



ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

Copyright © 2024 - 25

A COMPARATIVE STUDY OF CYBER SQUATTING IN INDIA AND USA

AUTHOR'S NAME – Ashutosh Kumar Pandey, LL.M (Corporate Law).

INSTITUTION NAME – Amity Law School, Amity University Lucknow.

RESEARCH METHODOLOGY**Aim and Objective of the Project:**

Firstly, to study the concept of domain name system and the influence of trademarks on domain names. Secondly, to explain the criminal intent through Cyber Squatting. Thirdly, to study the role of UDRP in regulating cyber-squatting. Finally, to propose eradivative measures for resolving disputes relating to cyber-squatting.

Research Problem:

In light of the above introductory remarks, the problem that is to be encountered is that there is no legal mechanism to deal with the issue of Cyber Squatting in India as compared to the USA.

Research Question:

- What is the importance of trademarks to domain names?
- What are Cyber Squatting and Typo squatting and how are they dealt with in India and USA?
- Whether there is any mechanism to deal with the disputes relating to domain names?
- What necessary steps should the Government of India take to keep a check on Cyber Squatting?

Hypothesis:

The project report proceeds on the hypothesis that there are not adequate provisions regulating Cyber Squatting in India at present and the concept is taken much more seriously under the Laws of the United States.

Research Methodology:

In this paper, the researcher has primarily used descriptive and analytical methodology research which involves a case study also. The researcher has mainly relied upon primary sources as well as secondary sources. The researcher has gone through various books and articles relating to Cyber Squatting and also relied upon web sources.

ABBREVIATION

WWW	:	World Wide Web.
UDRP	:	Uniform Domain-Name Dispute-Resolution Policy.
IP	:	Internet Protocol.
DNS	:	Domain Name System.
TLD	:	Top Level Domains Name.
SLD	:	Second-Level Domain Name.
HTTP	:	Hyper Text Markup Language.
E-mail	:	Electronic Mail.
SMTP	:	Simple Mail Transfer Protocol.
ACPA	:	Anti-cybersquatting Consumer Protection Act.
ICANN'S	:	Internet Corporation for Assigned Names and Numbers.
IDN	:	Internationalized Domain Name.
URL	:	Uniform Resource Locator.
IANA	:	Internet Assigned Number Authority.
NSI	:	Network Solutions Incorporation.

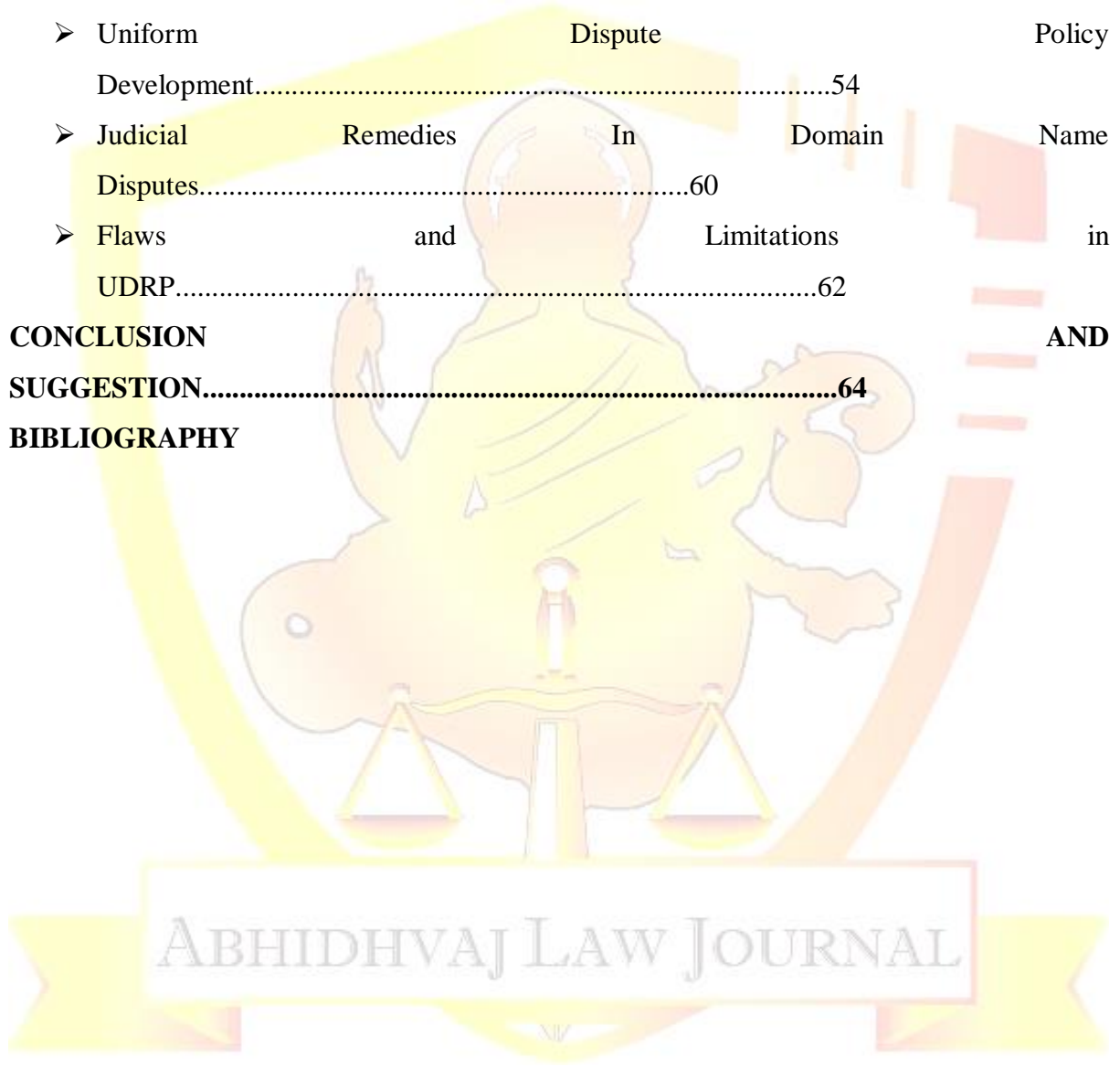


ABHIDHVAJ LAW JOURNAL

TABLE OF CONTENTS

CHAPTER 1:			
Introduction.....			9
CHAPTER 2:	Domain	Name	
System.....			11
➤ Domain Names.....			11
➤ Importance of Domain Names.....			12
➤ Creation of Domain Names.....			14
➤ Generic Domains.....		Top-Level	15
➤ Domain Names to be Trademark.....			20
➤ Importance of Domain Names to Trademark Owners.....			25
CHAPTER 3:	Concept	of	Cyber
Squatting.....			28
➤ History of Cyber Squatting.....			28
➤ Typosquatting.....			30
➤ Domain Name Registration System.....			31
➤ Cybersquatting in India.....			34
➤ Cybersquatting In USA.....			38
➤ Defenses of the Cybersquatter.....			49

CHAPTER 4: Uniform Dispute Resolution Policy Framework.....	51
➤ History of Domain Name Administration.....	51
➤ ICANN’S Dispute Policy Development.....	52
➤ Uniform Dispute Policy Development.....	54
➤ Judicial Remedies In Domain Name Disputes.....	60
➤ Flaws and Limitations in UDRP.....	62
CONCLUSION AND SUGGESTION.....	64
BIBLIOGRAPHY	



CHAPTER 1: INTRODUCTION

In the current age, the Internet has become an important part of the life of almost every individual in developed nations and is rapidly increasing in developing nations. For business entities, the internet has become a boon for communicating with the world.¹ A business entity's trademark contains immense importance. It helps an entity build up its identity over the WWW. The trademarks apply to the physical world, whereas the Internet is global in nature. The chances of face-to-face interaction in the internet world are very low and as a result, the consumers cannot inspect the goods before purchase hence the consumers have to rely only on trusted sources. In such a situation, the trademarks of the business entities play a vital role in assuring the consumers about the quality of the goods.²

Domain names are the establishment of the unmistakable structure on the Internet and are the premise on which E-trade has been developed.³ The web from a layman's perspective is very convoluted which is termed as "the internet" the most widely recognized route for buyers to discover what they are searching for is to sort in a space name containing the brand's name or organization they are searching for.⁴ If there are no domain names, a computer would have no idea where to look for a web page. Domain names are not just addresses, since they can be selected by the "addressee" and are closely associated with a particular service or product.⁵ In India, a domain name has at least two key parts: the second-level domain (such as .com or .gov) and the third-level domain.

Originally, Domain Names were intended to function as addresses, but today there are increasing numbers of cases of illegal registration of domain names called cyber-squatting, as a result, additional problems have occurred with regard to handling trademark disputes in cyberspace.⁶ Cyber-squatting occurs when a domain name is registered by a third party in bad faith⁷. Due to the increasing popularity of the internet business entities find it highly beneficial

¹ Shivani Mathur, Article-A Comparative Study Of Cybersquatting In India And USA, mondaq, (June. 7, 2024, 7:19 AM),<https://www.mondaq.com/india/trademark/867550/article-a-comparitive-study-of-cybersquatting-in-india-and-usa>

² *Id.*, at 1557

³ *Id.*, at 1557

⁴ *Id.*, at 1557

⁵ studocu, <https://www.studocu.com/en-us/document/the-pennsylvania-state-university/international-law/domain-name/56811851>, (last visited June. 6, 2024).

⁶ *Supra* note 01, at

⁷ Marc D. Wielansky, Internationalized Domain Names 2001,p306,

to register a domain name the same as the name of the company or product so that consumers can easily connect to them.⁸ The common association in the middle of trademarks and area names has been abused by some who have enrolled the trademarks of others as space names and afterward made high benefits by attempting to offer those space names back to the trademark proprietors or outsiders, known as digital hunching down. The most famous example is of the USA-based Yahoo Inc. where the court found that yahoo India was an intentional effort to trade on the fame of the yahoo trademark⁹. Registration of domain names is an inexpensive process and takes less than 24 hours. The registration of domain names is on the basis of first come first serve, making it easier for disputes to arise over entitlement to domain names¹⁰. The UDRP is an online arbitration-influenced administrative process available for the most serious types of trademark-related domain name disputes-those involving so-called cyber-squatting¹¹. As the number of domain name registrations is increasing the rate of trademark infringement is increasing day by day, but the biggest reason there are so many domain name infringement cases is a prevailing lack of knowledge among people. Most people, including the domain name registrant, are not aware of trademark laws, the legal significance and consequences of trademark infringement, and the determining factor if a domain name might infringe on a trademark.



ABHIDHVAJ LAW JOURNAL

⁸ *Supra* note 01, at 1558

⁹ *Yahoo Inc v. Akash Arora* 1999(2)AD(Delhi)229

¹⁰ Domain Names by Bromhead Johnson

Available at: http://www.intellectual-property.co.uk/pages/domain_names.

¹¹ Lilian Edwards and Charlotte Waelde (2009) *Law and the internet* (3rd ed) Hart publishing. p322

CHAPTER 2: THE DOMAIN NAME SYSTEM

1) WHAT ARE DOMAIN NAMES?

A domain name is a significant part of an Internet address. To humans, domain names seem like words, however, once a website name is employed on the web, it's translated into numbers¹². Domain name is defined as "the alphanumeric equivalent of an Internet Protocol ("IP") number"¹³.

The Internet is a powerful communication system. The operation of that system requires that every computer on the Internet have a unique identifier. Routing data on the Internet is accomplished via addresses consisting of Internet Protocol Addresses (IP Addresses), sometimes called Internet Protocol Numbers (IPN), each of which consists of four values ranging from 0 to 256 separated by periods (or dots), for example, "255.21.1.12." Very roughly, the IP Address of a computer on the Internet is the equivalent of the phone number of a telephone.

Like phone numbers, IP Addresses are relatively difficult to remember. The DNS allows an information provider to register a domain name corresponding to an IP Address. It is very difficult to remember the strings of numbers hence the DNS provides for an alphabetic system that is easy to remember. Instead of entering the number 233.72.2.11 the user can directly enter the domain name, for example, www.Jabong.com. The DNS itself transfers the alphabets into computer-readable numbers. It is like a telephone book that allows subscriber names to be translated into their unique telephone numbers. Most importantly, each address is unique in itself so other computers are able to locate and deliver messages to the correct address¹⁴. A domain name, such as "www.Jabong.com," consists of parts, which are separated by dots. These parts are organized into a hierarchy of level top-level domains. The end of the domain name or the string is the top level in the hierarchy. Thus, the domain name "www.Jabong.com" has as its top or first level ".com", and this is a top-level domain name (TLD). The second level of "www.Jabong.com" is ". Jabong"; this is called a second-level domain name (SLD). The

¹² Andre Fresh, "Internet Domain Name Protection: A Canadian Perspective" (1996). Last retrieved 5th October 2018.

¹³ Ramzi Madi, "The Conflict between Country Code Top Level Domains and Trademarks: A brief overview of the Jordanian nationals solution", Arab law quarterly (2006). <http://www.jstor.org/stable/27650565>, 5th October 2018.

¹⁴ Marshall Leaffer, "Domain names, Globalization, and Internet Governance", Indiana University press (1998). <http://www.jstor.org/stable/20644692>.

third level of “www.Jabong.com” is “www” and this is, of course, a third-level domain name. On the Internet, each computer has its own unique address. An Internet address identifies an individual’s computer and the communication on one basis takes place.

Different computers with the help of IP addresses can locate each other in large tangled web space, but due to the enormous size of the Internet and the innumerable computers being connected through it, it is very difficult for users to remember the IP Address of various computers¹⁵. Hence the DNS provides for mnemonic alphanumeric which is known as a domain name. The domain name system (DNS) is what allows average, everyday Internet users to “surf” through cyberspace using familiar strings of letters and numbers as their guide.

2) WHY ARE DOMAIN NAMES IMPORTANT?

Domain names are important and can be used for a variety of reasons. The most basic reason why domain names are important is because they simply allow applications that use the Internet to address servers (computers or other devices) on the Internet. Most end users are familiar with Hyper Text Transfer Protocol (HTTP), the application behind the World Wide Web. Internet browser programs, such as Internet Explorer, Mozilla Firefox, Google Chrome, or Opera, consist of an address bar that allows the user to enter a domain name in order to browse a particular website—lowering the time (and hence cost) of accessing websites. For example, if we enter www.flipkart.com the Flipkart home page opens. E-mail programs, such as Gmail or yahoo allow users to enter an e-mail address consisting of an email identifier, such as the “at” symbol, “@,” and a domain name, such as “microsoft.com.” SMTP uses the domain name in the e-mail address to route the data packets comprising the e-mail message to the appropriate computer on the Internet. Hence when we send an email the email address is shown as Shivani.mathur@student.amity.edu.

Domain names have made the life of people very easy and hence it is a less costly affair to navigate the Internet¹⁶. Apart from technical functions, domain names have gained another level of importance. The World Wide Web provides for economic significance. A linguistic convention has emerged whereby the domain name associated with the home page of a website becomes the name of the site itself. In the case of a dotcom—that is, a company that does

¹⁵ Natalma M. Mcknew, “Post Domain Infringement: in search of remedy”, American Bar Association vol19 (2010). <http://www.jstor.org/stable/23297558>.

¹⁶ Shuli Green, “Launching Trademark Law into Cyberspace”, American Bar Association vol 49(1997), <http://www.jstor.org/stable/40709886>.

business primarily on the Internet—the business itself may be named by the domain name or part of the domain name¹⁷. The name of the business Reebok.com, gives its consumers the impression that it is the original shoe company, and there lies the trust factor. It is identical to the domain name in the physical world. The first term in the name of the business eBay, Inc., is identical to the second-level domain name “.eBay”. Even when a company is not a dotcom, its website may acquire an identity of its own that is significant to the public image of the company.

So, the website “Apple.com” is an important public face of the enterprise, “Apple, Inc.” Apple products have gained popularity and today two out of four people have an Apple iPhone or iPod. Hence, the Trademark consists of a great economic value which is associated directly with its goodwill and it determines its reputation in the market the quality of the product and, its reliability, all depend on the reputation of the product and company¹⁸.

A large part of the market value of Apple.com, Inc. is constituted by the good will associated with its domain name. Thus, domain names have value, both as shortcuts for IP Addresses and as trade names. The value of such addresses gave rise to the practice of cybersquatting or registering a domain name that includes the trademark of an existing commercial enterprise and then attempting to sell that domain name to the enterprise. This practice of cyber-squatting, made the USA take a huge step in the adoption of a federal statute, the Ant cybersquatting Consumer Protection Act (ACPA), and a system of private arbitrations policies, including ICANN’s Uniform Dispute Resolution Policy (UDRP)¹⁹.

The economic value of domain names has also created a market for domain names that are easy to remember or that are obvious names for particular dotcom businesses. “Car.c0m” and “auto.com” square measure are obvious main names of an internet site that sells a product or service related to vehicles. If the current registrant of the domain name does not have a profitable business associated with the name, the registrant might choose to sell it instead. Until recently, someone who wished to register a domain name like “car” as a second-level domain could only do so in one of three unrestricted gTLDs, “.com,” “.net,” or “.org.”

¹⁷ Supra note 6, at 1561

¹⁸ Supra note 2, 1561

¹⁹ Lemley, Mark & Volokh, Eugene, “Freedom of Speech and Injunctions in Intellectual Property Cases” Duke Law Journal vol 48(1998).

3) HOW ARE DOMAIN NAMES CREATED?

A domain name comes into being when it is registered. In order to explain how this happens, four key terms have been defined:

- Registrant: A person who has a right to use a specific domain name.
- Registrar: An entity that sells domain name registration services to registrants. Registrars are middlepersons or retailers²⁰.
- Registry: An entity that provides domain name service for a TLD. Registries are the service producers; they deal with the customers through registrars.
- Domain Name Authority: An entity that provides root service.

When a user types in a domain name, a "domain Name server" translates it into the corresponding IP Numeric and then sends the numeric to the "root server" that holds the identifying information for domain names in the root server's top-level domain ("TLD")²¹.

Domain names are helpful in forming a noble identity. Business entities should opt for domain names that correspond to their names so that it becomes easy for the public to associate. There are multiple reasons for the development of a DNS that supports international domain names (IDNs) First of all, it allows the Internet to be the truly global phenomenon that so many people describe it to be²².

Up to this point, we have not described the actual operation of the Domain Name System (DNS). It is very important to note how does the address bar converts the domain name into an IP address That is, when I enter a domain name in the address bar of my browser, how does that name translate into a particular Internet Protocol Address?

The DNS is one of the most crucial elements of the Internet. It provides an efficient method of matching IP addresses to domain names in a manner that is transparent to most users. It is based on a relatively simple concept. Each domain has a responsibility to provide its own DNS servers for each of its sites²³. Therefore, when a user wishes to access a site, his or her Web browser queries a directory based on the top-level do- main name (such as .com or .net). This

²⁰Internet Corporation for Assigned Names and Numbers (ICANN): Rules for Uniform Domain Name Dispute Resolution Policy, American Society of International Law. <http://www.jstor.org/stable/20694028>.

²¹ Alexander Gigante, "Black hole in Cyberspace: The Legal Void in the Internet", 15 J. Marshall J. Computer & Info. L. 413 (1997). P. 415.

²² Supra note 2, at 1562

²³ Supra note 10, at 1562

directory lists the DNS for an IP address that matches the URL the user requested on that particular domain²⁴

4) GENERIC TOP-LEVEL DOMAINS

The TLDs are grouped into three categories: (1) generic, (2) country code, and (3) infrastructure. Although our primary focus is on gTLD policy, Let us discuss Country Code and Infrastructure TLDs first. Domain names, by their very nature, must be unique. For domain names to be unique there should be some organization to ensure that no duplication occurs. Until 1998 the body with this responsibility was the Internet Assigned Numbers Authority ("IANA"). The other relevant organization was a company called Network Solutions, Inc. ("NSI"), which held a contract with the US government to accept registrations for .com, .net, and .org domain names.²⁵ Until 1999 NSI was the sole registrar of such gTLDs domain names. In 1998 the US Government called for the establishment of a not-for-profit organization, with representation from a wide range of interests (both US and international), for the purpose of administering the domain name system generally. That organization is the Internet Corporation for Assigned Names and Numbers ("ICANN")²⁶.

The country code top-level domains are culturally and economically the competitors of the gTLDs. Each ccTLD consists of two letters (.uk, .nz, .fr, etc.). The two-letter codes are called "country codes" because they correspond to the two-letter abbreviations for countries such as .dk for Denmark, .in for India, .ae UAE, and .gl for Greenland that are included on the International Standards Organization's list of standardized abbreviations. The ccTLD for the United States is .us and, compared to the gTLDs such as .com, .us lacks substantial cultural and economic significance²⁷.

In many other nations, the national ccTLD demarcates the name space that is most significant to that nation's users of the Internet. In the United Kingdom, for example, the .uk name space dominates e-commerce. The UK version of Amazon.com is www.amazon.co.uk. In the United Kingdom, as an example, second-level domains operate in a fashion similar to the gTLDs. This is not to say that the gTLDs lack significance outside of the United States. For example, many

²⁴ Supra note 2, at 1563

²⁵ cnet, <https://www.cnet.com/tech/tech-industry/nsi-accused-by-rivals-of-hoarding-domain-names/>, (last visited June. 6, 2024).

²⁶ Patrick Gunning, "Trademarks and domain names", Cyberspace Law Resources (2000).

²⁷ *Id.*, at 1563

international firms use their .com address as the worldwide gateway to their various national sites.²⁸ So, for example, one can browse from www.nikon.com to www.nikon.fr or from www.sony.com to www.sony.co.jp.

The Generic TLDs:

Given below is a list of gTLDs that exist. For each gTLD, we indicate whether registration is restricted (to some groups) or unrestricted (open to all who pay a fee) and the associated operator or sponsor.

1. .Aero—restricted to members of the air-transport industry and sponsored by Society International de Telecommunications Aéronautique S.C. (SITA SC)²⁹.
2. .biz—restricted to businesses and operated by NeuLevel, Inc.³⁰.
3. .com—unrestricted and operated by Verisign, Inc.³¹.
4. .coop—restricted to cooperative associations and sponsored by Dot Cooperation LLC³².
5. .edu—restricted to degree-granting educational institutions of higher education that are accredited by one of the six U.S. regional accrediting agencies and operated by Educause³³.
6. .gov—restricted to use by the Government of the United States of America and operated by the US General Services Administration³⁴.
7. .info—unrestricted and operated by Afilias, Inc.³⁵.
8. .int—restricted to organizations established by international treaties between governments and operated by ICANN³⁶.
9. .mil—restricted to use by the armed forces of the United States of America and operated by the Department of Defense Information Center³⁷.
10. .museum—restricted to use by museums and sponsored by the Museum Domain Management Association³⁸.

²⁸ coursehero, <https://www.coursehero.com/file/p2nd7gv2m/Addressing-The-World-National-Identity-and-Internet-Country-Code-Domains-Rowman/>, (last visited June. 6, 2024).

²⁹ Internet Assigned Numbers Authority, Root-Zone Whois Information .aero—Top-Level Domain <http://www.iana.org/root-whois/aero.htm> .

³⁰ *Id.*, at 1564

³¹ *Id.*, at 1564

³² *Id.*, at 1564

³³ *Id.*, at 1564

³⁴ *Id.*, at 1564

³⁵ *Id.*, at 1564

³⁶ *Id.*, at 1564

³⁷ *Id.*, at 1564

³⁸ *Id.*, at 1564

11. .name—restricted to use by individuals and operated by Global Name Registry, Ltd³⁹.
12. .net—unrestricted and operated by Verisign, Inc.⁴⁰.
13. .org—unrestricted and operated by the Public Internet Registry⁴¹.
14. .pro—restricted to accredited professionals and operated by RegistryPro⁴².

The fourteen gTLDs can be categorized in a variety of ways. There is a history that distinguishes the gTLDs according to their period. The .com, .edu, .gov, .int, .mil, .net, and .org belong to the first wave of gTLDs. Three of these (.edu, .gov, and .mil) reflect the original tilt of the Internet toward the United States, where the Internet originated.⁴³ The .edu TLD is limited to accredited U.S. educational institutions, and .gov and .mil are reserved for the use of the government and armed forces of the U.S. The .int TLD is used only by International Organizations (IOs) established by treaty. For the purposes of our analysis, we will set these four TLDs aside. The remaining three members of the first wave of gTLDs are .com, .net and .org. These domains are currently unrestricted. Anyone can register any combination of Roman letters and Arabic numerals in these domains—although there are legal restrictions on the registration of domain names that are identical or substantially similar to trademarks. For these unrestricted gTLDs, the domain name space was allocated by a rule of first occupation. The first person to register the second-level domain name car.com was contractually granted the right to renew that registration. At some point, many persons began to realize that domain names could have significant economic value, and there was a “land rush” for the easy-to-remember domain names that could be used for e-commerce, advertising, or other economic activity.

5) WHETHER A DOMAIN NAME CAN BY ITSELF BE A TRADEMARK?

Domain names do not fit conveniently into the bifurcated world of copyright and industrial property (i.e., patent and trademark law), domain names are a hybrid form of intellectual property. On the one hand, they serve a useful purpose by designating where information is to be sent. On the opposite side, they often indicate origin, and the public views them as

³⁹ *Id.*, at 1565

⁴⁰ *Id.*, at 1565

⁴¹ *Id.*, at 1565

⁴² *Id.*, at 1565

⁴³ Coursehero, *Supra* note 28, at 1565

trademarks⁴⁴. The domain names in order to function properly must be unique. Confusion is likely to occur if more than one business entity has the same domain name on the internet as the other. This sets up an inherent and unreconcilable conflict with trademark law, which tolerates the use of identical marks by different persons so long as those uses do not cause confusion in the marketplace⁴⁵.

Domain names are frequently involved in disputes, such as Misleading Domain names and Cybersquatting, which is defined as "the practice of registering a trademark as a domain name with the intent of taking advantage of it by marketing it, usually to the trademark owner"⁴⁶. A domain name can be made up of any words. Usually, an entity or business organization would make its own business name or the trademark as its domain name for the convenience of the customers. Many people cannot recall the domain name of an entity or organization and hence are likely to think that the domain name would consist of an entity's trademark or trade name which would make it easier for them to locate that website. The principal goals of trade mark protection do not ultimately imply or necessitate that trademarks should be classified as a standard form of property, or that trade mark proprietors should enjoy the rights that the owners of real property do.

The prime reason for protecting patents and copyrights is to provide protection for inventors and artists in order to foster and promote creativity, which are as relevant today as when they were first conceived, these rights should remain restricted⁴⁷. Conflict among concurrent users begins with the fact that only one person can own a particular domain name⁴⁸. The existing conflict over domain names shows how the Internet has raised thorny perhaps contradicting problems for intellectual property. The intellectual property has not only played havoc with the law of copyright but also has engendered a number of confounding issues in the law of

⁴⁴Supra note 8, 1566

⁴⁵Supra note 8, 1566

⁴⁶ Monica Kilian, "Cybersquatting and trademark infringement", Murdoch University Electronic Journal Of law (2000).

⁴⁷Eddie Hurter, "The international domain name classification debate: are domain names 'virtual property', intellectual property, property, or not property at all?" Vol 42(2009), Institute of foreign and comparative law. P. 296. <http://www.jstor.org/stable/23253104>.

⁴⁸Christopher J Schulte, "the new anticybersquatting law and uniform dispute resolution policy for domain names", American Bar Association (2000). <http://www.jstor.org/stable/25763488>.

trademark⁴⁹⁵⁰. Some of the problems are often merely characterized as normal incidents of trademark enraptured to cyberspace; others, like the domain name issue, result from digital age particularity⁵¹.

Domain names play a very important role apart from being merely an address. It helps the consumers in associating with the entity that makes the website their domain name. Thus once a website is launched by an entity, the domain name becomes its trademark. Trade mark protection should operate in the context of a regulatory environment where the justifications for the protection of trademarks are balanced against the broader social, economic, constitutional, and practical considerations in a global society. A domain name is entitled to protection under trademark law if it can be shown that such a domain name has altogether gained a secondary meaning through which the public is able to associate the source of the entity.⁵² The Delhi High Court in the case of *Aqua Minerals Ltd v. Pramod Borse and Another*⁵³, has held that a domain name has the same protection as any trade name that has been provided under the Trade and Merchandise Marks Act 1958.

In *Cardservice International Inc. v. McGee*⁵⁴, it was held that the domain name serves a function as the trademark and is not a mere address or like finding number on the Internet and, therefore, it is entitled to equal protection as a trademark. It was further held that a domain name is more than a mere Internet address for it also identifies the Internet site to those who reach it, much like a person's name identifies a selected person or a lot of relevant to trademark disputes, a company's name identifies a specific company.⁵⁵ The most debatable issue that arises is whether a domain name can be a trademark by itself. This issue can be discussed with reference to The Trademarks Act 1999. The Trade Marks Act, of 1999, defines a Trade Mark as, " 'trade mark' means a mark capable of being represented graphically and which is capable

⁴⁹Supra note 8, at 1567

⁵⁰ Leaffer, Marshall. "Domain Names, Globalization, and Internet Governance." *Indiana Journal of Global Legal Studies* 6, no. 1 (1998): 139–65. <http://www.jstor.org/stable/20644692>.

⁵¹Sally M. Abel, "Trademark issues in Cyberspace: The Brave New Frontier" (1999). <http://www.mttr.org/volfive/abel.html>.

⁵² Supra note 19, at 1567

⁵³ AIR 2001 Delhi 463, 93 (2001) DLT 203.

⁵⁴ 950 F. Supp. 737 (E.D. Va. 1997)

⁵⁵ Yahoo!, Inc. Vs. Akash Arora & Anr.

of distinguishing the goods or services of 1 person from those of others and should include an embodying form of products, their packaging, and combination of colors; and,

i. in relation to Chapter XII (other than section 107), a registered trade mark or a mark used in relation to goods or services for the purpose of indicating or so to indicate a connection in the course of trade between the products or services, as the case may be, and some person having the right as proprietor to use the mark; and,

ii. in relation to different provisions of this Act, a mark used or proposed to be used in relation to goods or services for the purpose of indicating or to indicate a connection in the course of trade between the products or services, as the case may be, and some person having the right, either as proprietor or by way of permissible user, to use the mark whether or not with none indication of the identity of that person, and includes a certification trade mark or collective mark.⁵⁶ A 'mark' in turn is defined as, "a 'mark' includes a device, brand, heading, label, ticket, name, signature, word, letter, numeral, shape of goods, packaging or combination of colors or any combination thereof⁵⁷.

The definition of 'mark' under the Act is wide enough to include domain names within its ambit. The definition of trademark includes the use of a mark in connection with goods or services that should be capable of being represented graphically. The definition of service under the Act is wide enough to include a website that is involved in e-commerce or a website that provides any other web-based service⁵⁸. When a person uses a domain name, he has to put it into the browser which is a graphical representation. Thus a domain name can be said to be a mark being used in connection with goods or services and which is capable of being represented graphically. Thus it might appear that a domain name qualifies to be a trademark within the meaning of the Trade Marks Act, 1999. A domain name is a word with the suffix '.com', or any other top-level domain. Thus the domain name can be considered to be a representation of a trademark, but a domain name does not qualify as a trademark because it contains the top-level domain names which are common to a large number of domain names and hence they cannot be protected. If we remove the top-level domain situated at the end of

⁵⁶ FCS Deepak P. Singh, Assignment and Transmission of Trade Marks, Taxguru.in, (June. 7, 2024, 7:19 AM), https://taxguru.in/corporate-law/assignment-transmission-trade-marks.html#google_vignette

⁵⁷ Section 2(m)

⁵⁸ Fisher William, "Property and Contract on the Internet", Chicago Kent Law Review vol 73 (1998), <http://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/11>.

the string, we are left with only a simple word. Therefore a domain name as a whole cannot be said to be a trademark.

However, in the US and the UK, the scenario is different as domain names can be permitted to be registered as trademarks. The US Patent and Trademark Office has issued guidelines for registering domain names as trademarks.

6) IMPORTANCE OF DOMAIN NAMES TO TRADEMARK OWNERS

Initially, Domain names were created only to serve the technical function, that is, to provide addresses that are easier to remember than the numeric IP address. However, with the massive increase in commercial activity on the Internet, domain names play the most important function of providing a platform for the customers to communicate with the business entities as well as it makes easy for the consumers to identify the business through its trademark which serves as a badge of origin. Indeed, many second-level domain names are identical to registered trademarks⁵⁹.

Trademark law ensures that the consumer is not misled about the source of a product. The trademark acts as a kind of quality assurance for the consumer. The benefits of a trademark are not enjoyed only by the consumers but equally extend to the trademark owner. For a successful business, a trademark plays a significant role as the goodwill of the entity is a mark of trust and recognition. Trademarks are therefore valuable business assets that their owners are keen to protect. However, as soon as the Internet is becoming more of a commercial tool, companies are being attacked by cyber squatters, who register trademarks as domain names, and this restricts the original trademark owners from establishing web sites using their own mark. Cyber-squatting is not a new concept; it is only as old as the World Wide Web itself⁶⁰. Thus the emerging area of cyber law has concentrated primarily on trademark issues⁶¹. A domain name is simply the address of an individual computer connected to the Internet. From a consumer's view point, a domain name is an IP address in a human-friendly form. A domain name becomes a valuable asset once it coincides with the trademark of a business. There is no

⁵⁹Supra note 15, at 1569

⁶⁰ John D.Mercer, "Cybersquatting: blackmail on the information superhighway".

⁶¹Supra note 46, at 1569

magic of association let alone trademark with an IP address called 191.166.6.12.⁶² But as soon as the IP address turns into something like "reebok.com" a totally new page is displayed, that of goodwill of the business and consumer recognition is associated with a trade or service mark. As soon as it is associated with a trademark, a domain name becomes a powerful commercial tool⁶³.

While the APCA and the UDRP are designed to address the problem of cybersquatting, concern has developed that overly aggressive trademark owners may use the new rules in garden-variety trademark/domain name disputes, because neither confusion nor fame is necessary to prove cybersquatting, a whole new area of litigation may erupt because of trademark holders trying to create an aura of "bad faith" around a domain name registration⁶⁴.

In the Canadian case of *Browne & Co. Ltd. v. Bluebird Industries.Xb*, The domain name at issue was "browneco.ca". Tucows.com Co. registered this as a domain name on December 14, 2000, even though, Browne & Co. Ltd. has been exploiting "the name Browne & Co. Ltd. since at least as early as 1991". Therefore, the panel ordered the registrant, Bluebird Industries Inc., to "transfer the domain name Browneco.ca to the Complainant Browne & Co. Ltd.". Domain Names have become an important tool since internet users can communicate with any business entity or acquire any information related to the product without recourse to any centralized, complete directory⁶⁵. This makes short, easy-to-remember names of paramount value in choosing an address. Moreover, domain names are valuable corporate assets, as they facilitate communication with a customer base.

In *Rediff Communication Ltd v. Cyberbooth and Another*⁶⁶, once a company has registered a domain name, it amounts to reserving a significant part of cyberspace for that company. Domain names are now highly visible in "real space" as well – showing up on television commercials, billboards, magazine ads, and even the sides of buses. In these new guises, they

⁶² Monica Kilian PhD, *Cybersquatting and Trademark Infringement*, 7, Murdoch University Electronic Journal of Law, 01-05, 2000, <https://www5.austlii.edu.au/au/journals/MurUEJL/2000/26.html>

⁶³ Supra note 7, at 1570

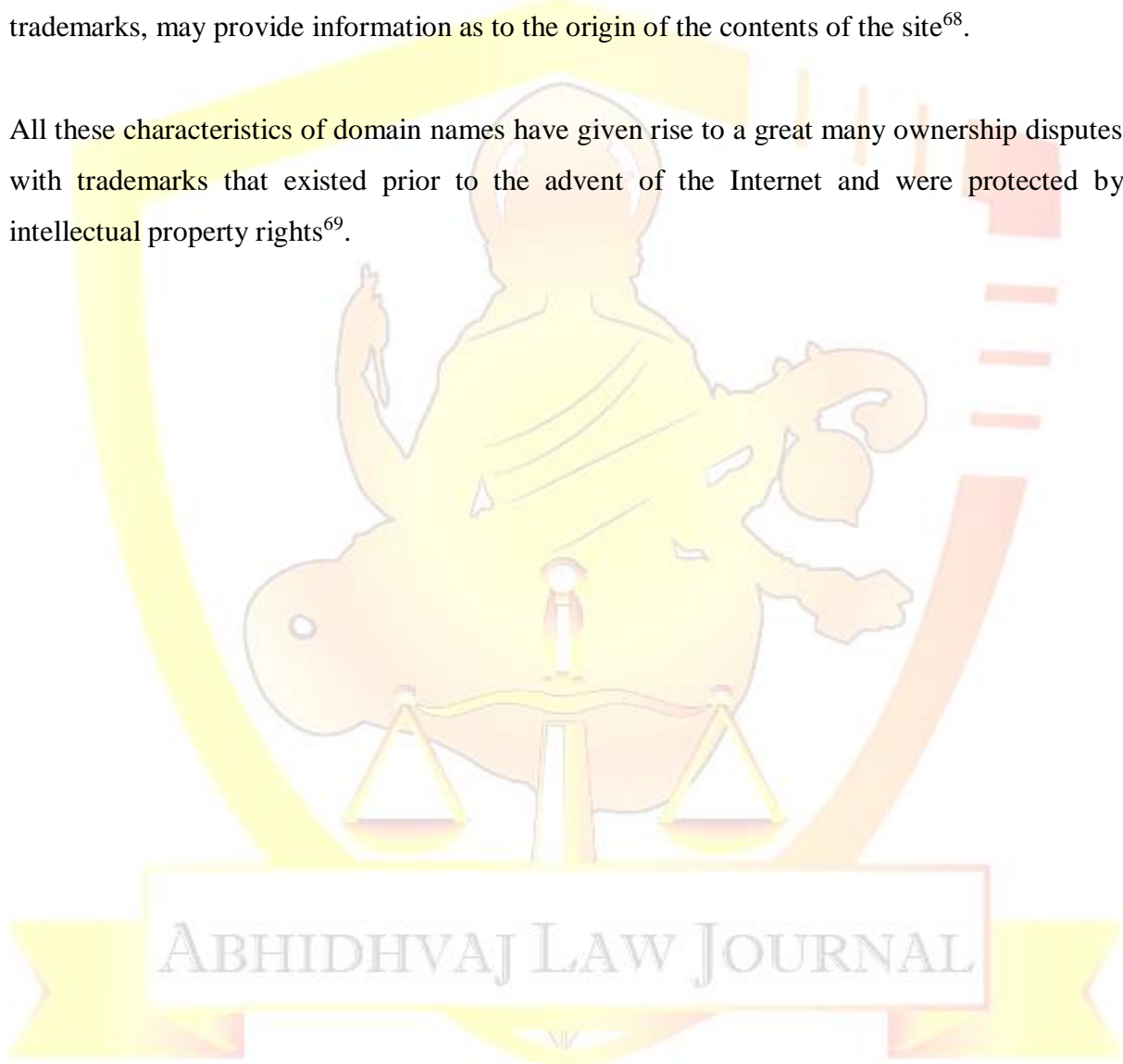
⁶⁴ Supra note 46, at 1570

⁶⁵ Burr, J. Beckwith, "Competition Policy and Intellectual Property in the Information Age", *Villanova Law Review* vol 41 (1996). <http://digitalcommons.law.villanova.edu/vlr/vol41/iss1/4>. Last retrieved: 1st February 2014.

⁶⁶ 1999 (3) All MR 164.

sometimes conflict with trademarks and other traditional business identifiers.⁶⁷ Two factors exacerbate this conflict. First, domain names are global and must be unique - a particular string of letters can link to only one site - while trademarks may overlap in different industries or different geographical locations. Second, it is common practice for many Internet users to guess at domain names. In addition to acting as an address, a domain name may also indicate to users some information as to the content of the site, and, in instances of well-known trade names or trademarks, may provide information as to the origin of the contents of the site⁶⁸.

All these characteristics of domain names have given rise to a great many ownership disputes with trademarks that existed prior to the advent of the Internet and were protected by intellectual property rights⁶⁹.



⁶⁷ cyber.harvard.edu, <https://cyber.harvard.edu/property00/domain/main.html>, (last visited June. 6, 2024).

⁶⁸ Christopher P.Rains, "A domain name by any other name: forging international solutions for the governance of internet domain names", *Emory International law review* (2000).

⁶⁹ *Supra* note 46, at 1571

CHAPTER 3: CONCEPT OF CYBERSQUATTING

1. HISTORY OF CYBER-SQUATTING

There is no single accepted definition of cyber-squatting. Generally, however, if anyone who lacks a legitimate claim registers a domain name with the intent to sell the name, stop the trademark holder from gaining access to the name, or divert traffic, this activity is thought to be known as cyber-squatting⁷⁰. As stated above, the registration system for domain names operates on a first-come, first-serve basis. Thus, a person with a bad intention can easily register a domain name of a well-known trademark that has goodwill in the market⁷¹. The Companies discover the fact that they cannot register the domain name of their respective trademark as it is already in use on the internet. Harmed by such an act, trademark owners have sought relief under trademark law to remedy the problem⁷².

Before 1999, the internet had not gained so much popularity and so the business world did not find it necessary to use it as a tool for success. They didn't feel the need to register their trademarks as domain names. However, from the point of view of cyber squatters, they did understand that the businesses were unaware of this mischief and took undue advantage. This is how cyber-squatting was born and began causing problems^{73,74}. Cyber squatters took advantage of those companies by registering domain names identical or similar to the business' trademarks. The most important drawback of Domain name registration was that, they accepted all applications for domain names by applicants until and unless there existed a similar domain name. Once the cyber squatter has the domain name registered, the business organization can no longer have its trademark as its domain name. This causes a problem since nowadays customers and clients try to find businesses online⁷⁵.

Reasons vary from person to person as to why they want to register a particular domain name. Most people select a domain name for entirely neutral or innocent reasons (i.e., an individual

⁷⁰ Cyber, *Supra* note 68, at 1572

⁷¹ *Supra* note 10, at 1572

⁷² *Supra* note 8, at 1572

⁷³ Melissa Kossler, "Cybersquatting" (2005). <http://faculty.ist.psu.edu/bagby/Fall05/346F05T8/history.htm>.

⁷⁴ Sangeetha Lakshmi V, THE MENACE OF CYBERSQUATTING AND THE AVAILABLE LEGAL MEASURES TO MITIGATE ABUSE OF DOMAIN NAMES, II, Indian Journal of Integrated Research in Law IJIRL, 01 -05, <https://ijirl.com/wp-content/uploads/2022/01/THE-MENACE-OF-CYBERSQUATTING-AND-THE-AVAILABLE-LEGAL-MEASURES-TO-MITIGATE-ABUSE-OF-DOMAIN-NAMES.pdf>

⁷⁵ *Id.* at 1572.

named "McDonald" may have always done business beneath his name). The process of domain name registration, however, has proven to be productive ground for those who have registered a domain name with bad intentions. Such registrants are known as cyber squatters who have registered the name of well-known companies as an Internet address and then tried to sell them back to the rightful owner. The process of allocating domain names inherently breeds conflicts of a trademark nature, no matter of the explanation why a certain party designated a domain name. Thus, any successful domain name regulation should serve 2 basic functions. First, it should offer a stable registration system that allocates distinctive domain names, avoiding conflict from a technical point of view. Second, it should have the power to resolve disputes between conflicting claims to a domain name beneath trademark principles⁷⁶. As domain names become ever more important to global commerce, it is hardly surprising that the use of trademark law has increased to resolve disputes over domain names⁷⁷. Unfortunately for trademark house owners, traditional trademark law provided little relief in claims against third parties who appropriated their trademark as a domain name. Trademark law is predicted on the probability of confusion⁷⁸. In earlier times, individuals discovered that entities did not register their domain names. Such individuals plunged into the cyber space by registering domain names that were similar to existing entities and later on sold them to the companies at a higher fee. Typical was cyber squatter Dennis Toeppen who cyber pirated such famous trademarks as "deltaairlines.com," "crateandbarrel.com," and "panavision.com"⁷⁹.

2. TYPOSQUATTING

A closely related aspect to cyber-squatting is typo squatting - where the domain name registrant registers a variant of a famous trademark. Typosquatting, which is also known as URL hijacking, is a form of cyber-squatting, and possibly brand jacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. The misprint squatter's URL can typically be one amongst four types, all similar to the victim site address⁸⁰:

⁷⁶ Supra note 46, at 1573.

⁷⁷ Aoki, Keith, "Intellectual Property and Sovereignty: Notes toward a Cultural Geography of Authorship", Stanford Law review vol 48(1996). <http://www.jstor.org/stable/1229388> .

⁷⁸ Supra note 46, at 1573.

⁷⁹ Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).

⁸⁰ Kelly M. Slavitt, "Protecting Your Intellectual Property from Domain Name Typosquatters" (2004). / help.owasp-juice.shop, <https://help.owasp-juice.shop/part2/vulnerable-components.html> (last visited June. 6, 2024).

- A common misspelling, or foreign language spelling, of the intended site: exemple.com
- A misspelling based on typing errors: xample.com or examlpe.com
- A differently phrased domain name: examples.com
- A different top-level domain: example.org

Typo squatters are individuals who hope to gain from typing mistakes, that is, they register mis-spellings of popular domains in the hope that they will be able to make money out of traffic from unintentional typing mistakes made by internet surfers. The website is designed in such a manner it tricks the users as a result they feel they are on the real site. A famous example of Typo squatting is Google.com, an extremely dangerous website that infects the user with spyware. Another similar thing is yuobe.com, which is similar to google.com except it targets YouTube users. Similarly, www.airfrance.com has been typo squatted by www.arifrance.com, diverting users to a website peddling discount travel.⁸¹

3. DOMAIN NAME REGISTRATION SYSTEM

Cyber-squatting includes three kinds of domain name registrations:

- A. Registration with the intention of selling the domain name.
- B. Registration with the intention of preventing the trademark holder from gaining access to the name.
- C. Registration with the intention of diverting traffic.

A) Registration with the intention of selling the domain name:

Registrants falling under this category attempt to profit from the Internet by reserving and later reselling or licensing domain names back to the companies that spent millions of dollars developing the goodwill of the trademark⁸².

⁸¹ towardsdatascience.com, <https://towardsdatascience.com/phishing-domain-detection-with-ml-5be9c99293e5> (last visited June. 6, 2024).

⁸² Intermatic Incorporated v. Dennis Toeppen, 947 F. Supp. 1227; 1996 U.S. Dist. LEXIS 14878.

When this happens, the company can either choose a different name or fight to get the domain name it really wants. These fights are called domain name disputes. Cyber-squatting is not considered illegal in spite of the fact that it creates problems and confusion among trademark owners and consumers. In other words, there are no laws in any jurisdiction, national or otherwise, that explicitly prohibit the practice⁸³. The courts in many countries have dealt with the cases of cybersquatting and have also given the judgment in favor of the trademark owners but it is also observed by the courts that the existing trademark law is not sufficient to deal with such cases.

B) Registration with the intent of restraining the trademark holder from gaining access to the domain name of his choice:

Although the trademark law has been extended to cases wherein the intention of the cyber-squatter was to resell the domain name to the trademark owner, it may not be possible to extend the said law to the cases wherein the only intention of the cyber-squatter is to hoard the domain name and restrain the original company from registering a domain name that would be most useful to it. The problem might be aggravated further by the fact that the registrant has not posted any website under that domain name. In such cases, the options that the aggrieved trademark owner has are to either serve his purpose by registering a different domain name to monitor the Internet for any potential infringing activity of the cyber-squatter or to wait for the expiry of the domain name and get it registered in his name before the cyber-squatter renews it.

C) Registration with the intention of diverting traffic:

This third category states that the intention of the cyber-squatter is to benefit from the reputation of the trademark owner, by diverting the users intending to access the trademark owner's website to the cyber-squatter website⁸⁴. This can be done in two ways, either he passes off his goods as those of the original trademark owner or he can do so by displaying defamatory material on the website to lower down the reputation and goodwill of the owner.

Most of the cases falling in this category satisfy all the requirements of the tort of passing off as well as trademark infringement, and consequently, the aggrieved trademark owner can seek

⁸³ Lessig, Lawrence, "Intellectual Property and Code", Basic Books. ISBN 0-465-03912-X.

⁸⁴ Supra note 6, at 1575.

remedies without much difficulty⁸⁵. In trademark infringement cases involving domain names, a possible question that could arise is whether the use of a trademark in the domain name of a website through which the goods and services are dealt with constitutes use in relation to goods and services. Section 101(e) says, ‘A person shall be deemed to apply a trademark or mark or trade description to goods or services who, in relation to the goods or services uses a trademark or trade description in any sign, advertisement, invoice, catalog, business letter, business paper, price list or other commercial document and goods are delivered or services are rendered to a person in pursuance of a request or order made by reference to the trademark or trade description as so used.’

Cases involving the use of domain names to pass off goods or services have been dealt with by the Indian Courts and they have been decided in favor of the trademark owners.

In *Yahoo, Inc. v. Akash Arora*⁸⁶, the learned single Judge of the Delhi High Court rejected the argument of the defendants that Internet users are sophisticated users and only literate people who are able to ascertain and approach the actual Internet site that they intend to visit. The learned Judge observed that if an individual is a sophisticated user of the Internet he may be an unsophisticated consumer of information and such a person may find his/her way to a different Internet site that provides an almost similar type of information as that of the plaintiff and thereby confusion could be created in the mind of the said person who intends to visit the Internet site of the plaintiff, but in fact reaches the Internet site of the defendant. In *Rediff Communication Ltd v. Cyberbooth and Another*⁸⁷, the Bombay High Court held, “with the advancement and progress in the technology, the services rendered in the Internet site have also come to be recognized and accepted and are being given protection so as to protect such provider of service from passing off the services rendered by others as his services.

4. CYBERSQUATTING IN INDIA

⁸⁵ Volokh, Eugene, “Sovereign Immunity and Intellectual Property”, Southern California Law review vol 73 (2000). <http://dx.doi.org/10.2139/ssrn.220130>.,

SandhyaGaur, Counterfeiting and Infringement of Trademarks in India, [legalserviceindia](https://www.legalserviceindia.com/legal/article-3076-counterfeiting-and-infringement-of-trademarks-in-india.html), (June. 7, 2024, 7:19 AM), <https://www.legalserviceindia.com/legal/article-3076-counterfeiting-and-infringement-of-trademarks-in-india.html>

⁸⁶ 1999 PTC (19) 201

⁸⁷ 1999 (3) All MR 164

Section 29 of the Trade Marks Act 1999 lays down the various cases in which a person will be said to have infringed another person's trademark. The ingredient that is common to all the cases is the use of the trademark in the course of trade and in relation to goods or services. The definition of Cybersquatting can be best summarised in *Manish Vij v. Indra Chugh*⁸⁸, the court held that "an act of obtaining fraudulent registration with an intent to sell the domain name to the lawful owner of the name at a premium".

The law relating to passing off is fairly well settled. The ingredients of passing off are that there is misrepresentation of goods or services by the defendant, this is done during the course of trade, when the consumers think that the goods and services offered are basically offered by the plaintiff which is not true it is in fact offered by the defendant. The problem that arises in the case of passing off is that the burden lies on the plaintiff to prove that the defendant has misrepresented his goods using the plaintiff's domain name. Only registering an IP address and not using it does not satisfy this requirement. Thus we realize that under the trademark law as it prevails in India today, taking any action against a person who merely registers a domain name made up of another person's trademark, without actually using the domain name to host a website engaged in commerce, may not be possible.

In the very first case of *Yahoo! Inc. v. Akash Arora*⁸⁹, "wherein the plaintiff, who is the registered owner of the domain name "yahoo.com" succeeded in obtaining an interim order restraining the defendants and agents from dealing in service or goods on the Internet or otherwise under the domain name "yahooindia.com" or any other trademark/ domain name which is deceptively similar to the plaintiff's trademark "Yahoo".⁹⁰

In *Tata Sons Ltd vs. Ramadasoft*⁹¹, "Tata Sons, the holding company of India's biggest industrial conglomerate, the Tata Group, won a case to evict a cyber-squatter from 10 contested internet domain names. Tata Sons had filed a complaint at the World Intellectual Property Organisation".

⁸⁸ AIR 2002 Del 243

⁸⁹ Supra note 51, at 1577

⁹⁰ Shubham Adhikari1, Shashank Tyagi, Trademark trafficking in cyberspace, 4, International Journal of Law, 220-222, 2018, <https://www.lawjournals.org/assets/archives/2018/vol4issue2/4-2-93-717.pdf>

⁹¹ 90(2001)DLT659; 2001 PTC 432

In *Sbicards.com vs Domain Active Property Ltd*⁹², “Sbicards.com was ordered by the World Intellectual Property Organisation to be transferred to the Indian Company from an Australian entity, which hijacked the domain name hoping to later sell it for a hefty sum to the State Bank of India subsidiary.⁹³ The panel accepted SBI Card counsel’s argument that “the Australian company was in the business of buying and selling domain name through its website”.⁹⁴

In *Bennett Coleman & Co Ltd vs. Steven S Lalwani*, since 1996, “the complainant has held the domain names, www.economicstimes.com, using them for the electronic publication of their respective newspapers. The complainant had registered in India this mark for literary purposes. However, in 1998, Steven S. Lalwani, USA registered the same domain name. The WIPO judgment made it clear that the complainant has a very substantial reputation in their newspaper titles arising from their daily use in hard copy and electronic publication. It was also categorically held that the registration and use of the domain names by the respondents is in bad faith in the sense that their use amounted to an attempt intentionally to attract, for commercial gain, Internet users to their web sites by creating a likelihood of confusion with the complainant’s marks as to the source, sponsorships, affiliation or endorsement of those web sites and the services on them”^{95, 96}.

In the case of *Intel Corporation v. Anil Handa*⁹⁷, “Intel Corporation filed an application seeking an interim injunction against the defendants to prevent them from using the word “Intel” as a part of their corporate name. The defendants are not using the word “Intel” as their trademark or trade name. Intel Engineering Pvt. Limited and Intel Travels Pvt. Limited was using the word “Intel” as a part of its corporate name. The defendant argued that they were carrying on their business for a long time in India and the plaintiff even after becoming aware of their existence, never complained to their

⁹² 2005 (31) PTC 455

⁹³ Shubham Adhikari1, *Supra* note91, at

⁹⁴ [slideshare.net](https://www.slideshare.net/slideshow/trademark-issues-in-cyberspace/14883332), <https://www.slideshare.net/slideshow/trademark-issues-in-cyberspace/14883332>, (last visited June. 6, 2024).

⁹⁵ Terese L Arenth, Trademark Protection in the Digital Age: Protecting Trademarks from Cybersquatting, [americanbar.org](https://www.americanbar.org/groups/business_law/resources/business-law-today/2019-june/trademark-protection-in-the-digital-age/), (June. 7, 2024, 7:19 AM), https://www.americanbar.org/groups/business_law/resources/business-law-today/2019-june/trademark-protection-in-the-digital-age/

⁹⁶ [academia.edu](https://www.academia.edu/1426116/Cybersquatting_and_Domain_Name_Dispute_Under_Trademark_Law), https://www.academia.edu/1426116/Cybersquatting_and_Domain_Name_Dispute_Under_Trademark_Law, (last visited June. 6, 2024).

⁹⁷ 2006 (33) PTC 553

corporate

name before. Further, the business of the defendants was entirely different than that of the plaintiff and therefore, there is no likelihood of confusion”.

*Dr. Reddy's Laboratories Ltd. V. Manu Kosuri*⁹⁸, “the plaintiff had a registered domain name www.drreddys.com. The Defendants who were also in the business of operating websites adopted the domain name drreddyslab.com. The Court observed that the defendant was liable to be prosecuted for an action of passing off since the domain name serves the same function as a trademark mark and thus the court was pleased to restrain the defendant”.

In January 2003, Maruti Udyog filed an arbitral complaint with the World Intellectual Property Organisation (WIPO) alleging that Mr Tella's domain name infringed Maruti's trademark, 'MARUTI' and, hence, had the right to the domain name. The plaintiff, Mr Tella said that his use of the domain name was lawful as the domain was at one point primarily used to post photos of a nephew named Maruti though later he converted the Web site to an engine portal. Mr Tella earned revenues from the site through an affiliated Web site that paid him every time someone clicked on www.maruti.com to reach the affiliated Web site. However, Mr Tella is known to be a cyber squatter with a history of registering Web sites having the names of trademarked companies.

Unlike many developed countries, in India we have no Domain Name Protection Law, and cyber-squatting cases are decided under the Trade Mark Act, of 1999⁹⁹. The Hon'ble Supreme Court in *Satyam Infoway Ltd vs Sifynet Solutions Pvt Ltd*¹⁰⁰; has observed that the “*distinction lies in the manner in which the two operate. A trademark is protected by the laws of a country where such a trademark may be registered. Consequently, a trade mark may have multiple registrations in many countries throughout the world. On the other hand, since the internet allows for access without any geographical limitation, a domain name is potentially accessible irrespective of the geographical location of the consumers. The outcome of this potential for universal connectivity is not only that a domain name would require worldwide exclusivity but also that national laws might be inadequate to effectively protect a domain*

⁹⁸ 2001 PTC 859

⁹⁹ blog.ipleaders.in, <https://blog.ipleaders.in/laws-tackling-cyber-squatters-cyber-squatting/>, (last visited June. 6, 2024).

¹⁰⁰ AIR 2004 SC 3540

name”.¹⁰¹ The Indian Courts though have recognized the lacuna, however, in the absence of explicit legislation, courts apply provisions of the Trade Marks Act to such disputes. The Court in Case (Supra) further observed that-

“As far as India is concerned, there is no legislation which explicitly refers to dispute resolution in connection with domain names. But although the operation of the Trade Marks Act, 1999 itself is not extra territorial and may not allow for adequate protection of domain names, this does not mean that domain names are not to be legally protected to the extent possible under the laws relating to passing off”. In *Starbucks Corporation v. Mohanraj*, “the respondent’s domain name www.starbucks.co.in was confusingly similar to complainants’ domain name www.starbucks.in.¹⁰² It was contended that the domain name of the respondent is identical and confusingly similar to the complainant’s domain name. Also, it was contended that the respondent had no legitimate interest in the domain name. Further, it was contended that the mark was used by the respondent in bad faith”.

In *Morgan Stanley v. Bharat Jain*, “the disputed domain name www.morganstanleybank.co.in was registered by the respondent on June 20, 2010. The complainant contended that addition of ccTLD “.co.in” was insufficient to render the disputed domain name dissimilar to the complainant’s mark MORGAN STANLEY.¹⁰³ Hence the disputed domain name was confusingly similar to the above-stated mark”. Where huge financial transactions are involved a check on cyber-squatting needs to be done. These cases happen when the cyber squatters get complete information about the consumer’s credit cards and they tend to misuse it. Hence big firms and banks have their own IT department which deals in such issues.

5. CYBERSQUATTING IN THE UNITED STATES OF AMERICA

Domain names are dealt with differently in different jurisdictions. A mooted issue in this context is whether the domain name is considered under the spear of intellectual property or

¹⁰¹ Sanya, Understanding The World Of Domain In Cyber And IT Law, legalserviceindia, (June. 7, 2024, 7:19 AM), <https://www.legalserviceindia.com/legal/article-7930-understanding-the-world-of-domain-in-cyber-and-it-law.html>

¹⁰² ssrana.in/ip-laws, <https://ssrana.in/ip-laws/domain-names-india/domain-names-faq/>, (last visited June. 6, 2024).

¹⁰³ Pratibha Ahirwar, Domain Name Disputes And Cybersquatting In India – Part II, mondaq.com, (June. 7, 2024, 7:19 AM), <https://www.mondaq.com/india/trademark/784296/domain-name-disputes-and-cybersquatting-in-india--part-ii>

only property, both of them or neither of them. In the United States, the question of whether a domain name constitutes a property right has not yet been finally resolved. There is no formal link between the international domain names system and the national trademark law system, new principle needs to be developed on an international level more clearly to define the nature of a domain name and the respective rights of domain name registrants and trade mark holders¹⁰⁴. Prior to November 1999, domain name disputes in the United States were decided by courts under three primary theories of trademark law.¹⁰⁵

- The first claim is traditional trademark infringement, which requires that the allegedly infringing use causes a likelihood of consumer confusion.
- The second cause of action, and one that is often the most successful in the context of domain names -- is the assertion that a domain name "dilutes" the value of a trademark.
- Finally, unfair competition a claim similar to trademark infringement may be used in cases where the trademark is not federally registered¹⁰⁶.

The approach that was adopted in the United States of America prior to 1999 can be understood by referring to the judgments in two landmark cases, namely *Panavision International v. Dennis Toeppen*, and *Intermatic Incorporated v. Dennis Toeppen*.

In both of these cases, the facts were almost similar. Defendant Toeppen had registered domain names containing the plaintiffs' trademarks, and without having used the domain names in relation to the sale of goods or services, Toeppen intended to sell the domain names to the plaintiffs. In both cases the Anti-Dilution Law has been applied to cyber-squatting. The Federal Anti- Dilution Act which is incorporated in the form of Section 43(c) in the Lanham Act defines the term "dilution" to mean "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".

¹⁰⁴ *Supra* note 33, at 1581

¹⁰⁵ cyber.harvard.edu, <https://cyber.harvard.edu/property00/domain/main.html>, (last visited June. 6, 2024).

¹⁰⁶ Froomkin, A. Michael, "Wrong Turn In Cyberspace: Using ICANN To Route Around The APA And The Constitution", *Duke Law Review* (2000). <http://personal.law.miami.edu/~froomkin/articles/icann.pdf>.

In order to prove a violation of the Federal Trademark Dilution Act, a plaintiff must show that

- (1) The mark is famous,
- (2) The defendant is making a commercial use of the mark in commerce,
- (3) The defendant's use began after the mark became famous,
- (4) The defendant's use of the mark dilutes the quality of the mark by diminishing the capacity of the mark to identify and distinguish goods and services.

In *Intermatic Incorporated v. Dennis Toeppen*, the Court held that “Toeppen’s desire to resell the domain name is sufficient to meet the “commercial use” requirement of the Lanham Act.”

In the case of *Panavision International v. Dennis Toeppen*, which involved similar circumstances, the Court affirmed the view taken in the *Intermatic* case and held that “Toeppen made a commercial use of Panavision's trademarks. It does not matter that he did not attach the marks to a product. Toeppen's commercial use was his attempt to sell the trademarks themselves.”

In an appeal, the Court of Appeal held that Toeppen's conduct diminished the capacity of the Panavision mark to identify and distinguish Panavision's goods and services on the Internet. This finding was based on the reasoning that any person visiting the website for the first time would guess that it should constitute the word Panavision. Having done so when the person would reach the website, and find that it belonged to some other entity, he would be frustrated, and angry and would in certain cases give up his search for Panavision’s website.

The Court of Appeal also observed that involuntarily forcing a company to leave its registered trade name and reputation to the mercy of a cyber-squatter constituted a "dilution" of the trade name. It must be noted here that the interpretation of ‘commercial use’ that was used in the above cases, cannot be used in situations where the domain name is merely registered without any further sign of an intention to sell the same. In some of such cases, the American Courts have come to the rescue of the trademark owner by broadening the meaning of infringement.

For instance in *Green Products Co. v. Independence Corn By-products Co.* “where the defendant registered a domain name containing the plaintiff's trademark, but did not post a website, the Court held that this act amounted to trademark infringement. The Court held that

ICBP intended to use its confusing domain name to lure potential customers to the site once it was created. While customers might not be confused as to affiliation once they get to the site, they may simply purchase ICBP's products rather than search for Green Products' real site. Under this scenario, ICBP would benefit unfairly from the use of Green Products' name".

Another important case is that of *OBH Inc v. Spotlight Magazine*¹⁰⁷ in this case "the defendant had registered the domain name containing the plaintiff's trademark. Although the site did not contain any material, that could be said to make the site being used in commerce, or in relation to goods or services, it did contain links to the defendant's other site through which they were dealing in their products. The mere existence of these links led the court to the conclusion that the site satisfied the use in commerce and in relation to goods or services requirement of the Lanham Act". Planned Parenthood, the well-known non-profit reproductive health organization was the target of a similar effort by a "competitor" to divert attention on the web. In *Planned Parenthood Federation of America. v. Bucci*¹⁰⁸, "Planned Parenthood obtained an injunction against an anti-abortion and anti-birth control advocate who set up a web site at <www.plannedparenthood.com> to provide information and promote sales of an anti-abortion book. Planned Parenthood was operating its own web site at <www.ppfa.org> (and its Houston affiliate at <www.plannedparenthood.org>). In finding a likelihood of confusion the court noted that the defendant admitted that he chose the domain name with the intent to divert Internet users who were seeking Planned Parenthood's web site to his own competing site".

*Comp Examiner Agency, Inc. v. Juris, Inc.*¹⁰⁹ is the first case in which a U.S. court applied a traditional likelihood of confusion analysis in the context of a domain dispute. "In that case, Juris, Inc., owner of a federal trademark registration of JURIS for its legal time and billing software products, had been forced to choose the domain <jurisinc.com> after learning its first choice, <juris.com>, had already been assigned to The Comp Examiner Agency ("Comp Examiner"). When Juris, Inc. subsequently accused Comp Examiner of trademark infringement, Comp Examiner, which used the domain for a legal information web site, filed an action seeking cancellation of Juris, Inc.'s JURIS trademark registration on grounds of genericness. Juris, Inc. then counterclaimed for trademark infringement. The court granted

¹⁰⁷ 86 F. Supp. 2d 176 (W.D.N.Y. 2000)

¹⁰⁸ 42 U.S.P.Q.2d 1430 (S.D. NY, 3/19/97)

¹⁰⁹ 96-0213-WMB (Ctx), 1996 WL 376600 (C.D. Cal. May 22, 1996)

Juris, Inc. a preliminary injunction which not only precluded Comp Examiner from using the domain <juris.com> but also from using "juris," <juriscom.com> or any confusingly similar variation for "the advertising, operation or maintenance of any Internet site or bulletin board service." The lawsuit was settled shortly thereafter. Juris, Inc. now owns both domains and operates under the domain <juris.com>".

In *Green Prods. Co. v. Independence Corn By-Prods. Co.*¹¹⁰ "Both companies were direct competitors in the corncob by-product industry. ICBP registered greenproducts.com but had not yet posted a web site when Green Products sued them. Even though no web site had been posted, the court held that ICBP intended to use its confusing domain name to lure potential customers to the site once it was created. While customers might not be confused as to the affiliation once they get to the site, they may simply purchase ICBP's products rather than search for Green Products' site, and thus ICBP would benefit unfairly from the use of Green Products' name. The court acknowledged that this is a different interpretation of consumer confusion than is typically used to find trademark infringement. Typically, courts examine whether a company intended to confuse consumers into thinking that its own products were made by a competitor company because ICBP could deceptively lure potential customers to its own site where they would be told how ICBP is better than Green Products, the court found such deceptive use of a competitor's trademark to qualify as consumer confusion. On these facts, the court found that there was infringement". Domain name law has gone through three phases. In the first phase, the existing trademark law was applied by the courts to deal with cyber squatting. In the second phase, the courts interpreted and applied the "Anti-Cybersquatting Consumer Protection Act" that became law in 1999. This Act increased the protection of trademark owners against domain name speculators. In the third phase, most claims have been settled under the Uniform Dispute Resolution Policy ("UDRP"), which all registrants of ".com", ".net", and ".org" domain names must accept. This policy tilted the rules even further in favor of trademark owners¹¹¹.

- **THE LANHAM'S ACT,1946**

¹¹⁰ 992 F.Supp.1070 (N.D. Iowa Sept. 25, 1997)

¹¹¹ Peter B.Maggs, "The ".us" Internet Domain", American society of comparative law, vol 50 (2002). <http://www.jstor.org/stable/840880>.

In *Vanity Fair Mills v. T. Eaton Co*¹¹² “Plaintiff, an American corporation had manufactured and sold women's undergarments in the United States and Canada since 1917, under a U.S. registered trademark, "Vanity Fair." The defendant, a Canadian corporation, had registered the same trademark in Canada in 1915, and for this reason, the plaintiff's application for a Canadian trademark was denied in 1919. From 1945 to 1953, the defendant purchased plaintiff's trademarked goods for resale in Canada. In 1953, the defendant began selling goods of Canadian manufacture with its own Vanity Fair trademark and threatened its competitors in Canada with infringement suits if they continued to sell the plaintiff's trade-marked goods. In an action brought in the United States District Court for the Southern District of New York, the plaintiff sought an injunction against the defendant's use of the trademark "Vanity Fair," claiming that the defendant's Canadian sales constituted trademark infringement and unfair competition under both the Lanham Act and the International Convention for the Protection of Industrial Property. The district court dismissed for lack of federal question jurisdiction over the alleged infringement and unfair competition occurring in Canada. On appeal to the Court of Appeals for the Second Circuit, held, affirmed”.

Prior to the Lanham Act of 1946, the law of trademarks and unfair competition was a checkerboard of federal and state law. Early federal trademark statutes had dealt solely with procedural matters, leaving the determination of substantive rights in trademarks to the common law. After it was determined that there was no general federal common law of trademarks, a trademark owner's rights in one state differed widely from the rights that he enjoyed in another. It was primarily to remedy this uncertain situation that the Lanham Act was passed¹¹³. By providing substantive rights in registration and conferring broad jurisdiction on the federal courts, it gave nationwide protection to registered trademarks. To deal with the rising issue of the trademark in the United States of America became a signatory to many treaties. To implement the treaties and provide for trademark rights as well remedies to foreigners similar to United States citizens the Lanham Act came into the picture which ensured an effective protection against any unfair practice¹¹⁴.

¹¹² (2d Cir. 1956) 234 F. (2d) 633, cert. den. 352 U.S. 871 (1956).

¹¹³ William R. Luney, “Trademarks: Extraterritorial Application of the Lanham Act”, *The Michigan Law Review Association*, vol 55(1957). <http://www.jstor.org/stable/1285935>.

¹¹⁴ Carl E. Simon, “Trademarks and Trade names: unclean hands as a defense in suit for infringement”, *California Law Review*, vol34. <http://www.jstor.org/stable/3477566>.

- **THE ANTI CYBERSQUATTING CONSUMER PROTECTION ACT, 1999**

Looking at the increasing rate and anticipating further cases of domain name disputes and cases of cyber-squatting, a need was felt for independent legislation that can exclusively deal with issues of cyber-squatting. The degree of legal protection for a trademark depends upon the strength of the mark. A mark to be a trademark should be distinctive only then can it be protected from infringement. Distinctive trademarks are "arbitrary" or "fanciful," that is, not logically connected to the product. For example, the Apple Computer logo has no connection to a computer and the Lotus logo has no relation to a sunscreen lotion. These marks have no natural connection with the products but have gained goodwill through their trademark owners. Descriptive names are protectable by trademark law only if it can be demonstrated that a "secondary meaning" has been advanced within the mindset of consumers. A secondary meaning is created when a word with an ordinary meaning (such as "bug") may after long use with a particular product, come to be known by the public as specifically designating that product"¹¹⁵.

The United States of America has been a pathfinder in this field by enacting the Anti Cybersquatting Consumer Protection Act, of 1999. Section 3002 of this Act amends Section 43 of the Trademark Act of 1946 (Lanham Act), by inserting sub-section (d) at its end. The section has been named Prevention of Cyber piracy. The provisions of this subsection which specifically deal with the cases falling under the term cyber-squatting are as follows: (d) (I) (A) "A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person –

- has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and
- registers, traffics in, or uses a domain name that –

¹¹⁵ Richard A. Spinello, "Online Brands and Trademark Conflicts: A Hegelian Perspective", Business Ethics Quarterly vol 16 (2006). <http://www.jstor.org/stable/3857920>.

- i. in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
- ii. in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or
- iii. Is a-trademark, word, or name protected by reason of section 706 of title 18, United States Code, or section 220 of title 36, United States Code”.

The above-mentioned section deals with a large pool of cases. Firstly, it covers the cases of cyber-squatting wherein a person registers a domain name that is identical or deceptively similar to the mark owned by another person, with the bad faith intention of selling the said domain name to the mark owner at a huge price. The section provides an illustrative list of factors that the Court may take into consideration while reaching a conclusion about the existence of a bad faith intention. The benefit of not making this list exhaustive is that it allows the Courts to look at new factors, which may indicate bad faith in the particular circumstances of a case.

A perfect example would be *Sporty's Farm LLC v. Sportsman's Market Inc*¹¹⁶. “In this case, the Court established bad faith on the basis of the fact that the defendant was set up, under the name similar to the plaintiff's trademark, by its parent company only after the domain name dispute had arisen, and it was only then that the domain name was sold by the parent company to the defendant”.

On examining this bad faith factor one realizes that the legislature's intention was to also cover a case wherein a person registers a domain name that is identical or deceptively similar to the mark owned by another person, with the intention of either using the website posted at that domain name to tarnish the goodwill of the mark owner, or to use the website to pass off his goods or services as those of the mark owner.

The section also includes the words ‘without regard to the goods or services of the parties.’ Under the traditional trademark law, in order to establish infringement of a trademark, the goods or services in relation to which the infringing use of the mark was made is an important factor to be considered. It is also necessary that the infringing use of the mark was made in the course of commerce. As seen earlier in the USA the Dilution Law came to the rescue of the

¹¹⁶ 202 F. 3d 489 (2d Cir. Feb. 2, 2000)

aggrieved mark owners in such cases. The words ‘without regard to the goods or services of the parties’ have been inserted keeping in mind the problem created by the traditional trademark law requirement.

In the USA before the Anti Cyber Squatting Consumer Protection Act the Anti-Dilution Law was in force to deal with such cases, where as in India there is no parallel to the Anti-Dilution Law. Therefore the indispensable need of the hour in India is to bring into force a separate law prohibiting cyber-squatting or any other malafide registration of a domain name¹¹⁷.

The major crunch faced by trademark owners today is that even though they can prove that the domain name of the defendant is infringing his trademark in reality he can never find out the true registrant of the domain name. This is the major drawback in the virtual world as people with bad intentions tend to put wrong information about their details. Moreover, the Internet being global in nature establishing jurisdiction can be difficult. Keeping this in mind a provision has been made in the Anti Cybersquatting Consumer Protection Act¹¹⁸, which enables an aggrieved trademark owner to file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located, if the domain name violates any right of the owner of a mark registered in the Patent and Trademark office, or protected under subsection (a) or (c) and the court finds that the owner is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1), or through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1). Paragraph (1) refers to the paragraph (1) of Section 43(d), which deals with cyber piracy.

The remedies that are available in a civil action under paragraph (1) of Section 43(d) or in an inrem action under paragraph (2) of the said section, are forfeiture or cancellation of the domain name or transfer of the domain name to the owner of the mark, by the Court’s order. The section makes it clear that these remedies would be in addition to remedies available otherwise. These

¹¹⁷ Sanjay Bhatia, “Domain names, cyber squatting and Trademarks in India- A Legal Perspective,” at <http://law.indiainfo.com/cyberlaw/10-5-2000.html>.

¹¹⁸ Section 43(d)(2)(A) of the Trademark Act 1946 (15 U.S.C. 1125)

would include an injunction, damages, or statutory damages under the Trademark Act 1946. Section 308 of the Anti-Cybersquatting Consumer Protection Act provides as follows, 'Nothing in this title shall affect any defense available to a defendant under the Trademark Act of 1946 or a person's right of free speech or expression under the first amendment of the United States Constitution.'

The defenses referred to in this section include the non-commercial use of a mark, its use in comparative advertising, or its use in any news item. Thus in short this section provides the other defenses that a domain name registrant can take in an action under the Act¹¹⁹. Thus the United States of America has taken a worthy step towards punishing cyber-squatters.

6. DEFENSES OF THE CYBERSQUATTER

The best defense for an accused cyber squatter is the act's "safe harbor provision," that is if the cyber squatter can prove that he did not have bad intentions and believed that registering of particular domain name was lawful, the use of the domain name was a fair use and if the court concludes that this belief was reasonable under the circumstances (15 U.S.C. s 1125 [d][I][B][ii]). Other attempted defenses by alleged cyber squatters, however, have met with little or no success. For example, courts have rejected defendants' assertions that the act did not apply to them because of the following:

- The domain name was pronounced differently from the identical trademark or trade name,

*Interstellar Starship Services Ltd. v. Epix, Inc.*¹²⁰, "in which the court ruled that these differences "are not readily discernible to the reasonable consumer" because "pronunciation's indistinguishable in printed advertisements".

- The domain name registered had significantly more characters than the trademark,

¹¹⁹ James T.Caleshu, "Trademark and the Free Ride Doctrine", Stanford Law review vol16 (1994). <http://www.jstor.org/stable/1227074>.

¹²⁰ (983 F.Supp. 1331, 45 USPQ2d 1304, D.Ore. 1997)

In *Mattel Inc. v. Internet Dimensions, Inc.* 2000, “in which the purveyor of an “adult” site on the Internet under the domain name “barbiesplaypen.com” was ordered to transfer the name to Mattel, Inc., the owner of the Barbie trademark”.

- The act is unconstitutional because it infringes on the cyber-squatters First Amendment rights

Lucent Technologies, Inc. v. Johnson 2000, “in which the creator of a site called “lucentucks.com” did not succeed in having Lucent’s suit dismissed, despite his argument that he only intended to embarrass Lucent when he registered the domain name “ lucentucks.com” and offered pornographic photographs and services for sale on the Web site”¹²¹. The observation of an American Court in *Hasbro v. Clue Computing*¹²² must be noted here. It observes, “if another Internet user has an innocent and legitimate reason for using the famous mark as a domain name and is the first to register it, that user should be able to use the domain name, provided that it has not otherwise infringed upon or diluted the trademark”.



ABHIDHVAJ LAW JOURNAL

¹²¹ Michael G. Walsh, “Marketer’s Boon in Cyberspace: the Anticybersquatting consumer protection Act”, American Marketing Association vol22 (2003). <http://www.jstor.org/stable/30000845>..

¹²² 994 F. Supp 34 (D. Mass. 1997).

CHAPTER 4: UNIFORM DISPUTE RESOLUTION POLICY FRAMEWORK

1. HISTORY OF DOMAIN NAME ADMINISTRATION

In earlier days internet was used for basic purposes like research work or education purposes. The domain name directory was maintained by Jon Postel, an academic who worked under a research contract from the United States government¹²³. Dr. Postel operated through an entity known as the Internet Assigned Numbers Authority (IANA). The registration policy was "first come, first served" with no review of rights. As the workload of entering and deleting names became heavier, the task was contracted out to a private corporation, now known as Network Solutions, Inc. (NSI)¹²⁴.

NSI continued Dr. Postel's policy but almost as soon as the Net was opened to commercial traffic, trademark disputes arose. The cases in these early days involved "cybersquatting" and "cyber piracy. Frequently unable to obtain service on remote infringers, or to identify the actual domain holder due to false registration data, trademark owners brought contributory infringement actions against NSI for wrongfully granting domain registrations to those without rights to use the mark. Although NSI routinely avoided liability in these contests, it began revising the registration contract signed by domain holders to impose a domain dispute policy that reflected these issues. This dispute policy was revised with some frequency. By 1999 it had several characteristics that were found unsatisfactory by both domain holders and trademark owners. It could only be used by owners of federal or national marks It could only be utilized against a domain name that was identical to the mark unlike the broader standard used in trademark law where infringement is found if the two names are "confusingly similar", And it did not reflect principles of fair use such as free speech or product criticism. In November 1998, the Department Of Commerce entered into a Memorandum of Understanding (MoU) with a private corporation established by Dr. Postel called the Internet Corporation for Assigned Names & Numbers giving ICANN oversight responsibility for domain names, numbers, protocol parameters, and the Root. ICANN had two years to develop methods and procedures for technical coordination in a manner that will ensure bottom-up coordination, market competition, global representation, and stable operations. Introducing competition,

¹²³ Diane Cabell, "Overview of Domain Name Policy", Harvard Law School (2003). <http://cyber.law.harvard.edu/udrp/library.html> .

¹²⁴ Id

however, meant the possibility of conflicting domain dispute policies, so the DOC contract specifically required that ICANN make recommendations regarding trademark/domain name policies particularly those proposed by the World Intellectual Property Organization (WIPO) concerning: (i) the development of a uniform approach to resolving trademark/domain name disputes involving cybersquatting; (ii) a process for protecting famous trademarks in the generic top-level domains; (iii) the effects of adding new gTLDs and related dispute resolution procedures on trademark and intellectual property holders; and recommendations made by other independent organizations concerning trademark/domain name issue¹²⁵.

2. ICANN'S DISPUTE POLICY DEVELOPMENT

ICANN's policy on domain disputes evolved fairly rapidly. The WIPO [proposals](#), which had been circulating for several years, were presented to ICANN in May 1999. They included the establishment of a uniform, mandatory domain name dispute policy for the resolution of cybersquatting disputes and a system of panels to arbitrate them. Many elements were adopted in a model agreement proposed for voluntary adoption by the half-dozen newly-accredited registrars and NSI. The models were presented for public comment during the summer which reported them to be unfairly burdensome on non-commercial and fair users, so the Board [insisted](#) on the following amendments:

- In determining whether a domain name has been registered in bad faith, consideration should be given to the following factors in addition to those stated in the WIPO and registrars'

policies:

- a. whether the domain name holder is making a legitimate non-commercial or fair use of the mark, without intent to misleadingly divert consumers for commercial gain or to tarnish the mark;

¹²⁵ Kevin Eng, "Breaking Through the Looking Glass: An Analysis Of Trademark Rights in Domain Names Across Top Level Domains" (2000).

- b. whether the domain name holder (including individuals, businesses, and other organizations) is commonly known by the domain name, even if the holder has acquired no trademark or service mark rights; and
 - c. Whether, in seeking payment for transfer of the domain name, the domain name holder has limited its request for payment to its out-of-pocket costs.
- There should be a general parity between the appeal rights of complainants and domain name holders.
 - The dispute policy should seek to define and minimize reverse domain name hijacking.

The resulting ICANN proposals, along with a Staff Report, were posted in September for 2 weeks of public comment. The final versions, Uniform (the Policy) and [Rules for Uniform Domain Name Dispute Resolution Policy](#) (the Rules) were accepted by ICANN at its Annual Meeting in Los Angeles in November. The UDRP became effective for all com-org-net registrars by January 2000.

3. UNIFORM DISPUTE RESOLUTION POLICY

The UDRP governs disputes "over the registration and use of an Internet domain name," prescribing a mediation process in which disputes might be resolved more swiftly than in other venues. The UDRP process involves filing a complaint with one of four "providers" approved by ICANN. These providers, which include the World Intellectual Property Organization (WIPO), the National Arbitration Forum (NAF), the Asian Domain Name Dispute Resolution Center, and the Czech Arbitration Court, are prime mediators approved to resolve domain name disputes consistent with the UDRP. In the United States, WIPO and NAF are the most frequently used providers¹²⁶.

Under the UDRP the trademark owner has the right to go for arbitration to obtain cancellation or assignment of infringing domain name if the registrant does not assign the domain name to the actual owner. The UDRP is available to all trademark owners, registered or otherwise. There are a number of authorized arbitration tribunals including but not limited to the World

¹²⁶ Matthew Coleman, "Domain Name Piracy and Privacy: Do Federal Elections Regulation Offer A Solution?" Yale Law and Policy Review vol19 (2000). <http://www.jstor.org/stable/40239564>.

Intellectual Property Organization (WIPO). Filing fees vary among these tribunals. The current filing fee at WIPO is \$1,500 for a single arbitrator¹²⁷.

To be successful in a UDRP arbitration, the complainant must show that:

- (i) The respondent's domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
- (ii) The respondent has no rights or legitimate interests with respect to the domain name;
- (iii) The respondent's domain name has been registered and is being used in bad faith.

It is of great importance amongst IPR practitioners to distinguish between the elements of proof in UDRP and elements of proof in trademark infringement. In UDRP proceedings proof of bad faith is mandatory whereas this is not the case in trademark infringement. If a domain name registrant was unaware of the infringement, that is, if he did not know that his domain name was similar to the trademark of the owner then he was not acting in "bad faith" within the meaning of the UDRP¹²⁸.

The UDRP identifies the following four examples of bad faith:

- (i) circumstances indicating that the respondent has registered or has acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring 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 in excess of his documented out-of-pocket costs directly related to the domain name; or
- (ii) the respondent has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the respondent has engaged in a pattern of such conduct; or
- (iii) The respondent has registered the domain name primarily for the purpose of disrupting the business of a competitor; or

¹²⁷ <http://www.wipo.int/about-wipo/en/budget>.

¹²⁸ Supra note 89, p.236.

(iv) By using the domain name, the respondent has intentionally attempted to attract, for commercial gain, Internet users to the respondent's website or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of the respondent's website or location or of a product or service on the respondent's website or location¹²⁹. The dispute is submitted to a panel of arbitrators from which one arbitrator will be appointed unless a party seeks a panel of three. On December 9, 1999, a week after the procedures of the UDRP were fully implemented, the first dispute, the one involving "worldwrestlingfederation.com," made its way into the system. The number of disputes grew rapidly, with over 400 proceedings concerning over 600 domain names commenced within the procedures' first five months of implementation. For the most part, the cases decided by ICANN-approved arbitrators have met the UDRP's objective of fast and effective resolution of true piracy cases.

For example, in *Perfumes Christian Dior v. Net power, Inc*¹³⁰ “the French perfume manufacturer Christian Dior complained of four domain name registrations: “christiandiorcosmetics.com,” “christiandiorfashions.com,” “diorcosmetics.com”, and “diorfashions.com”. The registrant, an Internet Service Provider (ISP), claimed that he registered the names on behalf of "prospective clients." The arbitrator grew skeptical of this explanation in light of the forty-six other domain names (that included Gucci, Versace, Giorgio Armani, Louis Vuitton, and Levi's) registered by the ISP. The arbitrator found bad faith and ordered the domain names transferred to Christian Dior”. 105 cases out of 120 cases of UDRP were decided in favor of the plaintiffs. This proves that UDRP was effective in punishing the cyber squatters and providing the trademark owners with their legitimate domain names.

The cases in arbitration proceedings in UDRP are decided in forty-five days but these decisions are not binding. The decisions are appealable in the federal court. An aggrieved party may appeal by filing an action in federal court. This process is consistent with the UDRP's goal of providing fast relief in cases of cyber piracy. The UDRP has been effective at removing cybersquatters of domain names.

¹²⁹ Bruce A. McDonald, “International Intellectual Property Rights”, American Bar Association vol 35(2001). <http://www.jstor.org/stable/40707887>.

¹³⁰WIPO Case No. D2000-0022 (Mar. 9, 2000).

For example, in *Western Hay Co. v. Forester*, “the panel identified that the registrant operated the domain name "westernhay.com" as a valid horse nutrition discussion site and not as a vehicle for extorting money from the trademark owner of Western Hay Company. The registrant agreed to transfer the domain name for the costs of registration and an apology. The panel held that this was not a case of bad-faith cybersquatting but, rather, more of a classic trademark dispute”.

A panel exhibited similar restraint in *Credit Mgmt. Solutions, Inc. v. Collex Resource Mgmt*¹³¹. “In that dispute, the parties offered credit services to different markets automobile dealers versus individuals. The panel noted that the registrant used the domain name as part of a bona fide non-competing business. The panel also noted that there was an issue of fact as to the likelihood of confusion between the parties that could not be resolved in a UDRP proceeding. The domain name was not transferred”.

In *Mondich v. Brown*¹³² case involved the New York owner of the American Vintage trademark against the California registrant of “americanvintage.com”. “The trademark was used on biscuits; the domain name was registered by an antique store (Big Daddy's Antiques). After the complaint was filed, the trademark owner spoke with the registrant who offered to sell the domain name. The registrant defaulted on the complaint and the panel found in favor of the trademark holder. Although a defaulting party rarely gets the benefit of the doubt, this case is troubling because the arbitrator was willing to infer bad faith solely from the registrant's failure to use the domain name for over two years and from its failure to present evidence of good faith. This approach reverses the requirement that the complainant affirmatively establish bad faith before obtaining any remedy under the UDRP. Here, the arbitrator was willing to infer bad faith because the registrant offered to sell the domain name to the trademark holder despite circumstantial evidence (Big Daddy was in the antiques business, after all) that the registrant's use of "americanvintage.com" was legitimate. This case was a default and should be considered in that context. It can be limited to a situation where two nonfamous, non-competing trademarks coexisted on opposite sides of the United States. A small antique store would likely be overwhelmed with the domain name dispute process, so the default is not surprising,

¹³¹ WIPO Case No. D2000-0029 (Mar. 17, 2000).

¹³² WIPO Case No. D00-0004 (Feb. 16, 2000).

although the outcome is troubling in that it posits a finding of bad faith in the absence of compelling facts”.

Other UDRP panels have found bad faith on marginal grounds. In *Dollar Financial Group, Inc. v. Roark*, “the arbitrator transferred the registrant's domain names "loanmart.org" and "loanmart.net" to the owner of the service mark Loan mart, in use for financial services. The registrant presented some plausible arguments that it chose "loanmart.com" as an acronym for "Lotions, Oils, and Nutriment Mart." The website was to be used for sales of health and beauty care items. The registrant had previously obtained a patent in 1995 for a lotion container. Most importantly, the registrant had checked the U.S. Patent and Trademark Office online database and discovered that the trademark owner held the registration to LOAN MART, but for a different class of services. The arbitrator focused on the fact that the registrant had asked for \$7,500 to transfer the domain names and on the registrant's lack of use of the domain names as evidence of bad faith. It is possible that the registrant created the lotion story in an effort to avoid transfer, but the case seems close to the facts. It is very much the kind of case that would benefit from full litigation to test the registrant's story”.

Another suspect decision is found in *Fiber-Shield Industries, Inc. v. Fiber Shield LTD*, “in which the complainant owned the 1999 federal trademark registration for FIBER-SHIELD and had registered "fibershield.com" in 1997. The registrant had been doing business in Canada under the trade name Fiber Shield LTD. The registrant attempted to register the domain name "fibershield.com" but, upon finding that it was in use, registered "fibershield.net" as an alternative. The arbitrator stripped the registrant of the domain name in a remarkable leap of logic. The arbitrator reasoned that the registrant had acted in bad faith because it knew that the "fiber shield.com" domain name was unavailable and because it did not claim "superior" rights to the trademark FIBERSHIELD. The decision is made more perplexing by the absence of any evidence of a bad-faith intent to profit from the domain name. This is an example of a case that would be more appropriately pursued as a conventional trademark/domain name dispute involving concurrent trademark usage”.

Better reasoned, but also questionable, is the decision in *America Online, Inc. v. Tencent Communications Corp.* “In that case, the registrant had registered "oicq.com, in 1999 and

"oicq.net" in 1998. America Online owns several registrations worldwide for the mark ICQ, in use with its instant messenger service. The registrant used the "oicq" domain names as portals to transfer users to "tencent.com," a Chinese website. The registrant argued that the Chinese market is separate from other AOL markets and that AOL had only recently introduced ICQ in Chinese. The arbitrator noted that the decision was difficult to make, but nevertheless found that the registrant had no legitimate interest in the use of "oicq" as a domain name and concluded that the name was registered in bad faith in order to attract, for commercial gain, users to its site by creating a likelihood of confusion with AOL's ICQ mark¹³³.

The UDRP despite being a fast and inexpensive procedure is considered to be imperfect. Specifically, it provides too little guidance to arbitrators, a flaw that has led to inconsistent decisions on several key domain name use issues and, related concern that some decisions exhibit a bias toward corporate trademark holders. Additionally, to the extent that the UDRP has provided uniform principles of dispute resolution, these principles are inapplicable to a growing segment of domain names; namely, those obtained through registrars not accredited by ICANN or through a country code authority that has not elected to bind its registrants to the UDRP.

4. JUDICIAL REMEDIES IN DOMAIN NAME DISPUTES

Trademark holders were given specific statutory protection against cyber-squatting in 1999 with the enactment of the United States Anticybersquatting Consumer Protection Act (ACPA). The main purpose of ACPA is to protect consumers and businesses "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". There were several lacunas in the dilution Law, because of which the ACPA was considered necessary, one of the drawbacks of dilution Law was that it was expensive and uncertain¹³⁴. The remedy section of the Lanham Act was correspondingly amended to provide trademark holders a strong weapon against cyber squatters, up to \$100,000 in statutory damages per domain name. Although courts outside of the United States also have addressed the cybersquatting issue to some extent, the ACPA is undoubtedly the most specific and widely applicable judicial remedy available¹³⁵.

¹³³ Supra note 34, at 1598

¹³⁴ Supra note 87, at 1598.

¹³⁵ Marilyn C.Maloney, "Intellectual Property in Cyberspace", American Bar Association vol53 (1997). <http://www.jstor.org/stable/40687783>.

The ACPA's in rem provision provides that a trademark holder may proceed in rem against any domain name in the judicial district in which the domain name registry is located", because in rem jurisdiction is conferred over the domain name itself rather than over an individual, it applies regardless of whether the participants are residents of other countries or even whether they have minimum contacts with the forum. Today, a savvy cyber squatter could evade this provision by registering with an ICANN-approved registrar in, for example, Kuwait or Singapore. Even then because of NSI and US-based registrars, many cases of cyber-squatting would be subject to United States jurisdiction. It may happen that other nations may find their order not binding if the United States continues to dominate the domain name registration system.

The UDRP In response to concerns about judicial remedies and the conflict between territorial trademark systems and the "global dimension" of domain name disputes, in June 1998 the World Intellectual Property Organization (WIPO) accepted a United States proposal that it will develop recommendations for a consistent international approach. Within a year, WIPO published a report concluding that ICANN should create a uniform administrative procedure for the resolution of disputes concerning generic top-level domain (gTLD) registrations. ICANN implemented most of WIPO's recommendations in its Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP represents a substantial departure from traditional international trademark law. International trademark issues customarily have been addressed through complex and time-consuming negotiations that result in multinational treaties¹³⁶.

Although ICANN plays a quasi-governmental role in the administration of the Internet, enforcement of the UDRP is based entirely on private contracts. The UDRP does not eliminate the availability of court proceedings for domain name disputes". Despite the availability of the judicial remedy, however, "only a minuscule handful" of decisions under the UDRP have been appealed through the court system. What is clear is that, although the UDRP was not intended to be a substitute for traditional infringement or cyber-squatting litigation, in many ways it has become a substitute. Furthermore, the UDRP has become the leading forum for domain name dispute resolution, with over 7500 proceedings initiated since December 1999¹³⁷.

¹³⁶ *Supra* note 96, at 1599

¹³⁷ Paul Godfred and Kristine Dorrain, "Survey of the Law of Cyberspace", American Bar Association vol 65(2009). <http://www.jstor.org/stable/40688586>.

5. FLAWS AND LIMITATIONS IN THE UDRP

No policy can be perfect in nature, and the same applies to UDRP. There lies a lot of inconsistency on the issues of domain names and this in turn makes the critics think that arbitrators are being biased towards the business entities¹³⁸. The ICANN's goal was to create uniform international standards, which the UDRP has still not accomplished. This shortcoming is inherently linked to the issues of consistency and fairness in individual cases, because even if ICANN can address these concerns successfully, it nonetheless is unable to implement the resulting uniform principles in a fully comprehensive international manner.

As a result, the current flaws in the UDRP have left the international Internet community with little approach to dispute resolution and a corresponding unfulfilled need for a comprehensive and consistent solution. ICANN is also suffering from the inconsistency of the UDRP as ICANN disseminated the UDRP. Already ICANN has been the target of a variety of legitimacy critiques since its birth, and the lack of consistency in the application of the UDRP supports these critiques by putting its integrity into question. The ICANN will have to take massive steps to save itself from the critiques like it will have to formulate strong policies. ICANN therefore should address the problem of inconsistent decisions under UDRP arguably ICANN's best-known policy is not only to improve the dispute resolution system but also to enhance its own integrity¹³⁹.

CONCLUSION AND SUGGESTION:

Today, cybersquatting has picked up a great deal of notoriety, there is most likely that even charge card cheats are less in the news but rather more space names and digital crouching. Since the Internet is a worldwide wonder, steps are as of now brewing to handle the threat of domain name dispute, particularly digital hunching down, on a universal level.

The way to a government solution for trademark proprietors who are abused by unapproved utilization of their imprints is extreme. The Lanham Act may offer a solution for post-space trademark encroachment, yet that cure accepts that the wronged mark proprietor can recognize

¹³⁸ Peter B. Maggs, "The ".us" Internet Domain", American Society of Comparative Law vol 50(2002). <http://www.jstor.org/stable/840880>.

¹³⁹ Lisa M. Sharrock, "The Future of Domain Name Dispute Resolution", Duke University School of Law, vol 51(2001) <http://www.jstor.org/stable/1373211>. Last retrieved: 13th February 2014.

and get a locale over the culpable client. There is a very logical alternative provided by amending the ACPA to deal with domain name disputes. An effective remedy in domain name disputes can only be obtained through the ACPA's in rem jurisdiction. With the advancement in the technology in the electronic medium the trademark owner's rights should not be affected, whether the mark is registered or not There should be protection of the goodwill of the firm. It can very well be argued in favor of the cyber-squatters that the domain name registration system itself is flawed. If a person wishes to register a domain name legitimately, he should not be penalized if he wishes to trade in it. Making easy money in itself is not a crime. From the legal point, it can be contended that a cyber-squatter does not deal in any goods and hence, his activities are not likely to cause confusion in the minds of the public. There are not many defenses to favor cyber squatters hence the alarming need of the hour is that the legislature understands the technical developments and passes a separate law prohibiting cyber-squatting or any other malafide registration of a domain name. The National Association of Software and Service Companies (NASSCOM) has made a recommendation to the Ministry of Information and Technology to bring about some more regulations in the statutory Acts pertaining to Copyrights and Trademarks applicable to the Internet to prevent cyber-squatting.

We cannot turn a blind eye to the fact that decisions of the WIPO are not as authoritative as the law stands in the country and the final decision lies in the hands of the court and legal mechanism in place will be followed for disputes that arise out of the domain names over the internet. Thus, it can be concluded from the above discussion that Cyber-squatting of domain names pertaining to Trademarks is going to pose real challenges to the legal fraternity in India in the near future. Various challenges are posed by the aspirants who indulge themselves in the global business market. As the virtual world is expanding, and as advanced techniques of accessing information unfold, the existing trademark law might not be able to cope with them. In such cases, the trademark owners might continue to be uncertain about their rights. Hence the Indian legislation is to be proactive in implementing suitable legislation.

One of the most ticklish issues facing the legal community today is the jurisdiction of the courts to decide Internet disputes. Internet disputes fall broadly under three categories:

- A. Internet crimes (hacking, pornography, defamation, etc.)
- B. Disputes relating to e-commerce (contracts, digital signatures, etc.)

C. Disputes involving Intellectual Property law (domain name disputes, caching, linking disputes, etc.)

The focus should be shifted to the scope of the territorial jurisdiction of the Indian Courts in entertaining disputes in relation to Intellectual Property law, (typically - a domain name dispute) especially in a situation where the defendant happens to be outside India. Domain name disputes are increasing at a high rate in India but unfortunately, India does not have any legislation to deal with the problem of cyber-squatting whereas this activity is punishable under US Law... Domain names have become a big trading business today and around 10,000 domain names get registered daily. A person aggrieved by the registration of a domain name has two legal remedies, i.e. to resort to the Uniform Domain Name Dispute Resolution Policy of the ICANN, or to file a civil suit in a competent court having jurisdiction, claiming a permanent injunction against the defendant seeking to restrain him from using the concerned domain name.

The only law in India, governing jurisdiction (in case of a domain name dispute) is the Code of Civil Procedure. In this regard, Section 20 of the CPC provides the plaintiff with two options:

- a) to file a suit in a court within whose jurisdiction the defendant (or one of them) resides, or;
- b) to file a suit in a court within whose jurisdiction the cause of action, either wholly or in part, arises. In effect, a court in India would have jurisdiction to entertain a domain name dispute, even if the defendant resides outside the country, in case the plaintiff establishes that the cause of action is within the territorial jurisdiction of the court. The requirement of the current time is to harmoniously apply the principles of the trademark law and the provisions concerning domain names. It is clearly time for a stringent law in India to deal with the issue of cyber-squatting. After all, managing a problem once is better than looking into the same problem repeatedly.

BIBLIOGRAPHY:**STATUTES, CONVENTIONS AND RULES REFERRED**

1. Information Technology Act 2000 (India)
2. Lanham Act, 1976 (USA)
3. Anti Cyber Squatting Consumer Protection Act, 1999 (USA)
4. Trade Marks Act, 1999 (India)
5. Trade and Merchandise Act, 1958 (India)

BOOKS AND ARTICLES REFERRED

1. Narayanan, P. (2004). Law of Trade Marks and Passing off (6th ed.). Kolkata: Eastern Law House. p. 3. [ISBN 9788171772322](https://www.isbn-international.org/product/9788171772322).
2. MarcD.Wielansky, Internationalized Domain Names (2001), <http://www.jstor.org/stable/40012207>.
3. BromheadJohnson, "Domainnames", [http://www.intellectualproperty.co.uk/pages/domain names](http://www.intellectualproperty.co.uk/pages/domain%20names).
4. Lilian Edwards and Charlotte Waelde (2009) Law and the internet (3rd ed) Hart publishing.
5. Andre F.Rush , "Internet Domain Name Protection: A Canadian Perspective"(1996).
6. Ramzi Madi, "The Conflict between Country Code Top Level Domains and Trademarks: A brief overview of the Jordanian nationals solution", Arab law quarterly (2006). <http://www.jstor.org/stable/27650565>.
7. Marshall Leaffer, "Domain names, Globalization, and Internet Governance", Indiana University press (1998). <http://www.jstor.org/stable/20644692>. Last retrieved: 10th January 2014.
8. "Internet Corporation for Assigned Names and Numbers (ICANN): Rules For Uniform Domain Name Dispute Resolution Policy, American Society of International Law. <http://www.jstor.org/stable/20694028>.

9. Alexander Gigante, "Black hole in Cyberspace: The Legal Void in the Internet", 15 J. Marshall J. Computer & Info. L. 413 (1997).
10. Patrick Gunning, "Trademarks and domain names", Cyberspace Law Resources (2000).
11. Monica Kilian, "Cybersquatting and trademark infringement", Murdoch University Electronic Journal Of law (2000).
12. Eddie Hurter, "The international domain name classification debate: are domain names 'virtual property', intellectual property, property, or not property at all?", vol 42(2009), Institute of foreign and comparative law. P.296 .<http://www.jstor.org/stable/23253104>.
13. Christopher J Schulte, "the new anticybersquatting law and uniform dispute resolution policy for domain names", American Bar Association (2000). <http://www.jstor.org/stable/25763488> .
14. Sally M. Abel, "Trademark issues in Cyberspace: The Brave New Frontier"(1999). <http://www.mttr.org/volfive/abel.html>.
15. D. Mercer, "Cybersquatting: blackmail on the information superhighway.
16. Christopher P. Rains, "A domain name by any other name: forging international solutions for the governance of internet domain names", Emory International law review(2000).
17. Melissa Kossler, "Cybersquatting"(2005). <http://faculty.ist.psu.edu/bagby/Fall05/346F05T8/history.htm>.
18. Kelly M. Slavitt, "Protecting Your Intellectual Property from Domain Name Typosquatters" (2004).
19. Peter B. Maggs, "The ".us" Internet Domain", American society of comparative law, vol 50 (2002). <http://www.jstor.org/stable/840880>.
20. William R. Luney, "Trademarks: Extraterritorial Application of the Lanham Act", The Michigan Law Review Association, vol 55(1957). <http://www.jstor.org/stable/128595>.
21. Carl E. Simon, "Trademarks and Trade names: unclean hands as a defense in suit for infringement", California Law Review, vol 34. <http://www.jstor.org/stable/3477566>.

22. Richard A. Spinello, "Online Brands and Trademark Conflicts: A Hegelian Perspective", *Business Ethics Quarterly* vol 16 (2006). <http://www.jstor.org/stable/3857920>.
23. Sanjay Bhatia, "Domain names, cyber-squatting and Trademarks in India- A Legal Perspective," at <http://law.indiainfo.com/cyberlaw/10-5-2000.html>. Last retrieved: 10th February 2014.
24. Michael G. Walsh, "Marketer's Boon in Cyberspace: the Anti- cybersquatting consumer protection Act", *American Marketing Association* vol22 (2003). <http://www.jstor.org/stable/30000845>.
25. Diane Cabell, "Overview of Domain Name Policy", Harvard Law School (2003). <http://cyber.law.harvard.edu/udrp/library.html> .
26. Kevin Eng, "Breaking Through the Looking Glass: An Analysis of Trademark Rights in Domain Names Across Top Level Domains" (2000).
27. Bruce A. McDonald, "International Intellectual Property Rights", *American Bar Association* vol 35(2001). <http://www.jstor.org/stable/40707887>.
28. Paul Godfred and Kristine Dorrain, "Survey of the Law of Cyberspace", *American Bar Association* vol 65(2009). <http://www.jstor.org/stable/40688586>.
29. Peter B. Maggs, "The ".us" Internet Domain", *American Society of Comparative Law* vol 50(2002). <http://www.jstor.org/stable/840880>.
30. Lisa M. Sharrock, "The Future of Domain Name Dispute Resolution", *Duke University School of Law*, vol 51(2001) <http://www.jstor.org/stable/1373211>.
31. Natalma M. Mcknew, "Post Domain Infringement: in search of remedy", *American Bar Association* (2010). <http://www.jstor.org/stable/23297558>.
32. Shuli L. Green, "Launching Trademark Law into Cyberspace", *American Bar Association* (1997), <http://www.jstor.org/stable/40709886>.
33. Marilyn C. Maloney, "Intellectual Property in Cyberspace", *American Bar Association* (1997). <http://www.jstor.org/stable/40687783>.
34. Matthew Coleman, "Domain Name Piracy and Privacy: Do Federal Elections Regulation Offer A Solution?" *Yale Law and Policy Review* (2000). <http://www.jstor.org/stable/40239564>.
35. James T. Caeshu, "Trademark and the Free Ride Doctrine", *Stanford Law review* (1994). <http://www.jstor.org/stable/1227074>.

36. Aoki, Keith, "Intellectual Property and Sovereignty: Notes towards a Cultural Geography of Authorship", Stanford Law review (1996). <http://www.jstor.org/stable/1229388> .
37. Burr, J. Beckwith, "Competition Policy and Intellectual Property in the Information Age", Villanova Law Review (1996).
38. Fisher William, "Property and Contract on the Internet", Chicago Kent Law Review (1998).<http://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/11> .
39. Lemley, Mark & Volokh, Eugene, "Freedom of Speech and Injunctions in Intellectual Property Cases" Duke Law Journal (1998).
40. Lessig, Lawrence, "Intellectual Property and Code", Basic Books.ISBN 0-465-03912-X.
41. Volokh, Eugene, "Sovereign Immunity and Intellectual Property", Southern California Law review (2000). <http://dx.doi.org/10.2139/ssrn.220130>.
42. Froomkin, A. Michael, "Wrong Turn In Cyberspace: Using ICANN To Route Around The APA And The Constitution", Duke Law Review (2000). <http://personal.law.miami.edu/~froomkin/articles/icann.pdf>.
43. <http://www.icann.org>.
44. http://www.nolo.com/encyclopedia/articles/ilaw/dn_trdmk.html.
45. <http://domain-names.org>.
46. <http://www.icann.org/udrp.html>.

CASES REFERRED

1. Yahoo Inc v. Akash Arora 1999(2)AD(Delhi)229
2. *Aqua Minerals Ltd v. Pramod Borse and Another* AIR 2001 Delhi 463, 93 (2001) DLT 203.
3. *Cardservice International Inc. v. McGee* 950 F. Supp. 737 (E.D. Va. 1997)
4. *Rediff Communication Ltd v. Cyberbooth and Another*1999 (3) All MR 164.
5. *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).
6. *Intermatic Incorporated v. Dennis Toeppen*, 947 F. Supp. 1227; 1996 U.S. Dist. LEXIS 14878.
7. *Yahoo, Inc. v. Akash Arora* 1999 PTC (19) 201
8. *Rediff Communication Ltd v. Cyberbooth and Another* 1999 (3) All MR 164

9. ***Manish Vij v. Indra Chugh* AIR 2002 Del 243**
10. *Tata Sons Ltd vs. Ramadasoft*90(2001)DLT659; 2001 PTC 432
11. *Sbicards.com vs Domain Active Property Ltd* 2005 (31) PTC 455
12. *Intel Corporation v. Anil Handa* 2006 (33) PTC 553
13. *Dr. Reddy's Laboratories Ltd. V. Manu Kosuri* 2001 PTC 859
14. *Satyam Infoway Ltd vs Sifynet Solutions Pvt Ltd* AIR 2004 SC 3540
15. *OBH Inc v. Spotlight Magazine* 86 F. Supp. 2d 176 (W.D.N.Y. 2000)
16. *Planned Parenthood Federation of America. v. Bucci* 42 U.S.P.Q.2d 1430 (S.D. NY, 3/19/97)
17. *Comp Examiner Agency, Inc. v. Juris, Inc* 96-0213-WMB (Ctx), 1996 WL 376600 (C.D. Cal. May 22, 1996)
18. *Green Prods. Co .v. Independence Corn By-Prods. Co.* 992 F.Supp.1070 (N.D. Iowa Sept. 25, 1997)
19. *Vanity Fair Mills v. T. Eaton Co* (2d Cir. 1956) 234 F. (2d) 633, cert. den. 352 U.S. 871 (1956).
20. *Sporty's Farm LLC v. Sportsman's Market Inc* 202 F. 3d 489 (2d Cir. Feb. 2, 2000)
21. *Interstellar Starship Services Ltd. v. Epix, Inc.* (983 F.Supp. 1331, 45 USPQ2d 1304, D.Ore. 1997)
22. *Hasbro v. Clue Computing* 994 F. Supp 34 (D. Mass. 1997).
23. *Christian Dior v. Net power, Inc* WIPO Case No. D2000-0022 (Mar. 9, 2000).
24. *Credit Mgmt. Solutions, Inc. v. Collex Resource Mgmt* WIPO Case No. D2000-0029 (Mar. 17, 2000).
25. *Mondich v. Brown* WIPO Case No. D00-0004 (Feb. 16, 2000).

ABHIDHVAJ LAW JOURNAL