Archives of Business Research – Vol.6, No.12
Publication Date: Dec. 25, 2018
DOI: 10.14738/abr.612.5786.
Singh, H. P. (2018). Domain Name Disputes and Their Resolution under UDRP Route: A Review. *Archives of Business Research, 6(12),* 147-156.

Domain Name Disputes and Their Resolution under UDRP Route: A Review

Dr. Harman Preet Singh
Department of Management and Information Systems,
College of Business Administration,
University of Hail, Kingdom of Saudi Arabia

ABSTRACT

Domain names have a dual role in today's internet driven market place – to map IP addresses and to act as identifier of trademark of a company. Unlike trademarks, domain names are not sufficiently protected by the laws of a country. There is no uniformity to protect domain names among the laws of various countries. In order to protect the domain names and bring uniformity, ICANN developed the Uniform Domain Name Resolution Policy (UDRP). In this research, the various kinds of domain name abuses are identified. The application of UDRP, domain name registration process and dispute resolution service process are examined. The major domain name dispute cases resolved under UPRP by WIPO are studied. It has been found that UDRP is applicable to generic top level domains (gTLDs) and new gTLDs. It is much less relevant for country code top level domains (ccTLDs). The losing party still has the option of appealing to a court of competent jurisdiction in case of gTLDs and new gTLDs. However, this option is seldom exercised. In order to protect the domain names in a better way, there is a need to bring uniformity to domain name laws of various countries. ICANN should formulate a model domain names dispute resolution law for adoption by various countries. Also, there is a need to strengthen the UDRP.

Keywords: Cybersquatting, ccTLDs, domain name disputes, DNS, gTLDs, ICANN, typo-squatting, UDRP

INTRODUCTION

In the current internet driven marketplace, trademark have emerged as the vital tool of e-commerce. In the offline marketplace, trademark owners have exclusive rights over their products or services that allow them to distinguish from their competitors (Ngoc, 2011). Companies are increasingly seeking to leverage the offline reputation of their trademarks to the online world (Lipton, 2005). This is done with the help of the Domain Name System (DNS). DNS provides recognizable names to numerically addressed internet resources.

Every computer on the internet has unique numerical address resource, called Internet Protocol (IP) address. These IP addresses are hard to remember. DNS makes it easy to remember websites instead of esoteric IP addresses. So, instead of remembering 207.151.159.3, it is easier to remember www.internic.net (ICANN WHOIS, 2018). Also, domain names are increasingly used as business identifiers in internet driven marketplace. They have a significant impact on online brand building, advertising, search engine optimization etc. (WIPO, 2010).

Trademark is protected by the laws of the country where it is registered. So, it can be registered in multiple countries. On the other hand, domain name is accessible throughout the world. Due to this universal connectivity, domain name requires universal exclusivity. Also, laws of a country might be inadequate to protect the domain name and there is no uniformity among the laws of various countries (Bach, 2001).

DOMAIN NAME SYSTEM

Domain Name System (DNS) is essential to handle the growing number of internet users. It is a global addressing system which translates domain names into corresponding IP addresses. It is organized as a hierarchical tree like structure, where each domain is a node in a tree. The root node of the tree is called the DNS root domain (.). Under this, there are sub-domains like .com, .edu, .gov, .mil etc. These sub-domains are called Top Level Domains (TLDs). The responsibility for managing each TLD is delegated to a particular organization, called registry operator. Under the TLDs, there are Second Level Domains (SLDs) (such as "example" in "www.example.com"). Under SLDs, there could be third-level domains (like "www" in "www.example.com").

DNS is managed by Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization (Kruger, 2014). Under DNS, the domain names can be broadly categorized into following types:

- Generic Top Level Domains (gTLDs) – These domains are used by a particular class of organizations for different purposes. Each gTLD bears 3 or more letters (such as .com, .net, .org etc.). gTLDs could be sponsored top level domains (sTLDs) or unsponsored top level domains (uTLDs). sTLDs are restricted and run by a sponsor, who represents a specific community of users. uTLDs are unrestricted, open and governed by ICANN policies. In 1980's, ICANN established 7 gTLDs - 4 restricted (.edu, .gov, .int, and .mil) and 3 unrestricted (.com, .org, and .net). In the year 2000, 7 additional gTLDs were created by ICANN – 3 sponsored (.aero, .coop, and .museum) and 4 unsponsored (.biz, .info, .name, and .pro). In 2004, ICANN approved 7 sponsored gTLDs - (.asia, .cat, .jobs, .mobi, .post, .tel, and .travel) (Katz et. al., 2010). In June 2011, ICANN announced the creation of new gTLDs to enhance competition and consumer choice (ICANN, 2011a). In 2014, new gTLDs became available to entrepreneurs. This enabled them to create new gTLDs that they could control on their own. At present, there are unlimited amount of gTLDs. Business owners can pay to have their websites end on gTLDs like .xyz, .toys, .soy, .wed, and more (Roesler, 2015). According to Namestat (2018), the top 10 biggest selling gTLDs include .top, .loan, .xyz, .club, .online, .vip, .site, .ltd, .work and .shop. Along with new gTLDs, introduction of Internationalized Domain Names (IDNs) by ICANN also made significant changes to the global DNS landscape. IDNs are formed by taking characters from different scripts like Arabic, Chinese, Cyrillic or Devanagari (IDN, 2018). These developments in gTLDs have created new opportunities to engage with customers, drive revenue and promote brands online (Roesler, 2015).
- Country Code Top Level Domains (ccTLDs) – They are assigned to each country and administered independently by nationally designated registration authorities. Each of the ccTLD bears 2 characters of country code derived from the ISO 3166-1 standard for country codes https://www.iso.org/iso-3166-country-codes.html). Examples include: '.au' for Australia, '.br' for brazil, '.in' for India, '.jp' for Japan, '.gr' for Germany, '.us' for United States, '.uk' for United Kingdom, '.sa' for Saudi Arabia etc. The administration of a ccTLD is left to the individual country concerned. Thus, the policies and rules of each ccTLD for allocating domain names are distinct from the other. ICANN has only a consultation role in these domain registries but is in no position to regulate the terms and conditions of how a domain name is allocated or who allocates it in each of these country level domain registries. Some countries allow anyone in the world to acquire a domain in their ccTLD. Other countries (like United Kingdom, Mexico, and United States etc.) allow only residents to acquire a domain in their ccTLD (OECD, 2006). There were 252 ccTLDs in use as of June 8, 2017 (WIPO, 2017). Most corporations apart from registering their trademark names and some of their core brands as gTLD's, also register them as ccTLD's in certain select countries where they foresee business

potential. For example, Yahoo.com is a gTLD. However, yahoo.co.in is a ccTLD registered in India and yahoo.co.fr is a ccTLD registered in France.

- In addition to gTLDs and ccTLDs, there is another TLD .arpa. It is used for technical infrastructure purposes. It is administered by ICANN in cooperation with the Internet technical community under the guidance of Internet Architecture Board (http://archive.icann.org/en/tlds/).

OBJECTIVES OF THE STUDY

The following are the objectives of this study:

- To identify the various kinds of abuses of domain names
- To appreciate the role of UDRP to resolve domain name disputes
- To study cases of various domain name disputes resolved by WIPO
- To examine the limitations of UDRP to resolve domain name disputes

ABUSES OF DOMAIN NAMES

With the explosion of Internet, companies are trying to leverage the goodwill obtained by their trademarks offline in the online cyber-space. Domain names are analogous to offline trademarks. They indicate quality of a company and serve as its goodwill repository (Ahmed, 2010). However, there is a lack of connection between the systems that register trademarks and domain names (WIPO, 1998). So, some miscreants try to use this short-coming and do abusive registration of domain names. Abusive registration of domain names happens when miscreants register domain names in which they have no legitimate interest and they register in it bad faith. When a domain name is confusingly similar to a trademark, it has the effect of confusing the Internet browsers and the users.

Types of Abuses of Domain Names

The abuses of domain names are of the following types:

- Cybersquatting – Registering a domain name completely identical with a well-known trademark is called cybersquatting (Chissick and Kelman, 2002). The cyber-squatter can then try to extract large sum of money from the trademark owner in return for transferring the domain name (Mercer, 2000).
- Typo-squatting – It occurs when a party registers a trademark which is very similar to a well-known trademark or domain name. The purpose of this is to capitalize on Internet users typographical errors when entering a web address (Holland, 2005; Szurdi and Christin, 2017).
- Cyber piracy – It involves integration of trademarks in domain names in order to attract more traffic to the related web-pages associated with a common domain name (Ventsislav, 2012).
- Pseudo cybersquatting – It is the act of registering a domain name analogous to a trademark without the intention of using it. The domain name is not connected with any active website or online webpage. This is also called blocking registration. This practice intends to block the legitimate trademark holders from using the domain name (Ventsislav, 2012).
- Cyber smearing – It is the act of registering derogatory domain names, which contain trademarks joined to other words with negative connotations. Individuals who want to represent a trademark in a negative way can use this practice (CMS, 2007). One of the practices involve adding the word “suck” as a suffix to a trademark to defame it (Koščík, 2008)
- Reverse domain name hijacking – It occurs when a trademark owner attempts to secure a domain name by making false cybersquatting claims against a rightful owner using a trademark registration as a leverage (Rustad, 2013).

- Registration by another party upon inadvertent failing to renew domain name by legitimate party – When a company registers a domain name, it is given that domain for a particular amount of time. This time is typically 1 year. The company has to pay the renewal fees according to its contractual agreement with the registrar. Another party can try to take advantage of this lapse by the legitimate trademark holder and register the domain in its name. It may further try to offer the domain back to the legitimate trademark holder in return for large sum of money (Levine, 2012).

Remedies for Abuses of Domain Names

In case of abuses of domain names, following remedies are available to the affected party:

- Trademark holder can try to buy the domain name from the cyber-squatter. However, this is expensive. Also, it is unprofessional as it involves giving in to mal-practices.
- Trademark proprietor can file a lawsuit in court of law based on national legislation for trademarks, unfair competition and other related legislations. However, this is an expensive and slow process.
- Trademark proprietor can go for arbitration proceedings under Uniform Domain Name Resolution Policy (UDRP) developed by ICANN.

UNIFORM DOMAIN NAME RESOLUTION POLICY

In order to resolve the domain name disputes, UDRP was developed by ICANN in August 2009. Under UDRP, most types of trademark-based domain-name disputes must be resolved by agreement, court action, or arbitration. After resolution, registrar of companies can cancel, suspend, or transfer a domain name. The policy offers an expedited administrative proceeding for trademark holders to contest abusive registrations of domain names. UDRP endeavors to create a process that is faster and cheaper than the legal system. The UDRP proceedings are conducted by arbitrators having expertise in trademark law. This guarantees that UDRP cases are decided by the experts, which may or may not happen in courts (WIPO gTLDs, 2018).

Application of UDRP

UPRP policy provides legal framework for resolution of domain name disputes between registrant (end user) and third party. UDRP currently applies to various gTLDs (like .aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and travel) and new gTLDs (WIPO gTLDs, 2018). 76 ccTLD's have adopted UDRP on a voluntary basis. The countries include Antigua and Barbuda (.ag), Columbia (.co), Ecuador (.ec), Fiji (.fj), Loas (.la), Malawi (.mw), Panama (.pa), Pakistan (.pk), Puerto Rico (.pr), Romania (.ro), Somalia (.so), Tajikistan (.tj) etc. (WIPO ccTLDs, 2018). Some countries have adopted their own alternative dispute resolution mechanism which is unrelated to UDRP. Examples include Canada's Domain Name Dispute Resolution Policy managed by Canadian Internet Registration Authority (CIRA) (https://cira.ca/) and UK's Domain Dispute Resolution Service managed by Nominet (https://www.nominet.uk/). India's Dispute Resolution Policy (INDRP) is on lines of UDRP and the relevant provisions of the Indian IT Act 2000 (INDRP, 2005). Some countries like Austria have not adopted any alternative dispute resolution mechanism. So, cases can only be filed in Austrian courts to resolve domain name disputes.

Domain Name Registration Process

Domain name registration processes are governed by 2 main contractual relationships. They are:

- Agreement between ICANN and registrar under Registrar Accreditation Agreement (RAA) – Registrar needs to enter into binding RAA with ICANN to be accredited and offer domain name services to registrants. RAA states the registrar responsibilities in

the DNS and provides procedures to manage the registrants. RAA does not cover ccTLD registrations. This is because ccTLD registry operators manage accreditation of registrations for ccTLDs (ICANN, 2010). Every gTLD and new gTLD in the world has a RAA in force with the ICANN. So, ICANN has administrative authority over entire DNS for gTLDs and new gTLDs (Michaelson, 2016). RAA provides "flow through" pre-requisite. Under this pre-requisite, registrars must include similar provisions in their agreements with registrants. So, registrants become bound to follow the ICANN policies and specifications. The term of the RAA is 5 years and can be renewed by ICANN if registrar met obligations under previous RAA. Registrar can also terminate a RAA by giving 30 days advance notice to ICANN ((ICANN, 2011b). Disputes arising under RAA can be resolved in a court of competent jurisdiction or by an arbitration conducted under the rules of American Arbitration Association (ICANN, 2009).

- Agreement between registrar and registrant under the umbrella of Registrar Accreditation Agreement (RAA) – The UDRP is incorporated by the registration agreement that the registrant had with the registrar at the time of registering its domain name. By virtue of the incorporation of the UDRP into the registration agreement, the registrant submits itself to the jurisdiction of the approved dispute resolution providers and binds itself to the UDRP (ICANN, 2011b). The registrar has to ensure that the registered domain name is available and it will match IP address with the domain name. Registrant can keep the registered domain name, provided the renewal fees has been paid and no infringement of intellectual property of others has taken place (Caruana, 2015).

Dispute Resolution Service Providers

According to the UDRP policy, any person or entity with rights in a trademark can complain to dispute-resolution service providers, which can be corporations or non-profit organizations. Currently, the following are the approved dispute resolution service providers (ICANN, 2018):

- Arab Center for Domain Name Dispute Resolution Center (ACDR)
- Asian Domain Name Dispute Resolution Centre (ADNDRC)
- The Czech Arbitration Court Arbitration Centre for Internet Disputes (CAC)
- National Arbitration Forum (NAF)
- World Intellectual Property Organization (WIPO)

Each provider has a list of panelists from which either one or three are chosen to decide a particular domain name dispute.

Dispute Resolution Service Process

In the event that a trademark holder considers that a domain name registration infringes on its trademark, it may initiate a proceeding under UDRP. The UDRP permits complainants to file a case with a dispute resolution service provider, specifying, the domain name in question, the respondent or holder of the domain name, the registrar with whom the domain name was registered and the grounds for the complaint etc.

According to paragraph 4(a) of UDRP, a trademark owner has the right to apply to the ICANN dispute resolution service providers if three elements are met. These elements are (ICANN, 1999):

- Respondents domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- Respondent has no right or legitimate interest in respect of the domain name; and
- Respondent's domain name has been registered and is being used in bad faith.

Paragraph 4(b) of the UDRP policy stipulates certain inclusive factors for determining bad faith registration and use, which are stated below (ICANN, 1999):

- Registering the domain name with the primary purpose of subsequently selling it at a profit.
- Registering the domain name primarily for the purpose of disrupting the business of the competitor.
- Registering the domain name in order to prevent the owner of the trademark from reflecting the mark in a corresponding domain name.
- Using the domain name to attract Internet users to one's Web site by creating a likelihood of confusion with the complainant's trademark.

After the domain name dispute is resolved, it could either be transferred or the complaint could be denied. It is also possible to seek cancellation of the domain name. There are no monetary damages applied in UDRP domain name disputes, and no injunctive relief is available. The losing party can bring a lawsuit against the winning party in a court of competent jurisdiction within 10 business days (ICANN, 1999). The accredited domain name registrars – which have agreed to abide by the UDRP – implements the dispute resolution panel's decision after waiting for a period of ten business days. The panel decisions are mandatory in the sense that accredited registrars are bound to take the necessary steps to enforce a decision, such as transferring the name concerned. However, under the UDRP, either party retains the option to take the dispute to a court of competent jurisdiction for independent resolution. But this option is exercised very seldom.

MAJOR DOMAIN NAME DISPUTE CASES RESOLVED UNDER UDRP BY WIPO

WIPO is the leading domain name dispute resolution service provider (https://www.wipo.int/amc/en/domains/gtld/). So, the cases resolved by WIPO are examined in this section.

Major domain name dispute cases resolved under UPRP by WIPO are presented in Table 1 below:

Table 1: Major Domain Name Dispute Cases Resolved Under UDRP by WIPO

Case	Details
Philip Morris Incorporated v. r9.net (2007)	This is a case of cyber-squatting. Marlboro marks are well recognized trademarks in United States. They are the trademark of complainant (Phillips Morris, USA). The respondent (r9.net) registered domain name <marlboro.com> through ICANN. Complainant alleged that the respondent has misappropriated the famous Marlboro marks by registering the domain name. It was alleged that the registered domain name is confusingly similar to its trademark. The complainant also alleged that the respondent has no legitimate interest in the Marlboro marks and have registered them in bad faith. The respondent did not reply to the complainant contentions. The WIPO panel found the arguments of complainant valid and transferred the domain name <marlboro.com> to Phillips Morris, USA.
Shell Trademark Management B.V. v. Domains - Best Domain (2003)	This is a case of typo-squatting. Shell International Petroleum Company (complainant) is a well-known company in United Kingdom and other countries. It owns and operates oil and gas refineries. The respondent (Domains - Best Domain) registered the domain name <wwwshell.com> through ICANN. The complainant stated that the registered domain is confusingly similar to its trademark "Shell". The complainant alleged that respondent is a cyber-squatter as it linked the <wwwshell.com> domain name to www.abortionismurder.org website. The complainant also submitted that the respondent has no legitimate interest in the domain name. Further, the complainant stated that respondent has registered the domain name in bad faith and offered to sell the domain to complainant for $549,000. The respondent did not reply to the complainant submissions. The WIPO panel found the assertions of complainant true and transferred the domain name in its favor.
SAFE Credit Union v. Mike Morgan (2006)	This is a case of cyber piracy. The complainant is SAFE Credit Union and respondent is Mike Morgan. The respondent registered the domain name <safecreditunion.org>. The complainant has the domain name <safecu.org> The complainant stated that the respondent domain name is identical to its trademark and name. The complainant also alleged that the respondent does not have a legitimate interest in the domain name. The complainant further stated that the respondent is using the domain name to promote competing and non-competing products and services. The respondent did not reply to the complainant contentions. The WIPO panel held the respondent domain name registration in bad faith and transferred it to the complainant.
Hitachi Ltd. v. Value Domain (2010)	This is a case of pseudo cybersquatting or blocking registration. The complainant is Hitachi Ltd. from Japan and respondent is Value Domain from Japan. The complainant holds the trademark "Hitachi" in over 175 countries. Hitachi Capital has been extensively involved in asset management. The respondent registered the domain name <hitachi-am.com> with eNom Inc. The complainant submitted to the WIPO panel that the registered domain is confusingly similar to its trademark "Hitachi". The complainant further stated that "-am" corresponds to asset management function of Hitachi Capital. The complainant also stated that the respondent has no legitimate interest in the domain name and has registered the domain name in bad faith. At the same time, complainant argued that the respondent has not been using the domain name and blocking the complainant from using it. The respondent did not reply to complainant contentions. The WIPO panel agreed with the complainant contentions and transferred the domain name in its favor.
Koninklijke Philips Electronics N.V. v. In Seo Kim (2001)	This is a case of cyber smearing. The complainant (Koninklijke Philips Electronics N.V.) has registered trademark "Philips" in various countries. The respondent (In Seo Kim) has registered 14 domain names ending in <sucks.com>. The complainant alleged that the domain name registered by the respondent <philipssucks.com> is confusingly similar to its registered trademark. The complainant also stated that the respondent has no legitimate

	interest in the domain name and is indulging in cyber smearing to disrupt its business. The WIPO panel agreed with the contentions of the complainant and transferred the domain name to it.
Goldline International, Inc. v. Gold Line (2001)	This is a case of reverse domain name hijacking. The complainant in this case was Goldline International, Inc. and respondent is Gold Line. The complainant claimed bad faith registration of its trademark against the respondent. However, the businesses were unrelated. The respondent submitted that the complainant has already been apprised of the facts related to the case before bringing the case to the WIPO panel. The WIPO panel held that the complainant actions in this case constitute bad faith. The panel considered this a case of reverse domain name hijacking and dismissed the case.
Donna Karan Studio v. Raymond Donn (2001)	This is a case of inadvertent failing to renew domain name. The complainant is this case is Donna Karan Studio from USA and respondent is Raymond Donn from UK. The complainant failed to renew the domain name <dknyjeans.com> inadvertently. Subsequently, the respondent registered the domain name in its favor. The WIPO panel held that the respondent has registered the domain name in bad faith and transferred it to the complainant.

CONCLUSIONS

Domain names have emerged as important business identifiers in today's internet driven marketplace. However, they are increasingly abused by miscreants. ICANN UPRP is playing its part in resolving the domain name disputes. The main findings of this research are:

- Cybersquatting, typo-squatting, cyber piracy, pseudo cybersquatting, cyber smearing, reverse domain name hijacking, and registration by another party upon inadvertent failing to renew domain name by legitimate party, are major type of domain name abuses.
- UDRP provides a fast and cheaper option than courts to resolve domain name disputes.
- UDRP cases can be resolved by parties upon mutual agreement.
- UDRP cases are decided by experts in trademark law, which may or may not happen in courts.
- UDRP can resolve domain name disputes only in case of gTLDs and new gTLDs. UDRP has limited applicability to ccTLDs.
- No monetary damages can be awarded by the UDRP panel against the miscreants.
- The party that lost case in UDRP can still file a case in a court of competent jurisdiction.

It can be said that the UDRP mechanism still has limitations to effectively protect the domain names. The losing party can still file a case in the court of competent jurisdiction and try to take advantage of differences in laws across countries. So, ICANN should formulate a model domain names dispute resolution law. The countries should amend their existing laws to bring it in line with the proposed ICANN model domain names dispute resolution law. Also, the mechanism of UDRP should be further strengthened. The losing party should be able to appeal to courts of competent jurisdiction only in exceptional cases, not all cases.

References

Ahmed, S. (2010). Cybersquatting: Pits and Stops. *Indian Law Institute Law Review*, 1(1), 79.

Bach N.M. (2001). *Understanding of Vietnamese Civil Law: The Intellectual Property Rights*. Dong Nai General Publishing House, 2001.

Caruana, C. (2015). The Legal Nature of Domain Names. Retrieved from www.elsa.org.mt/

Chissick, M. and Kelman, A. (2002). *Electronic Commerce: Law and Practice*. 3rd ed. London: Sweet & Maxwell, 24.

CMS (2007). Protection of Trade Marks: Online Use and Anticybersquatting, A European Perspective, A CMS IP Group Publication. Retrieved from http://docplayer.net/

Donna Karan Studio v. Raymond Donn (2001, June 27). Case No. D2001-0587. Retrieved from https://www.wipo.int/

Goldline International, Inc. v. Gold Line (2001, January 4). WIPO case D2000-1151. Retrieved from https://www.wipo.int/

Hitachi Ltd. v. Value Domain (2010). Case No. D2010-1433. Retrieved from https://www.wipo.int/

Holland B. (2005). Tempest in a Teapot or Tidal Wave? Cybersquatting Remedies Run Amok. *Journal of Technology Law and Policy*, 10, 307.

ICANN (1999, October 24). Uniform Domain Name Dispute Resolution Policy. Retrieved from https://www.icann.org/

ICANN (2009, May 21). Registrar Accreditation Agreement. Retrieved from https://www.icann.org/

ICANN (2010, February 15). Non-Lawyers' Guide to the May 2009 Registrar Accreditation Agreement*. Retrieved from https://www.icann.org/

ICANN (2011a). New Generic top Level Domains. Retrieved from https://newgtlds.icann.org/en/announcements-and-media/2011

ICANN (2011b, June 27). Registrant Rights and Responsibilities under the 2009 Registrar Accreditation Agreement. Retrieved from https://www.icann.org/

ICANN (2018). List of Approved Dispute Resolution Service Providers. Retrieved from https://www.icann.org/

ICANN WHOIS (2018). Glossary of WHOIS Terms. Retrieved from https://www.icann.org/

IDN (2018). Internationalized Domain Names. Retrieved from https://www.icann.org/resources/pages/idn-2012-02-25-en

INDRP (2005). INDRP Rules of Procedure. Retrieved from https://registry.in/

Katz, M., Rosston, G. and Sullivan, T. (2010, June). An Economic Framework for the Analysis of the Expansion of Generic Top-Level Domain Names. Retrieved from https://archive.icann.org/en/

Koninklijke Philips Electronics N.V. v. In Seo Kim (2001, November 12). Koninklijke Philips Electronics N.V. v. In Seo Kim, Case No. D2001-1195. Retrieved from https://www.wipo.int/

Koščík, M. (2008). "Suck Cases" in WIPO Domain Name Decisions. Masaryk University Journal of Law and Technology. Retrieved from https://journals.muni.cz/

Kruger, L.G. (2014). Internet Domain Names: Background and Policy Issues. Congressional Research Service Report. Retrieved from https://www.ipmall.info/

Levine, G.M. (2012). Inadvertent Lapse of Domain Name Registration. Retrieved from http://iplegalcorner.com/

Lipton J.D. (2005, August 6). Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy. *Wake Forest Law Review*, 40(4), 1–64.

Mercer, J.D. (2000). Cybersquatting: Blackmailing on the Information Superhighway. *Journal of Science and Technology Law*, 6. Boston University School of Law.

Michaelson, P. (2016, April 13). Emergency Arbitration: Fast, Effective and Economical. Just Resolutions, American Bar Association Dispute Resolution Section, March 2016. Retrieved from https://ssrn.com/abstract=2762715

Namestat (2018). Top 10 Biggest Selling gTLDs. Retrieved from https://namestat.org/

Ngoc, T.P. (2011). *Well-known Trademark Protection. A comparative Study between the Laws of the European Union and Vietnam*. Published Thesis, The Faculty of Law, Lund University.

OECD (2006, November 17). Evolution in the Management of Country Code Top-Level Domain Names (ccTLDs). DSTI/ICCP/TISP(2006)6/FINAL. Retrieved from https://www.oecd.org/

Philip Morris Incorporated v. r9.net (2007, November 30). Philip Morris USA, Inc. v. Andrey Kulikov, Case No. D2007-1450. Retrieved from https://www.wipo.int/

Roesler, P. (2015). Will New Top Level Domains Matter in 2015? Retrieved from https://www.inc.com/peter-roesler/will-new-top-level-domains-matter-in-2015.html

Rustad, M. (2013). *Global Internet Law*, West Academic, 746-747.

SAFE Credit Union v. Mike Morgan (2006, July 18). Case No. D2006-0588. Retrieved from https://www.wipo.int/

Shell Trademark Management B.V. v. Domains - Best Domain (2003). Shell International Petroleum Company Limited, Shell Trademark Management B.V. v. Domains - Best Domain, Case No. D2003-0066. Retrieved from https://www.wipo.int/

Szurdi J. and Christin N. (2017, November 1-3). Email Typo-squatting. Internet Measurement Conference, London, United Kingdom. Retrieved from https://doi.org/10.1145/3131365.3131399

Ventsislav, P. (2012). The Prevention of Cybersquatting in Europe: Diverging Approaches and Prospects for Harmonization. MIPLC Master Thesis Series (2012/13). Retrieved from https://ssrn.com/abstract=2427582

WIPO (1998, December 23). WIPO Internet Domain Name Process. The Management of Internet Names and Addresses: Intellectual Property Issues, Interim Report of the WIPO Internet Domain Name Process. Retrieved from http://www.wipo.int/

WIPO (2010). WIPO General Assembly - Thirty-Ninth (20th Extraordinary) Session Geneva. Retrieved from http://www.wipo.int/

WIPO (2017, June 8). Arbitration and Mediation Center ccTLD Database. Retrieved from http://www.wipo.int/

WIPO ccTLDs (2018). Domain Name Dispute Resolution Service for Country Code Top Level Domains (ccTLDs). Retrieved from https://www.wipo.int/

WIPO gTLDs (2018). Domain Name Dispute Resolution Service for Generic Top-Level Domains. Retrieved from https://www.wipo.int/