DOMAIN NAME DISPUTE IN THE AGE OF SOCIAL MEDIA AND E-COMMERCE

Jaivardhan Singh, Dr Bhim Rao Ambedkar National Law University, Sonepat

ABSTRACT

In the digital era, domain names are vital for businesses to establish their online identity, functioning similarly to trademarks in the physical world. This article examines the legal framework for domain name disputes, focusing on the intersection of domain names and trademarks under the Trade Marks Act, 1999, and the Uniform Domain-Name Dispute-Resolution Policy (UDRP) by ICANN. It explores common disputes such as cybersquatting, typosquatting, cyber twins, and reverse domain name hijacking, emphasizing their impact on businesses and consumers. Traditional legal systems face challenges like jurisdictional issues, slow resolution, and high costs, making the UDRP a preferred alternative for its speed and affordability. However, the UDRP is criticized for bias towards trademark holders, inconsistent decisions, lack of transparency, and no appeal mechanism. The article concludes with recommendations to improve the UDRP, including clearer definitions, expanded scope, an appeal process, and greater transparency. Addressing these issues will ensure fair and effective resolution of domain name disputes, protecting online business identities in an evolving digital landscape.

Introduction

In the present world, where businesses, companies and organisations want to make a name for themselves on the internet, the question arises: how do the consumers or the traffic identify one business from another? The answer is through a domain name. A domain name is a mark of distinctiveness, just like a physical logo of a brand. Through the domain name, people on the internet identify a particular business from millions of others. And since the domain name acts as a brand's reputation in the virtual world, it is highly likely to be duplicated or misrepresented. Therefore, the need arises to protect the distinct identity of these businesses, i.e., the protection of domain names. In this article, we shall go through the legal provisions, relevant sections and case laws in relation to preserving the domain name and discuss the interconnectedness of trademark and domain name as an instrument of business identifier.

Domain Name & Trademark – A relation

According to Section 2(1) (zb) of the Trade Marks Act, 1999, a 'Trademark' means a mark that is capable of being represented graphically and capable of distinguishing the goods or services of one person from those of others and may include the shape of goods or their packaging and combinations of colours[1].

On the other hand, a domain name, though not defined legally, refers to a distinct string of characters that makes up a unique address on the web[2]. Trademarks and business names are frequently the same or similar to domain names.

The Supreme Court in *Satyam Infoway Ltd. V. Sifynet Solutions Pvt. Ltd.*[3] held that domain names are subject to the restrictive framework that's applied to trademarks beneath the Trademark Act, 1999.

To sum it all up and clear all confusion, the term Trademark is described as any mark used in terms of trade. It is used to distinguish one business or product from another, just like a domain name is used to determine a brand or business over the internet. Thus, it can be concluded that a Domain name is an extended version of a Trademark.

[1] Essensee Obhan and Taarika Pillai, Trademark Comparative Guide, MONDAQ (April 23, 2024), Trademarks Comparative Guide - - India
[2] Domain Name and Trademark Conflicts, NIBUSINESSINFO.CO.UK, Relationship between trade mark and domain name | nibusinessinfo.co.uk
[3] Satyam Infoway Ltd. v. Siffynet Solutions (P) Ltd., (2004) 6 SCC 145 (India).

Law governing Domain Name disputes

Before discussing domain name disputes and their legal implications, we need to understand under what realm these disputes fall, i.e., what law applies to these domain name infringements. Due to a domain name's similar characteristics to a trademark and the fact that there is no exclusive law for domain names, disputes related to domain names also come under the purview of the Trademark Act 1999.

Now, for a domain to be registered successfully, it has to pass the same test as a trademark needs to pass, which is mentioned in Section 9 (majorly known as a test for distinctiveness or similarity) and Section 11 (known as a test for deceptiveness or confusion)[4] of the Trademark Act 1999. Thus, it now becomes clear that an action for a domain name infringement is brought under the Trademark Law.

On an international level, domain names are protected by the International Cooperation for Assigned Names and Numbers (hereinafter referred to as 'ICANN'). ICANN is a private, non-profit corporation responsible for International Protocol address space allocation, protocol parameter assignment, domain name system management, and root server system management functions[5]. In 1999, ICANN established the Uniform Domain Resolution Policy (hereinafter referred to as 'UDRP') to settle domain name disputes. We will discuss more about ICANN and UDRP in the coming parts of this article; for now, we need to understand what are the types and how domain name infringements crop up.

Nature of Disputes

Domain name disputes are of varied natures, extending from a business using a similar domain name address in good faith and in which a complainant has a legitimate interest in registering a domain name that resembles a well-known organisation with mala fide reasons. Some disputes of domain name infringements are given below.

i. Cybersquatting

Another name for cybersquatting is domain squatting. Cybersquatting is the act of someone registering a domain name that is similar to a well-known company without permission in order to make money. Domain registrants purchase domain names with the goal of damaging the company's reputation and goodwill. Selling the domain name

[4] Trademark Act, 1999, §9, §11.
[5] Peter Loshin, ICANN (Internet Corporation for Assigned Names and Number), TECHTARGET (Nov. 2021), What is ICANN (Internet Corporation for Assigned Names and Numbers)? - Definition from WhatIs.com

to the original trademark or service owner is primarily done in order to make a profit. Occasionally, someone will register a name with the expectation of selling it to the highest bidder at a later time. An initial case in India that dealt with cybersquatting was *Yahoo Inc v. Akash Arora*[6], where Yahoo Inc. filed a suit for injunction against Akash Arora, who registered a similar trademark of Yahoo Inc. as "Yahoo.com". The High Court decided in favour of the plaintiff, restraining the defendant from using "Yahoo!" as the defendant's domain was deceptively similar and confused the consumers in spite of adding the word "India" in its domain name.

ii. Typosquatting

A typo squatter is someone who registers a domain name with common typos of the company's primary domain name to divert the traffic from the main website to its website. For Example – A typo squatter registers a similar domain name, cscglobl.com to divert traffic from the original address of the website as cscglobal.com. Thus, taking advantage of common typing errors people make while entering any URL. As we are already familiar with domain names being the goodwill of a business on the internet, these duplicate and fuzzy domain names of the original domains create confusion in the minds of the consumer, which in turn depreciates the goodwill of the business, leading to losses.

iii. Cyber Twin

Cyber twins are those who possess two domain names and are legitimately entitled to them. In *Indian Farmers Fertilisers Cooperation Ltd v. International Foodstuffs Co*[7], the defendant in a lawsuit before the WIPO arbitration center had registered and was making good-faith use of his lawful domain name. Additionally, the plaintiff possessed a legitimate interest in the defendant's domain name. The Arbitration Center dismissed the claims brought against the defendant in this case for directing traffic. Due to the plaintiff's inability to establish malicious intent, the complaint was dismissed, and it was decided that both parties had a rightful claim to the domain name.

iv. Reverse Domain Name Hijacking

The act of a trademark holder attempting, in bad faith, to seize ownership of a domain

[6] Yahoo!, Inc. v. Akash Arora, 1999 SCC OnLine Del 133 (India)
[7] Indian Farmer Fertilisers Cooperation Ltd v. International Foodstuffs Co., Case No. D2001-1110, WIPO Decision at ¶ 7 (Jan. 4, 2002, WIPO).

> name from another party with a rightful interest in it is known as reverse domain name hijacking or RDNH. Rule 15e of the UNDRP states that if the panel finds that the complaint was brought in bad faith, for example, in an attempt at Reverse Domain Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and thus, constituting an abuse of the administrative proceeding[8].

As we are already familiar with domain names being the goodwill of a business on the internet, these duplicate and fuzzy domain names of the original create confusion in the minds of the consumer, which in turn depreciates the goodwill of the business, leading to losses both monetary and to the reputation.

Resolving Domain Name Disputes – Analysis

Just like traditional trademark disputes, the courts and judges do have the right to grant control and ownership of domain names, but in the case of domain name disputes as well but the traditional legal system is slow and is often unsuitable for resolving domain name disputes due to the reasons mentioned below:

- *Jurisdictional Challenges*: Firstly, the internet is global, and domain name disputes involve parties from varied countries; determining which court has jurisdiction over the domain name disputes can be challenging because traditional courts usually operate inside predetermined geographic bounds.
- *Speed of Resolution*: Secondly, conventional legal proceedings can be time-consuming and take months or even years to complete. A speedier response is required in the fast-paced online environment, and where domain names can greatly affect the business in terms of both economics and reputation, a speedy system of resolution becomes essential.
- *Cost of Litigation:* The traditional cost of litigation can be costly due to the associated lawyer fees, court costs and other expenses, and this high cost of resolving the dispute may be too expensive for many parties, particularly smaller companies and individuals, making them hesitant to pursue domain name disputes in traditional courts.

Due to the above and other similar challenges, ICANN was established in 1998 to supervise domain name management and create guidelines for dispute resolution. Initially, the core task

[8] Rules for Uniform Domain Name Dispute Resolution Policy, 2024, Rule 15(e).

assigned to it was the use of trademarks as domain names without the trademark owner's consent. Later, in 1999, ICANN introduced the UNDRP, laying out the procedures and other requirements for settling domain name disputes and making it mandatory for all registrars to follow the UNDRP policy.

The UDRP procedure is applicable for companies and individuals globally to file domain name complaints, mostly for generic top-level domains (gTLD) and top-level domains (TLDs) such as '.com', '.net', '.edu', '.gov' etc. It may also be applied for disputes related to a country code top-level domain (ccTLD) if the ccTLD registration authority has voluntarily adopted the UDRP policy. To file a complaint, the UDRP, according to Paragraph 4(a) prescribes that a complaint must involve three mandatory elements[9]:

- How is the domain name identical and confusingly similar to a trademark or service mark in which the complainant has rights?
- Why does the respondent have no rights or legitimate interest in the domain name?
- How the domain has been registered and is being used in bad faith?

It is mandatory that each of these three elements are present to initiate the administrative proceedings. The next step is the appointment by the chosen dispute resolution service provider of an administrative panel of one or three persons who will decide the dispute. After the appointment, the panel issues its decision and notifies the relevant parties. The decision is then implemented by the registrar(s) concerned should there be a decision that the domain name(s) in question be cancelled or transferred. This procedure is typically completed within 60 days of the WIPO Centre receiving the Complaint, making the UDRP's administrative procedure more favourable than traditional legal proceedings.

Issue of Vague Terms – 'bad faith'

The UDRP was created to establish a uniform or standard means of administering domain name conflicts however, the key terms are sometimes vague and unfamiliar. As a result, domain name registrants are still unsure about the interpretation of these terms after thousands of decisions.

For example, Paragraph4(b)(iv) of the UDRP says that bad faith arises when a registrant uses a domain name "for commercial gain… by creating a likelihood of confusion,", Paragraph

[9] Uniform Domain Name Dispute Resolution Policy, 2024, Rule 4a

4(b)(i) of UDRP mentions that bad faith arises when a registrant's primary purpose in registering the domain name is to sell it for "valuable consideration in excess of its documented out-of-pocket costs," even after several decisions and interpretation of the term 'bad faith' still it is open to more than one interpretation so as to what type of use would constitute 'bad faith'. Parties often rely on the ambiguities of the guidelines to assert their respective arguments. Even if the meaning of the term 'bad faith' is vague, the complainant still needs to show that the respondent acted in 'bad faith', then only an action can be taken by the concerned authority. It has been held in *Hemlock Farms Community Association v. Emma Djiya*[10] that good faith acquisition negates bad faith. In the above-mentioned case, the Complainant was unable to show that the Respondent had acted in bad faith and on the fact it was clear before the court that the Respondent had, in good faith, purchased the domains when it purchased the estate agency. In another case, *Telstra Corporation Limited v. Nuclear Marshmallows*[11], it was concluded by the panel that in some circumstances, registration alone could be sufficient to establish ill faith even in the absence of any further overt act.

Thus, it can be concluded that the meaning of the term 'bad faith' varies from one case to another, creating a vacuum in relation to the interpretation of the above term.

Shortcomings of UDRP

UDRP acts as a mechanism through which domain name disputes are resolved by way of out-of-court proceedings and can be implemented across international boundaries. While it has been praised for its efficiency and accessibility, it is not without shortcomings and criticism. The UDRP has certain flaws in its present form, and it can be demarcated as follows:

- *Perceived Bias Towards Trademark Holders*

  The UDRP often benefits trademark owners (complainants) over the domain name registrants (respondents). Critics often argue that the policy was designed with the interest of the trademark owners in mind at the expense of legitimate domain name holders in mind. This bias often leads to trademark holders using the UDRP to engage in reverse domain name hijacking, attempting to seize domain names from rightful owners without a lawful claim.

[10] Hemlock Farms Community Association v. Emma Djiya, Case No. D2023-1347, WIPO Decision at ¶ 7 (June 26, 2023, WIPO).
[11] Telstra Corporation Limited v. Nuclear Marshmallows, Case No. D2000-0003, WIPO Decision at ¶ 8 (Feb. 18, 2000, WIPO).

- *Lack of Transparency and Inconsistency in decisions*

  One of the significant criticisms that UDRP faces is the inconsistency of the decisions made by the panels in cases having similar facts, leading to a lack of predictability in the outcomes. Decision-making under UDRP is often criticised for being opaque, as the panellists are not required to explain their reasoning in detail, which makes it difficult for the parties to understand the reasoning behind the decision.

- *Limits of UDRP in certain disputes*

  There have been instances where the cases have been denied because they are outside the scope of UDRP, as it is difficult to draw a line between a trademark/commercial dispute and a domain name dispute. A recent example is the M31 case (WIPO Case D2021 – 2297). The complainant has pre-existing trademark rights and submitted evidence of the respondent using the contended domain name for a similar service, as well as a similar colour scheme.[12] The above case was denied by the majority of panellists, giving the reasoning that the dispute "exceeds the relatively limited 'cybersquatting' scope of the Policy and would be more appropriately addressed by a court of competent jurisdiction.

- *Lack of an Appeal Process*

  UDRP does not provide any mechanism for a formal appeal process. Once the panellists take a decision, the only recourse for the losing party is to file a lawsuit in a national court, which is costly and time-consuming. It, thus, creates concerns about accountability and the quality of decisions.

- *Potential for Abuse*

  Some complainants may file UDRP cases diplomatically to pressure domain name owners into surrendering valuable domain names. This, in turn, becomes a form of legal bullying, exploiting the lower cost and quicker resolution time of UDRP proceedings compared to traditional litigation.

Thus, it can be deducted from the above criticisms or shortcomings that UDRP, while being a valuable tool for resolving domain name disputes, suffers from several shortcomings that can hamper its reputation and put questions on its fairness and effectiveness. The above-mentioned

[12] James Taylor, The limits of the UDRP in trademark and commercial disputes, WTR (July 21, 2022), The limits of the UDRP in trademark and commercial disputes - WTR

shortcomings must be addressed by improving transparency, ensuring greater consistency in decisions, and further introducing an appeal process that could enhance the UDRP's ability to serve all parties in the dispute**.**

Conclusion and Suggestions

Although, the UDRP has certain shortcomings but in this ever-evolving digital landscape, where most businesses rely on the internet to establish their presence and identity, the protection of domain names has become an important task and thus, UDRP is the only rapid and economical recourse which the parties have, to settle the domain name dispute.

The following suggestion may be considered:

- Providing more precise definitions and examples for terms such as bad faith and legitimate interest.
- Provide guideline for refusal of cases and scope of UDRP must be re-evaluated so it can include more complex matters.
- An Appeal Mechanism must be formulated to address concerns about the lack of recourse for the losing party.
- And lastly the panellists should be required to provide detailed reasoning for their decisions to enhance transparency and consistency.

By addressing the identified shortcomings, UDRP and other related frameworks can evolve to better serve the needs of all stakeholders in the digital marketplace, ensuring that domain names remain secure, distinctive, and fair representations of online business identities.