the process through which the Uniform Dispute Resolution Procedure ("UDRP") was created and developed. After discussing the background of UDRP and the necessary developments of the procedures, Part V examines how UDRP has addressed internet-based issues throughout the years in an effort to provide effective relief for trademark holders affected by cyber-squatters. It also discusses the idea of WIPO and the Internet Corporation of Assigned Names and Numbers ("ICANN") expanding their efforts by developing a verification process in which a domain name applicant is analyzed during the application phase, especially through a process of clearing the applicant of previous cyber-squatting cases.
Part VI of this article addresses ICANN’s new application process, developed for generic Top-Level Domain’s (“gTLD’s”), scheduled to become effective in January of 2012. It will examine the principles underlying this application process and will further compare how those principals directly apply to domain names.

Lastly, Part VII summarizes the above parts and asserts that in order for Intellectual Property to continue to develop, while still protecting the rights of both the general public and trademark holders, additional steps need to be taken in the verification process when granting domain names. These additional steps are necessary to provide an individual with resources other than limited judicial proceedings to stop the abusive use of their trademarks in domain names now in place. The additional steps include a new application process for gTLD’s which calls for strict verification processes to protect trademark holders and the general public as a whole; a concept not so new to Intellectual Property. Therefore, the same underlying principles should be kept in mind when discussing domain name applications.

II. THE WORLD INTELLECTUAL PROPERTY ORGANIZATION

The World Intellectual Property Organization (“WIPO”) is the center of the international Intellectual Property system. Its efforts are geared toward developing a balanced system which promotes and rewards creativity, allowing innovation while protecting the public interest. WIPO is a specialized agency of the United Nations that is incorporated into the United Nations System. Under the Agreement between WIPO and the United Nations, WIPO is responsible for “promoting creative intellectual activity and for facilitating the transfer of technology related to

---

3 Id.
4 Id.
industrial property to the developing countries in order to accelerate economic, social and
cultural development, subject to the competence and responsibilities of the United Nations and
its organs.”

In July of 1967, WIPO was established through the WIPO Convention to protect
intellectual property rights relating to “literary, artistic and scientific works, performances of
performing artists, phonograms, and broadcasts, inventions in all fields of human endeavor,
scientific discoveries, industrial designs, trademarks, service marks, and commercial names and
designations, protection against unfair competition, and all other rights resulting from intellectual
activity in the industrial, scientific, literary or artistic fields.” Membership in WIPO is fairly
open either to any member of the United Nations or any state which is part of a specialized
agency of the United Nations, or is a party to the Statute of the International Court of Justice. In
addition, a party may be invited to become a member by the WIPO General Assembly (“General
Assembly”). Currently, there are 184 member states, which include Intellectual Property
powerhouses as well as third world countries with limited technological resources. The member
states of WIPO determine WIPO’s strategic direction, including WIPO’s budget for these
activities. WIPO operates through its member states, who meet in Assemblies, Committees and
by other decision making bodies of the organization.

---
5 AGREEMENT BETWEEN THE UNITED NATIONS AND WORLD INTELLECTUAL PROPERTY ORGANIZATION (1974).
6 CONVENTION ESTABLISHING THE WORLD INTELLECTUAL PROPERTY ORGANIZATION, Art. 2 (1967).
7 Id. at Art. 5.
8 Id.
10 See generally id.
11 Id.
The General Assembly is the primary organ of WIPO.\textsuperscript{12} It consists of one delegate per member state, as well as a Director General.\textsuperscript{13} The General Assembly is tasked with adopting budgets, approving measures suggested by the Director General, adopting financial regulations of the organization, determining which states that are not members of the organization and which intergovernmental and international non-governmental organizations may be admitted to its meetings as observers, as well as exercising all other necessary functions deemed appropriate under the WIPO Convention.\textsuperscript{14} The General Assembly meets once every second calendar year or when an extraordinary session is called for, all of which are held at WIPO’s headquarters in Geneva.\textsuperscript{15} Each member is entitled to one vote in the General Assembly and the majority of the decisions made by the General Assembly require a two-thirds majority of the votes casted.\textsuperscript{16}

In addition to the General Assembly, another organ of WIPO that plays an essential role is the WIPO Conference.\textsuperscript{17} The WIPO Conference consists of one delegate from each member state.\textsuperscript{18} The WIPO Conference is tasked with discussing “matters of general interest in the field of intellectual property and may adopt recommendation relating to such matters” as well as adopting the budget of the conference, establishing legal-technical assistance teams, and exercising other functions deemed appropriate by the convention.\textsuperscript{19} Each member state is entitled to one vote in the WIPO Conference, which also requires two-thirds of the majority votes cast.\textsuperscript{20}

\textsuperscript{12}CONVENTION ESTABLISHING THE WORLD INTELLECTUAL PROPERTY ORGANIZATION, Art. 6 (1967).
\textsuperscript{13}Id.
\textsuperscript{14}See generally id.
\textsuperscript{16}CONVENTION ESTABLISHING THE WORLD INTELLECTUAL PROPERTY ORGANIZATION, Art. 6 (1967).
\textsuperscript{17}Id.
\textsuperscript{18}Id. at Art. 7.
\textsuperscript{19}See generally id.
\textsuperscript{20}Id.
Additionally, the Coordination Committee was established in the Convention, and is tasked with giving advice to the organs of WIPO, drafting an agenda of the General Assembly, drafting an agenda and program as well as the budget of the WIPO Conference, nominating a candidate for appointment of Director General and performing all other functions deemed appropriate under the Convention.21

A. WIPO Arbitration and Mediation Center

As Intellectual Property became more competitive, especially on an international level, the need for a dispute resolution system amplified. In the past, alternative dispute resolution, was not generally recognized as a means for settling disputes in the Intellectual Property field. As Intellectual Property became an essential business asset, parties needed a dispute resolution mechanism that matched their business requirements in the sense of a private, cost effective, efficient and flexible means of settling disputes. With this in mind, in September of 1993, WIPO’s General Assembly approved the establishment of the WIPO Arbitration and Mediation Center, which provided mediation, arbitration and expedited arbitration at a cost much lower than court proceedings.22

As of the writing of this article, this center is the leading resource for private party resolution on an international level outside of the judicial system.23 This is so mainly because these services can take place in any country, in any language, and under any law.24 However, this

---

21 CONVENTION ESTABLISHING THE WORLD INTELLECTUAL PROPERTY ORGANIZATION, Art. 8 (1967).
23 Id.
recourse is completely voluntary in nature; therefore each conflict would come before the system only if all parties freely and willing agreed.25

B. International Trademark Registration

Registering a trademark in the United States is somewhat different then obtaining a trademark registration on an international level. In the United States, a potential trademark owner sends a relatively simple application to the Patent and Trademark Office (“PTO”) that will examine the application and either grant or deny the trademark registration.26

On an international level, the Madrid System uses an application that is filed with WIPO, giving trademark owners an option of essentially international trademark protection, pending approval.27 The Madrid System allows a trademark owner to file a single application with either a national or regional trademark office. The international mark, once registered, is considered identical to that which would be filed directly with each individual country designated by the applicant.28 The designated countries receive the trademark application, and if they do not refuse protection of the trademark within the allotted time frame, protection is extended to that trademark.29 The Madrid System encourages international registration of trademarks by making the process as simple as possible. It also allows for an easily accessible system for revisions, renewal, and managing the payment of fees.30

III. HOW CYBER-SQUATTERS AFFECT TRADEMARK HOLDERS

25 See generally id.
26 Section 43(a) of the U.S. Lanham Act expressly protects trademark owners rights for trademarks which are not only registered but the trademarks which are not registered as well.
29 Id.
As the Internet developed throughout the years, it became essential to any business, organization or individual to use the trademark or service mark as a domain name. A domain name acts as a location identifier for a business on the Internet, therefore, serving as either a trademark or service mark. To be registered and act as a trademark, the domain name must actually indicate the source or origin of goods or services; it cannot simply be the physical internet address.

Domain names are a part of the Uniform Resource Locator ("URL"), which is a string of words and numbers used to locate websites throughout the Internet. The domain name itself is the final section of the URL and consists of two parts. The first part of the domain name is the generic Top-Level Domain ("gTLD"). Currently, there are more than two dozen domains for which an applicant can apply for domain names with. The second level of the name is the business, organization, agency or sponsor of the website; for example, “Buybooks” in buybooks.com. The process of registration has changed minimally throughout the years.

Originally, there was only one registrar, Network Solutions, Inc. ("NSI"), who had registered the initial gTLD’s including the most famous “.com.” In 1999, the Internet Corporation of Assigned Names and Numbers ("ICANN") assumed responsibility for overseeing

31 A trademark is any word, symbol, design, device, logo, or slogan that identifies and distinguishes one product or service from another. They identify the origin of the product or service. If the trademark is used for services rather than products, it is referred to as a service mark. Trademark rights do not necessarily vest when the logo, design, etc. are created, rather when the mark is used in commerce.
33 Id.
34 Id. at 185.
35 Richard Stim, Trademark Law 185 (2000); Current gTLD’s include: .com, .edu, .gov, .int, .mil, .net, .org, .biz, .info, .name, .pro, .aero, .coop, .museum, .asia, .cat, .jobs, .mobi, .tel, and .travel.
36 See generally ICANN Accredited Registrars, Internet Corporation of Assigned Names and Numbers ("ICANN") (Nov. 15, 2011 9:30pm) http://www.icann.org/en/registrars/accredited-list.html.
38 See generally Network Solutions: Domain Names, Network Solutions (Nov. 13, 2011, 11:00am) http://www.networksolutions.com/
and registering the domain name system.\textsuperscript{39} ICANN is a not-for-profit public-benefit corporation that includes members from around the world whose primary goals are to keep the Internet as secure and stable as feasibly possible.\textsuperscript{40} ICANN attempts to promote competition while developing policies on the Internet’s unique identifies, essentially, domain names.\textsuperscript{41}

Actual registration of a domain name is quite simple; the applicant accesses ICANN’s website and searches available domain names.\textsuperscript{42} If the name the applicant is attempting to register is not previously registered, the applicant will fill out an on-line form providing ICANN with all necessary contact information and the applicant will pay a basic fee for the registration of the domain name.\textsuperscript{43} Essentially, registration for a domain name is on a first come, first serve basis.\textsuperscript{44} ICANN currently does not verify the accuracy of the information which is supplied throughout the application.\textsuperscript{45} Thus, there is no verification process that takes place to determine if the person, entity or organization seeking the domain name has any actual affiliation with the name they are attempting to register.\textsuperscript{46} Therefore, an individual can file an application and be granted a registration for a domain name that they have no connection to or that rightfully belongs to someone else. For example, if goggle.net has not yet been registered by goggle, an applicant can apply for and be granted the domain name simply because they were the first to apply and without having any actual affiliation to Goggle.

\textsuperscript{39} Richard Stim, Trademark Law 185 (2000).
\textsuperscript{40} See generally What is ICANN? Internet Corporation of Assigned Names and Numbers (Nov. 13, 2011, 11:00am) http://www.icann.org/en/about/.
\textsuperscript{41} See generally id.
\textsuperscript{42} Internationalized Domain Names, ICANN (Nov. 13, 2011, 11:30am) http://www.icann.org/en/topics/idn/.
\textsuperscript{44} Richard Stim, Trademark Law 185 (2000).
\textsuperscript{45} Richard Stim, Trademark law 185 (2000).
\textsuperscript{46} Id.
Beginning in the mid-1990’s, trademark owners were faced with an extremely large amount of cyber-squatters.\textsuperscript{47} Cyber-squatting was defined by the sixth circuit in 2004 as occurring when “one 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 holders.”\textsuperscript{48}

Cyber-squatters can attempt to profit from the abusive domain name registration in various different ways. The “Traditional” cyber-squatter will register a well known trademark as a domain name in an attempt to later profit in the sale of the domain name to the owner of the trademark.\textsuperscript{49} A “Pseudo” cyber-squatter will register a misspelling or another variation of a well known mark in an attempt to also sell the domain name to the trademark owner.\textsuperscript{50} Lastly, a “Siphoner” will register a domain name that is remarkably similar to an established trademark usually with a different spelling or a slight variation and use that similar mark to essentially “siphon” customers from the well known site to its own site.\textsuperscript{51}

Both on a domestic and international level, it was recognized that some efforts needed to be taken to combat the ever increasing amount of cyber-squatters. The trademark owners were resorting to purchasing the domain names that were registered improperly by the cyber-squatter because it was simply more cost-effective to buy the domain name rather than initiating court proceedings.

\textbf{A. Development of the Anti-Cyber-squatting Consumer Protection Act}

\textsuperscript{47} Id. at 186.
\textsuperscript{48} DaimlerChrysler v. The Net, Inc., 388 F.3d 201, 204 (6th Cir. 2004).
\textsuperscript{49} Richard Stim, Trademark Law 186 (2000).
\textsuperscript{50} Id.
\textsuperscript{51} Id.
In 1999, the United States adopted the Anti-Cyber-squatting Consumer Protection Act ("ACPA"). ACPA prohibits the use, registration or trafficking of a domain name that is identical or confusingly similar to the trademark.\textsuperscript{52} In cases of famous marks, ACPA allows for an action if the domain name dilutes the famous trademark.\textsuperscript{53} ACPA only applies to the bad faith registration of a domain name with an intent to profit at a later date, which the court determines by using a balancing test.\textsuperscript{54} ACPA also allows for remedies that include the collection of the domain name owner’s profits, actual damages and costs associated with the case as well as transfer or cancellation of the domain name.\textsuperscript{55}

**IV. THE DEVELOPMENT OF THE UNIFORM DISPUTE RESOLUTION PROCEDURE**

On an international level, ICANN is the main registry for domain names.\textsuperscript{56} ICANN assumed control of the domain name registry in 1999.\textsuperscript{57} After ICANN assumed control, it adopted and implemented the Uniform Domain Name Dispute Resolution Policy ("UDRP").\textsuperscript{58} This newly adopted policy results in arbitration of the pending dispute, rather than litigation, thereby calling for a cost effective and efficient resolution mechanism.\textsuperscript{59} Even within the U.S.,

\textsuperscript{52}Trademark law in the United States is centered around the idea that a trademark owner should be able to prevent someone from creating a sense of confusion as to the origin or source of the goods or services.

\textsuperscript{53}Dilution typically occurs when a famous marks reputation is either blurred or tarnished by the commercial use of a similar mark. Here, unlike trademark infringement cases, there need not be consumer confusion as to the source or origin of the goods or services. Rather, the parties do not need to be in direct competition and all that needs to be established is that the senior users trademark is famous, became famous prior to the junior user and that the junior, by using the trademark, is tarnishing or blurring the senior users trademark. This is often accomplished by disparaging the senior mark or source through the use of a similar mark or causing the famous mark to lose part of its distinctiveness. See generally Richard Stim, Trademark Law 185-210 (2000).

\textsuperscript{54}Mary LaFrance, Understanding Trademark Law 237 (2005).

\textsuperscript{55}See generally id. at 237-247.


\textsuperscript{57}Mary LaFrance, Understanding Trademark Law 247 (2005).

\textsuperscript{58}Id.

\textsuperscript{59}Richard Stim, Trademark Law 188(2000).
the UDRP is the leading mechanism for resolving domain name disputes outside of the Lanham Act.⁶⁰

Perhaps the first step in creating the UDRP was made by WIPO in what is known as the WIPO First Process.⁶¹ WIPO member states decided to take on the process of Internet-based and in-person consultations throughout the world to obtain the widest possible range of participation and expertise.⁶² The WIPO First Process was published in April of 1999.⁶³ The report addressed four major areas: dispute prevention; a uniform system of dispute resolution; protection of famous and well-known marks in generic top level domain (“gTLD’s”); and the impact on Intellectual Property as a whole by adding those already existing gTLD’s.⁶⁴ Directly following this report, in August of 1999 ICANN adopted the resolution mechanism introduced by the WIPO First Process.⁶⁵

The UDRP became effective December 1, 1999.⁶⁶ Its primary function was to address the bad faith registration of domain names in an efficient and cost effective system.⁶⁷ It established a panel consisting of one to three experts which were to be appointed by WIPO’s Arbitration and Mediation Center to efficiently review claims and quickly eliminate cases of clear abuse and bad faith.⁶⁸ The panel’s ability to quickly dispose of cases would also alleviate the congestion in the

---

⁶² See generally id.
⁶⁴ Id.
⁶⁷ Id.
courts caused by the rash of cyber-squatting cases and provide trademark owners a cost effective mechanism to challenging cyber-squatters instead of purchasing the bad faith registration of their own trademark by the cyber-squatter. WIPO’s Arbitration and Mediation Center was the first of many accredited dispute-resolution providers accredited by ICANN.

In less than three months, WIPO’s Arbitration and Mediation Center had received a total of eighty-nine cyber-squatting cases. The procedure requires that each dispute be resolved within forty-five days of filing. Remedies are limited to the cancellation or transfer of the domain name to the trademark holder. A Second WIPO Domain Name Process was adopted less than one year after the First. While the First WIPO Process addressed abusive, misleading, bad-faith registration of personal names, geographical indications, indications of source or geographical terms generally, the Second WIPO Process addressed country names. The Second WIPO Process was completed by October of 2002 and the UDRP was amended to reflect the recommendations made by the Second WIPO Domain Name Process in February of 2003. This process called for a number of expansions, including providing protections for country names.

Since the adoption of UDRP in 1999, the principal provisions have been incorporated into each domain name registration agreement, requiring that the domain name registrant accept the provisions as a condition to the registration of the domain name. The primary purpose of

69See generally id.
70Id.
72Id.
73Id.
75See generally id.
76Id.
the UDRP was to allow for a non-judicial option for trademark owners to bring a dispute quickly and at a more affordable cost through a form of non-binding arbitration utilizing approved dispute resolution providers. Currently, all remedies offered by UDRP are strictly limited to cancellation of the offending domain name or the transfer of the registration to the successful complaint.

A. Uniform Dispute Resolution Proceedings

The UDRP proceedings are the leading dispute resolution mechanism for domain names because they allow a dispute before the panel regardless of where the registrar or the domain name holder or the complainants are located. This essentially allows for jurisdiction on an international scope. The UDRP provides a faster and less expensive resolution to a dispute than a judicial proceeding. A complainant will have a decision within sixty days of filing at a relatively low cost, while still having the option of a judicial remedy.

Prior to obtaining a registration for the domain name, the registrant must consent to the UDRP policies requiring participation in a UDRP proceeding with a third party. Section 4(a) of the UDRP states that “you are required to submit to a mandatory administrative proceeding in the event that a third party (a “complainant”) asserts to the applicable Provider, in compliance with the Rules of Procedure, that (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complaint has rights.”

78 Id.
79 Jurisdiction in a Uniform Dispute Resolution Procedure (“UDRP”) proceeding is consented to as part of the domain name registration agreement.
81 Id. at 248.
The UDRP’s Rules of Procedure require three elements be set forth in the complaint in order for a dispute to move before a UDRP Provider concerning the abusive registration of a protected trademark. These three elements are: the domain name registered must be identical or confusingly similar to a trademark or service mark for which the complainant has rights to; the domain name registrant has no rights or legitimate interests in respect to the domain name before the panel; and the domain name has been registered and is being used with bad faith.

If the complainant owns the trademark in question, this is typically regarded as satisfying the threshold requirement. The first element is often viewed as the standing requirement which requires the domain name to be “confusingly similar” to the trademark and that there is a likelihood of Internet user confusion. Typically, the panel decides this issue by doing an actual visual comparison.

Section 4(a)(ii) of the UDRP requires that the complaint must prove the “respondent has no rights to or legitimate interest in the Domain Names.” The complaint can establish a prima facie showing that none of the three listed circumstance establishing that “legitimate interest or rights apply”; the burden of production will shift over to the respondent to rebut the showing. The three listed circumstances include “before any notice to you [Respondent] of the dispute, your use of, or demonstrable preparations to use, the domain name. . . in connection with a bona fide offering of goods or services; or you [respondent]. . . have been commonly known by the

---

84 Id.
86 Id.
88 Id.
Domain Name”, even if no trademark or service rights have been acquired, or “you [Respondent] are making a legitimate noncommercial or fair use of the Domain Name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trade mark or service mark at issue.”

Lastly, Section 4(a)(iii) requires that the domain name has “been registered and is being used in bad faith.”91 There have been circumstances in which the UDRP panels have found bad faith but they are all without limitation.92 Evidence of registration and use of a domain name in bad faith includes instances indicating you have attempted to sell, rent or otherwise transfer the domain name registration to the complainant who “is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration; or the domain name was registered to prevent the actual trademark owner from reflecting the mark in a corresponding domain name; or the domain name was registered for purposes of disrupting the business of a competitor; or the domain name was registered with the sole intention of attempting to attract Internet users to a website by creating “a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement” of the website.”93

Proving the third element is usually regarded as more difficult, requiring that there be some bad faith element of the domain name in use. Even if the domain name has been acquired prior to the trademark rights vesting in the trademark, this in and of itself does not prevent the finding of identical or confusingly similar marks but it does prove to be a difficult task when

90 Volve Trademark Holding AD v. e-motordealer LTD., WIPO Case NO. D2002-0036 (March 22, 2002).
93 UDRP ¶ (4)(b)(i); ¶ (ii); ¶ (iii); ¶ (iv), available at http://www.icann.org/en/dndr/udrp/policy.htm.
proving bad faith mainly because there were non-existent trademark rights at the time of the
domain name registration.\textsuperscript{94}

ICANN sets forth a non-exclusive list of bad faith indicia in an effort to guide
complainants in successfully meeting the third element of the UDRP procedures for arbitration in
order to prevail.\textsuperscript{95} ICANN states that proof of the legitimate interest should include whether the
name used in the domain name is connected to the “bona fide offering of goods or services”;
whether the domain name holder is “commonly known by the named used as a domain name”; or
whether the domain name holder is making a “legitimate non commercial or fair use of the
domain name without intent to divert consumers or tarnish the trademark in question.”\textsuperscript{96}

A party who is dissatisfied with the outcome of the UDRP proceeding may commence a
separate legal proceeding in a court of competent jurisdiction.\textsuperscript{97} If UDRP has ruled to cancel or
transfer the domain name registration, the domain name registrar will implement that decision
with ten business days unless it receives official documentation indicating that the registrant has
taken judicial actions.\textsuperscript{98}

In short, the UDRP proceedings were essentially created to address a narrower group of
cases involving “abusive registration” rather than every action involving domain names.\textsuperscript{99}
Therefore, the dispute services do not extend to cases where the registered domain name is

\textsuperscript{94} Many decisions have held that the registration of domain names prior to the vesting of the trademark rights
would not have been in bad faith because the registrant would not have known, nor contemplated the
complainant’s non-existent rights in the trademark. \textit{E.g.,} Digital Vision, Ltd. \textit{v.} Advanced Chemill Systems,
\textsuperscript{95} See generally Mary LaFrance, Understanding Trademark Law 237-249 (2009).
\textsuperscript{96} UDRP ¶ 4(c), available at \url{http://www.icann.org/en/dndr/udrp/policy.htm}.
\textsuperscript{97} Mary LaFrance, Understanding Trademark Law 248 (2009).
\textsuperscript{98} Id.
\textsuperscript{99} Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy, ICANN (Nov. 9,
2011, 10:45am) \url{http://www.icann.org/udrp/udrop-second-staff-report-24oct99}. 
subject to a legitimate dispute, or where the trademark violation is considered an infringement or dilution.\textsuperscript{100} This is considered a major attraction of the UDRP; it is an established inexpensive administrative dispute resolution procedure for a narrow group of cases providing relief faster than judicial proceedings.\textsuperscript{101}

\textbf{B. Recent developments in the Uniform Dispute Resolution Proceedings}

By the end of 2001, roughly two years after the UDRP was launched, some one thousand, five hundred and six cases were brought before the UDRP providers covering over six thousand domain names.\textsuperscript{102} On May 20, 2003, WIPO received its five thousandth case under the UDRP proceedings which, in total, covered over fifteen thousand cases of cyber-squatting.\textsuperscript{103} Thus, by late May of 2003, WIPO had seen over twenty thousand cyber-squatting domain name cases.\textsuperscript{104} The Director General of WIPO, at that time the Deputy Director General, in a press release accounting the five thousandth case, stated that the UDRP trend is “encouraging and indicates that the expedited on-line dispute resolution service has been effective in dissuading Internet pirates. . .” and that efforts will continue to “ensure that the Internet becomes a secure market place for people to do business.”\textsuperscript{105}

In 2004, it was recognized that the issue of abusive registration is primarily directed to “high-value brands.”\textsuperscript{106} It was said that reducing the practice of cyber-squatting is an “important

\textsuperscript{101} See Generally WIPO Receives 5,000\textsuperscript{th} Cybersquatting Case Under UDRP, World Intellectual Property Organization (Nov. 15, 2001, 10:00pm) \url{http://www.wipo/int/pressroom/en/prdocs/2003/wipo_upd_2003_103.html}.
\textsuperscript{102} Id.
\textsuperscript{103} Id.
\textsuperscript{104} Id.
\textsuperscript{105} Id.
element in enabling the Internet to develop as a secure and reliable environment which inspires confidence” and to support that, over eighty percent of the cases that went before UDRP involving cyber-squatting were decided in favor of the trademark holder.\(^{107}\)

Efforts continued in 2005 when another statement discussing online mechanisms playing an essential role allowing for basically world-wide dispute service in any language at any time was released.\(^{108}\) With the introduction of seven new gTLD’s in mid-2005, WIPO prepared a response to ICANN’s request for a comprehensive strategy to prevent cyber-squatters in the new expansion of domains.\(^{109}\) It is here that WIPO discussed its experience thus far with the UDRP proceedings and suggested that while case filings have been somewhat stable, additional mechanisms need to be used to prevent the abusive registration during the introductory phase of these new gTLD’s, thereby strengthening the ability to combat cyber-squatting cases.\(^{110}\)

In a 2006 press release, WIPO reported a twenty percent increase in the number of cyber-squatting cases brought before UDRP.\(^{111}\) Then again in a 2007 press release, WIPO stated another increase in cyber-squatting cases which reached twenty-five percent since the end of 2006.\(^{112}\) It wasn’t until March of 2009 that trademark holders saw any change in the main UDRP proceedings. In December of 2008, WIPO proposed to ICANN an e-filing system for the UDRP

\(^{107}\) Id.
\(^{110}\) See generally id.
process. Essentially, since WIPO recognized that Internet-based communications were increasing at rapid speeds, it moved to eliminate paper filings and improve the timeliness of UDRP proceeding. WIPO also updated the panel decisions on-line allowing for various searches to track developments in cases involving domain names.

Recently, WIPO launched another addition to its on-line tools allowing for an easily accessible search tool to locate records relating to all internationally protected trademarks, as well as any other state emblems including names and abbreviations. The Director General stated that this on-line search tool was an “important part of WIPO’s efforts to facilitate access to such valuable assets and reflects the Organizations commitment to narrowing the global knowledge gap by improving access.” In addition to the search tool, most recently, WIPO announced a new major update to the overview of WIPO which reflects necessary information for both the trademark holders and counsel on an international level to determine their “bearings in cyber-squatting jurisprudence.”

V. CONNECTING TO END AN ERA OF CYBER-SQUATTING

The world today relies on internet usage more than ever to do everyday functions from personal banking to ordering prescription medication to starting a business. For these very reasons, it seems strange that the process of registering a trademark can be so disconnected from the process of registering a domain name.

114 See generally id.
115 See generally id.
117 See generally id.
The issues which stem from this disconnection have been addressed when ICANN and WIPO joined forces in the creation of UDRP to provide for a relief method for trademark holders who have been attacked by cyber-squatters. Rather than continuing to develop remedies to this disconnection, a solution to cyber-squatters needs to be addressed.

A. *Publication for Opposition*

In the United States, within 13 months of a trademark application being filed with the PTO, the application is published for opposition in the Official Gazette.\(^{119}\) This enables any third party who feels that they will be harmed if the registration of the trademark is granted a right to oppose the application before the Trademark Trial and Appeal Board (“TTAB”).\(^{120}\) The mark is published in the Official Gazette for a time period between one to three months, thereafter registration will only be granted if no opposition has been made, or the opposition made is unsuccessful.\(^{121}\) For an opposition to be brought before the TTAB, the party must have a “real interest” in the mark and proceeding meaning, for example, they must either be claiming priority of the mark, or a commercial interest in the mark.\(^{122}\)

This process of having an open publication of a trademark prior to being given registration allows a third party to bring an opposition before a board if they feel the applicant’s falls under one of the many bars to registration found in the Lanham Act. This simple process, publishing applications, can be altered to fit the needs of the domain name registration practice. Here, in domain name registration, ICANN could take the applicant’s domain name and publish it in a similar gazette accessible on a World Wide basis via the Internet and allow for a one to

---


\(^{120}\) *Id.*

\(^{121}\) *Id.*

\(^{122}\) Mary LaFrance, Understanding Trademark Law 107 (2009).
three month period of opposition prior to granting the domain name. Many would argue that a
three month period would affect the growth of the business with the fast paced Internet
development however, the initial period could allow for a one month opposition timeframe. If
after one month, the applicant hasn’t received oppositions from parties with standing, the domain
name could be granted. If however, the applicant received an opposition, the domain name
should remain published for a total of three months allowing full review for the domain name
before a designated appeal board.

   Similar to other UDRP proceedings, the party opposing registration could file an appeal
through an on-line database where the designated appeal board could access and review all
related files. Essentially, the appeal board could meet at any time, any place, making a decision
regarding the opposition all through an on-line procedure. This very idea could potentially
eliminate clear cases of abusive registration of domain names by allowing major corporations
and business an opportunity to monitor domain names confusingly similar to their trademarks
which are being registered by cyber-squatters.

B.  WIPO Verification

   Protocols are sets of agreements used to amend or supplement a treaty between various
international organizations. Here, a seemingly realistic and practical solution to address the rise
of cyber-squatting cases would be for ICANN to enter into a protocol with WIPO authorizing
WIPO to assist in the limited verification process in place now. If a protocol is in fact put in
place, this could allow WIPO to ensure that the registrant of the domain name has some
legitimate interest - some affiliation - with the domain name they are attempting to register. By
verifying affiliation, WIPO can assist in reducing the amount of cyber-squatters who
intentionally register domain names just to later profit from the sale of that domain name to the trademark holder as well as reduce the amount of cyber-squatters attempting to siphon customers from well-known trademarks.

C. Deterrence Factors

Additionally, while UDRP proceedings call for the cancellation or transfer of the domain name found to be abusively registered, measures can be taken to prevent future cyber-squatting by the liable parties. If an individual or entity is found to be a cyber-squatter in a UDRP proceeding, their name should be placed on a registry which can be kept private by ICANN in an effort to bar future registration. This registry should be kept private purely for policy reasons. Typically, placing the contact information of the general public on-line is not regarded as a customary practice. Additionally, in the event of corruption at any point throughout the UDRP proceedings, one would not want an individual publicly placed on the cyber-squatter registry if the showing of corruption could be legitimately made. Proving corruption has proven throughout the years to be a difficult task. If an individual is placed on a public registry, rather than a private registry, it could take years for that individual to prove corruption behind a domain name decision, potentially affecting all aspects of his business if such corruption could even be eventually proven. Therefore, the registry of prior cyber-squatters should be kept private.

Once this private registry is in place, ICANN would be able to run a simple search of the individual or entity name to see if they receive any hits on their private database or through past UDRP panel decisions. Barring future registration of guilty cyber-squatters would not only prevent the same cyber-squatter from committing the acts more than once, it would deter others

123 Corruption can be any abuse of a position of trust to gain an undue advantage. Here, the dispute resolution provider may be corrupt, using his power entrusted in him to grant a holding in favor of the party who will at a later date supply the provider with a large sum of money or a future favor.
from registering a mark without conducting simple background research to find out if their domain name is associated with any current businesses or organizations. Concerns associated with this bar could be addressed in a judicial proceeding. Often, a party dissatisfied with a UDRP decision will file an action initiating a judicial proceeding. A party can have his domain name case addressed as well as his bar to future registration. The deterrence factor combined with the prevention of repeat offenders would decrease the amount of cases before the UDRP providers. More often than not, people are deterred from committing fraudulent acts when they are aware of the serious consequences when caught.

Currently, the UDRP Rules of Procedure do not allow for financial remedies.\textsuperscript{124} In addition to a bar from future registration, if a domain name registrant is found to have registered the domain name in bad faith in an attempt to either sell the domain name to the trademark owner and profit off that sale or siphon customers from the true trademark owner, financial remedies should be made available to the trademark holder in the form of a flat fine to be paid by the cyber-squatters. This would be an effective deterrence for cyber-squatters who have a clear showing of abusive registration. There should be a formula used to calculate a fine placed on the cyber-squatter which includes factors such as the length of time the domain name was used by the cyber-squatter and may include the amount the cyber-squatter profited. This could either be determined by the amount the cyber-squatter paid for registration versus the amount the cyber-squatter attempted to sell the domain name for or by a showing of actual profit.

Perhaps the biggest change yet lays in the very idea of the Internet. Founders of the Internet spent years developing the idea of endless, uninterrupted connections between people and businesses around the world. Therefore, it is only reasonable that measures are taken to

\textsuperscript{124} Richard Stim, Trademark Law 188 (2000).
mend the very lack of connection between the domain name registries and the trademark registration process allowing for these abusive registration cases.

D. *Rise of New Generic Top-Level Domains*

ICANN’s primary goals are “preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet,” as well as, “respecting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination.” ICANN also focuses on the introduction of domain names and promoting competition in the registration of domain names where “practicable and beneficial” to the public interest. Therefore, it was foreseeable that eventually ICANN would allow for new gTLD’s. However, the application procedure and standards are much different than seen in the past. The reasoning behind the significant background screening and intensive application process for new gTLD’s couples with the underlying standards used to develop ICANN’s goal in the expansion of the internet. These very standards should be applied to develop a more stringent domain name application process.

**VI. THE NEW GENERIC TOP LEVEL DOMAIN APPLICATION PROCESS**

Amongst the failed efforts to combat the increasing number of cyber-squatting cases, ICANN is attempting to expand the Internet even further. ICANN will be opening an application period for new gTLD’s in order to promote the economy by attempting to find the newest “.com”. ICANN is looking to extend the Internet possibilities, a process which once allowed for two dozen gTLD’s could now allow for hundreds of new registries, hopefully achieving

---

125 See generally *About*, ICANN (Nov. 18, 2011, 10:30am) [http://www.icann.org/en/about/](http://www.icann.org/en/about/).

126 *Id.*
participation from around the world. One would only assume that this will open the door to hundreds to thousands of new cyber-squatting cases with the possibilities of abusive registration of domain names eventually being unlimited. Even if ICANN allows a small number of new gTLD’s, this allows cybersquatters to abusively registrar dozens of new identical or confusingly similar marks.

ICANN is allowing any established entity to apply for a new gTLD from January 12, 2012 to April 12, 2012 so long as they can show they have the ability to create and operate a registry business able to support an Internet domain name system. The business entity will be running a piece of visible Internet infrastructure and thus will need to have the resources to do so.

There have been pre-established requirements included within the application review process. The application will be reviewed upon completion by allowing a public portion section initially. The public comments are for review purposes and will not be considered formal objections; they will merely help the panel determine whether to grant or deny the new gTLD.

The initial evaluation is to be done concurrently with the public portions section of the application review. The initial evaluation essentially includes two parts; the background screening consisting of a string review and an application review. The string review is performed

---

129 See generally Id.
130 ICANN, gTLD APPLICANT GUIDEBOOK, MODULE 1 §1 (2011) HTTP://NEWGT LDS.ICANN.ORG/APPLICANTS/AGB.
131 ICANN, gTLD APPLICANT GUIDEBOOK, MODULE §1.1.2.3 (2011) HTTP://WWW.ICANN.ORG/EN/TOPICS/NEW- GTLDS/INTRO-CLEAN-19SEP11-EN.PDF.
132 Id.
to determine if the gTLD the applicant has applied for will cause any problems with a reserved name.\textsuperscript{133} The application review will consider the required technical, operational and financial capabilities for the entity applying for registration.\textsuperscript{134} ICANN will publish its findings from the initial evaluation, which will be followed by a period of time allowing for formal objections.\textsuperscript{135} ICANN has determined that any party with standing to object may formally object to the grant of the gTLD.\textsuperscript{136} If a formal objection is given to a gTLD, the dispute resolution services will proceed. If the applicant successfully completes all of the prior steps, the applicant will enter into the next phase, which requires that a series of agreements be signed including the registry agreement.

ICANN has predicted a number of possible scenarios based on different applicants passing and/or failing certain steps and estimated certain timelines in which an applicant will be notified of approval or denial.

The review process for each application is much more complex and detailed compared to that of the basic domain name registration. Essentially, for an applicant to be granted a new gTLD, it must be an established corporation, organization or institution that is in good standing. An application from an individual will not be considered for a new gTLD, nor will either pending joint ventures or other presupposing future formation of a legal entity.\textsuperscript{137} The application calls for information including but not limited to information relating to the organization or

\textsuperscript{133} ICANN, gTLD APPLICANT GUIDEBOOK, MODULE §1.1.2.5 (2011) \url{HTTP://WWW.ICANN.ORG/EN/TOPICS/NEW-GTLDs/INTRO-CLEAN-19SEP11-EN.PDF}.
\textsuperscript{134} Id.
\textsuperscript{135} Id.
\textsuperscript{136} ICANN, gTLD APPLICANT GUIDEBOOK, MODULE §1.1.2.6 (2011) \url{HTTP://WWW.ICANN.ORG/EN/TOPICS/NEW-GTLDs/INTRO-CLEAN-19SEP11-EN.PDF}.
\textsuperscript{137} ICANN, gTLD APPLICANT GUIDEBOOK, MODULE §1.2.1 (2011) \url{HTTP://WWW.ICANN.ORG/EN/TOPICS/NEW-GTLDs/INTRO-CLEAN-19SEP11-EN.PDF}. 
business entities legal establishment as well as the identification of their directors, officers, partners, and major shareholders.

Additionally, the amount of back-screening is extensive compared to the essentially non-existent screening done when applying for domain names. ICANN will be conducting a background test on both the entity and individual level in a strong effort to confirm actual eligibility. They will look for both general business diligence as well as criminal history along the lines of “crimes of trust”.  

The biggest step which ICANN has taken to minimize cyber-squatting cases is the actual process of screening for prior cyber-squatting behavior associated with the entity members. ICANN will be reviewing prior UDRP panel decisions as well as other legal publications as they deem “financially reasonable”. ICANN has placed strong emphasis on the background screening in an extended effort to “protect the public interest in the allocation of critical internet resources”.  

ICANN stated that it reserved the right to deny an otherwise qualified application based on any of the information found during this stage of the application review. Subject to application approval, the entity will have to agree to all of the terms and policies being set forth by ICANN especially designed for the new applications of gTLD.  

**VI. UNDERLYING STANDARDS**

ICANN has projected that they can receive up to one thousand new gTLD per year, which would allow for two to three hundred new Top-Level Domain Names. ICANN’s idea

---

138 Crimes of trust standard is typically used throughout the banking and finance industry; id.
139 Id.
140 Id.
behind expanding the Internet and allowing for further economic development seems like the ever promoted goals for the future stemming from Internet developers. However, it seems that new connections should not be opened until all of the loose ends are connected.

ICANN, in regards to their application process for new gTLD’s, seeks to protect the public while promoting the expansion of the Internet to achieve a successful growth in the economy. ICANN is using public comments as a means of developing and implementing their new policies. ICANN states that they are completely dedicated to preserving the security and stability of the Internet while effectively promoting competition, achieving representation of a global internet community by “developing policy appropriate to its mission through bottom-up, consensus-based processes.” Meaning, the new gTLD application process includes background scans and participation by stakeholder groups in various public discussions. All of these underlying concepts are the very reasons domain name registries were created. Part of the domain name registration process is to check to see if the domain name has previously been registered, and if not, it is registered. This is kept simple to promote registration in order to promote the growth of the economy; the very idea of economic growth is built into security and stability. Background screens as simple as checking whether the registrant has an affiliation with the entity they are attempting to register, or requiring a submission of proof of trademark ownership would drastically reduce cyber-squatting. If one protects the consumer from confusion, which is the very essence of trademark law, one allows for growth and promotion of the economy.

VII. CONCLUSION
Intellectual Property promotes creativity, inventions, artistic works, and industrial designs. In order for technology to continue to develop, these rights need to be protected. WIPO was established to protect these very ideas and allow for growth through Intellectual Property.

Throughout this article, the reasoning behind the establishment of WIPO has been discussed, as well as membership and organizational goals. In addition, the dispute resolution procedures were discussed from the time at which they were initially developed with the policy reasons promoting their development to the current state they are in. This article discussed how WIPO initiated a dispute resolution service for domain names that were abusively registered against a trademark holder who has legitimate rights to the domain name.

Next, this article discussed how, rather than continuing to develop a dispute resolution service, actions need to be taken to reduce the amount of abusive registration trademark holders are faced with. In this part, several arguments are made suggesting the addition of verification processes and fines for abusive registration as well as bars to future registration when clear cases of abusive registration are presented.

Additionally, this article discusses ICANN’s new application process in an attempt to find the next big “.com” to promote the development and expansion of the Internet. Here, the principals underlying this expansion are applied to the already existing domain name registry system suggesting similar goals and presenting the agreement that these very processes being used for the new applications should be applied to the existing domain name applications.

Instead of waiting for an individual to bring a claim before UDRP, this article suggests the idea that it would be better to address the initial problem by incorporating a verification process within the domain name application similar to that of the new gTLD applicants.
Additionally, smaller steps can be taken to deter cyber-squatters by imposing mandatory fines when the UDRP finds a clear case of abusive registration or more simply, and by banning a cyber-squatters of future domain name registration, thereby eliminating repeat offenders. Therefore, WIPO and ICANN through the use of UDRP, can attempt to prevent another increase in the amount of cyber-squatting cases for the year 2012.