UNRAVELING THE DIGITAL DECEPTION: A COMPARATIVE STUDY OF THE LEGAL RESPONSE TO CYBERSQUATTING IN SRI LANKA

Mahamalage Lourdith Ashinika Perera[#]

ABSTRACT

With the rapid evolution of the digital landscape, domain names have become a valuable corporate asset that reflect the personality of the business. The “first come, first served” basis inherent to the registration process of a domain name provides the opportunity for any individual to register a domain name, similar or identical to a trademark, and acquire rights over its original owner. The term “cybersquatting” refers to any such act carried out by any party with a mala fide intent, such as to earn profits off the goodwill. The trademark laws in several jurisdictions have been revised to address the burgeoning challenges of cybersquatting in the digital realm. This study aims to evaluate the effectiveness of the existing legal framework in Sri Lanka to address cybersquatting, with special reference to the relevant legal frameworks of the UK, USA, and India. This study engages in a comparative analysis of the legal frameworks in the aforementioned jurisdictions and assesses their strengths and weaknesses in order to propose recommendations for improving protection against cybersquatting in Sri Lanka. Furthermore, the study explores the international alternate dispute resolution mechanisms along with national alternate dispute resolution mechanisms implemented by the above jurisdictions to address domain disputes alongside the traditional litigation route. Findings from this study reveal that Sri Lanka, being new to the emerging challenge of cybersquatting, can effectively address it by implementing the existing legal framework and making advancements in the Sri Lankan domain name operator's dispute resolution

[#] CIMA Dip MA, LLB (Hons) (Colombo), Attorney-at-Law (Received 06th Apr 2024, Revised 21st Jun 2024, Accepted 27th Jun 2024).

policy. The researcher employs qualitative research methodology, drawing on primary sources such as international policies, domestic laws, and case law. Secondary sources, such as books and journal articles, are also utilized for further insights.

Keywords: Trademark, Cyber-squatting, Top level domain (TLD), Passing-off, Dilution

1. INTRODUCTION

With the rapid growth of e-commerce in the digital environment, it is imperative for a business to maintain an online presence to gain market share and remain competitive. Therefore, the identity of a business is significantly dependent on its unique domain name. The Court in *Card-service Int'l v McGee* observed that "A customer who is unsure about a company's domain name will often guess that the domain name is also the company's name".[1] Thus, in the modern era of technological advancement, a domain name is a marketing tool that mirrors the trademark and goodwill of a business, product, or service.[2] Nevertheless, given that the domain registration process operates on a first come first served basis, any individual may secure a domain name provided that they are the first to do so. Hence, individuals may partake in the unethical practice of manipulating the domain name registration process by

1 *Cardservice Intern., Inc. v. McGee,* 950 F. Supp. 737 (E.D. Va. 1997).

2 In *Rediff communication* v *Cyberbooth Rediff Communications LTD, v Cyberbooth* (AIR 2000 Bom 27) Court held that, "the Internet domain names are of importance and can be a valuable corporate asset. A domain name is more than an Internet address and is entitled to the equal protection as trade mark. With the advancement and progress in the technology, the services rendered in the Internet site have also come to be recognised 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.", Similar views can be found in *Tata Sons Ltd v. Monu Kasuri & others* 2001 PTC 432.

registering domain names that bear resemblance to established trademarks, with the intention of profiting from their subsequent sale. This practice is commonly recognized as cybersquatting. The emergence of cybersquatting has led to significant trademark implications, prompting various jurisdictions to amend existing laws and introduce new legislation to address this challenge. Sri Lanka, being new to the challenges of domain disputes, doesn't explicitly address this rising challenge of cybersquatting through existing laws. Therefore, the research problem of the present study will be to evaluate the effectiveness of the existing legal framework in Sri Lanka related to cybersquatting to address the In answering the research problem, a special reference will be drawn to the legal framework pertaining to cybersquatting in the UK, USA, and India, whilst evaluating the alternative dispute resolution mechanisms implemented by global entities and the relevant jurisdictions.

This study comprises 7 Parts, where Part 2 presents the methodology employed and Part 3 engages in a conceptual analysis related to domain names and the concept of cybersquatting. Part 4 explores the international policies related to addressing trademark disputes stemming from cybersquatting, whereas Part 5 entails a comparative analysis of the legal framework and the remedies offered by the above four jurisdictions. Based on insights drawn from other jurisdictions, Part 6 provides suggestions to enhance the protection against cybersquatting in Sri Lanka. Finally, Part 7 concludes the study with an overview of the research.

2. METHODOLOGY

This study adopts qualitative research methodology to assess the legal framework in Sri Lanka pertaining to cybersquatting in comparison with

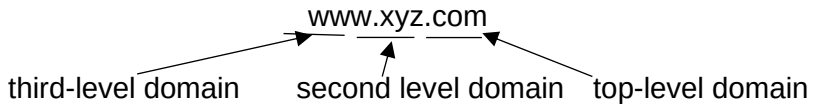
the jurisdictions of the UK, USA, and India. The researcher employs primary sources such as international policies, legislative enactments, and case laws of the UK, USA, India, and Sri Lanka, along with decisions from the WIPO Arbitration and Mediation Centre. Secondary sources, such as websites, books, and journal articles, are also utilized to gain further insights.

3. CONCEPTUAL ANALYSIS

3.1. Domain Name

A domain name is simply the unique name of a website that allows access to the website of an organisation. The primary purpose behind the creation of internet domain names was to locate a website using a user-friendly, and an easy-to-remember address.[3] Similar to a physical address, this alphanumeric address locates a specific computer within the internet network. Due to the rapid increase in commercial transactions conducted online and, the resulting constraints on domain names, they have become crucial identifiers for both businesses and individuals. This has led internet users to perceive domain names as crucial “intellectual property”.

Domain name is based upon a hierarchical structure that consists of a top-level domain (TLD), second-level domain and third-level domain as follows.



[3] Torsten Bettinger and Allegra Waddell, *Domain Name Law and Practice an International Handbook* (2nd edn, Oxford Academic,2015).

Furthermore, domain names can be classified into 2 types as, “Generic Top-Level Domains” (hereinafter known as gTLDs) and “Country Code Top Level Domains” (hereinafter known as ccTLDs).[4] gTLDs are used by companies that intend to achieve a global presence (. com/.org), whereas ccTLDs represented by two denominator characters are country-based. (.in). ICANN is the organisation that coordinates and manages in relation to the Generic Top-Level Domains while registrar services carried out by different countries perform registration services related to Country Code Top Level Domains.[5]

In the recent past, there has been a growth of several types of domain disputes all over the world, among which, cyber-squatting has become one of the major threats posing to trademark rights and cyber security.

3.2. Cyber Squatting

Cybersquatting is an emerging unethical practice, wherein an entity deliberately registers a domain name that closely resembles or is identical to another party's trademark, with the intention of acting in bad faith.

The United States Ninth Circuit, in a case involving the ACPA, has determined that “*Cybersquatting is the Internet version of a land grab. Cybersquatters register well-known brand names as Internet domain names in order to force the rightful owners of the marks to pay for the right to engage in electronic commerce (e-commerce) under their own name*”.[6]

---

4 Harman Preet Singh, 'Cyber Squatting and the Role of Indian Courts : A Review' (2022) 2 Amity Journal of Computational Sciences (AJCS).

5 Justice Mellor and others, *Kerly’s Law of Trade Marks and Trade Names* (Sweet & Maxwell 2011) 859.

6 *Interstellar Starship Services, Ltd. v Epix, Inc*., 304 F 3d 936, 946 (9th Cir, 2002).

Accordingly, this scenario could be compared to an act of land grab, where an outsider may squat a piece of land belonging to someone else.

Indian courts in Manish Vij v. Indra Chugh defined cybersquatting as an act of "obtaining fraudulent registration with an intent to sell the domain name to the lawful owner of the name at premium".[7]

Therefore, if a person with no inherent right or an identical trademark registration acquires illegal profits by registering a domain of another legitimate user, it would be defined as cybersquatting.

One of the detailed definitions for cybersquatting can be found in the Anticybersquatting Consumer Protection Act ("ACPA") which defines cybersquatting as the

> "registration, trafficking in, or use of a domain name similar to a trademark or service mark of another that is distinctive at the time of registration of the domain name, or dilutive of a famous trademark or service mark of another that is famous at the time of the registration of the domain name, without regard to the goods or services of the parties, with the bad-faith intent to profit from the goodwill of another's mark.[8]

At present, cybersquatting has taken different shapes in the digital domain, which includes classic cybersquatting, typo squatting, identity theft, name-jacking, reverse-cybersquatting, and many other methods. Typo squatting, is the act of including intentional typographical errors to mislead internet users to visit the website.[9] In identity theft, the squatter

---

7 *Manish Vij And Ors.* vs *Indra Chugh and Ors.* (AIR 2002 Delhi 243).

8 Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d).

9 David Lindsay, *International Domain Name Law ICANN and the UDRP* (Hart Publishing 2007) 259.

registers the domain name when the original domain owners fail to regularly; renew the registration; as a result, the customer gets misled by the impersonation of the squatter.[10] Meanwhile, name-jacking involves registering the name of a person, especially that of a celebrity, to earn benefits such as web traffic.[11] Furthermore, reverse cybersquatting is the act of pressuring or intimidating an original domain owner to transfer the domain to the squatter.[12]

Recently, the development of technology has allowed the registration of domain names with non-ASCII characters such as non-English languages, etc.[13] In addition, cybersquatting of social media accounts has been another recent trend in this crime, which is known as name-squatting. Therefore, the elimination of cybersquatting has become further complicated with evolving technology. However, several social media policies have included terms to protect users from name-squatting.[14] E.g.: 'Tony La Russa', the manager of the St. Louis Cardinal, instituted an action against Twitter for allowing the squatter to create an account in his

10 Sukrut Deo, Sapna Deo, 'Cybersquatting: Threat to Domain Name' (2019) International Journal of Innovative Technology and Exploring Engineering (IJITEE) 1432.

11 ibid.

12 ibid.

13 ibid.

14 **Facebook**-In case of an infringement of a registered trademark, Facebook allows the user to recover usernames. Reporting of such trademark infringement to Facebook has been allowed to the trademark owner by introducing a "username infringement form." Facebook further adopts a "mobile number authentication," procedure, through which the users must validate their account using their mobile device.

Twitter-Twitter's name squatting regulation prohibits cybersquatting and removes "username for sale" accounts.

Instagram-Instagram has adopted the "verified account," concept which distinguishes the original trademark owner with a blue tick in the owner's account.

name along with offensive tags.[15]

4. INTERNATIONAL REMEDIES

4.1. Arbitration proceedings under the Internet Corporation for Assigned Names and Numbers (hereinafter ICANN)

ICANN is a non-profit organisation that coordinates unique identifiers on the Internet, such as domain names, IP addresses, protocol ports, and parameter numbers.[16] ICANN has exclusive jurisdiction over the registration of generic top-level domains (gTLDs) and several country-code top-level domains (ccTLDs), which are facilitated through accredited registrars.

In order to address disputes arising from domain names and to facilitate their resolution in a cost-effective and efficient manner, ICANN has implemented a mechanism known as the Uniform Dispute Resolution Policy (UDRP).[17]

4.1.1. Uniform Dispute Resolution Policy (UDRP)

The Uniform Dispute Resolution Policy (UDRP) is a global arbitration system related to the Generic Top-Level Domains (gTLDs), which enables trademark owners to contest domain names that are identical or confusingly similar to their trademarks and have been registered and used

[15] Thomas J. Curtin, 'The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites' (2010) 19 J. L. & Pol'y https://brooklynworks.brooklaw.edu/jlp/vol19/iss1/13 accessed 20th March 2024.

[16] ICANN- Mission and Core Values, Art 1(1).

[17] S Deo, 'Cybersquatting: Threat to Domain Name' (2019) 8 International Journal of Innovative Technology and Exploring Engineering (IJITEE), 1432.

in bad faith.[18]

Paragraph 1 of the UDRP requires registrars to include mandatory terms in the registration agreement, which registrants must adhere to in the event of a dispute regarding a registered name.[19] As per Para 4 (a) of the UDRP, the complainant must fulfill 3 requirements that:

1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

2) the domain name holder has no rights or legitimate interests with respect to the domain name; and

3) the domain name has been registered and is being used in bad faith.[20]

The Domain Name Dispute Resolution Policy (UDRP) can be initiated by filing a complaint with any of the following dispute resolution service providers that have been approved by ICANN.[21]

1. The World Intellectual Property Organisation (WIPO)
2. The Forum (formerly known as the National Arbitration Forum)
3. The Czech Arbitration Court (CAC)
4. The Asian Domain Name Dispute Resolution Centre (ADNDRC)

---

18 Torsten Bettinger and Allegra Waddell, *Domain Name Law and Practice an International Handbook* (2nd edn, 2015) 1263.

19 UDRP (1999) para 1.

20 ibid 4(a).

21 ibid 4(d).

5. The Arab Center for Dispute Resolution (ACDR)
6. Canadian International Internet Dispute Resolution Centre (CIIDRC)

Paragraph 4(g) of the UDRP stipulates that the complainant must bear any fees imposed by their elected provider, unless the domain name holder (registrant) has opted for an expanded panel, in which case the fees will be split between both parties.[22] As per Para 4(i), the available remedies would be limited to canceling or transferring the domain name to the complainant. Paragraph 4(k) of the UDRP allows either party in the dispute to pursue court proceedings.

As opposed to international mechanisms, domestic mechanisms provide a variety of remedies beyond the transfer or cancellation of the domain name in disputes related to cybersquatting. Hence, this study will proceed to analyze the legal frameworks concerning cybersquatting in the United Kingdom, the United States of America, India, and Sri Lanka.

5. DOMESTIC LEGAL FRAMEWORK IN THE UK, USA, INDIA AND SRI LANKA

5.1. The UK

When dealing with the emerging issue of cyber-squatting, the UK has opted to address such issues using existing legal frameworks instead of seeking to introduce new statutes. In cases where a domain name may conflict with an existing trademark owner, the Court would not hesitate to address such issues by way of trademark law and the common law

[22] ibid 4(g).

principles of passing off.[23]

In the UK, a company called Nominet UK operates the Register Database for the .uk CCTLD, which also provides details of the domain name registrant and its registration agent.[24] The "Whois" service is an appealing feature introduced by Nominet for the public to look up the details of the registrant of a specific domain name.[25] This feature is beneficial, for instance, when an individual needs to contact the owner of a domain name upon discovering a potential trademark violation.

The most common dispute resolution methods for brand owners in cases of trademark infringement are alternative dispute resolution mechanisms, court action, or registrar takedowns.

5.1.1 Alternative dispute resolution mechanisms

One mechanism involves the Uniform Domain-Name Dispute-Resolution Policy (UDRP), which applies to all legacy gTLDs, all new gTLDs, and approximately 40 ccTLDs.[26] In addition, although not as widely applied as UDRP, the Uniform Rapid Suspension System (URS) covers several gTLDs.[27] EURid Alternative Dispute Resolution (ADR) is another mechanism that specifically applies to the .eu and. ею ccTLDs.[28] More importantly, the DNS operator of the country offers an independent dispute

---

23 Lionel Bently and Brad Sherman, *Intellectual Property Law* (4th edition, Oxford University Press 2014) 824.

24 Justice Mellor and others, *Kerly's Law of Trade Marks and Trade Names* (Sweet & Maxwell 2011) 870.

25 *British Telecommunications v. One in a Million* [1998] Ent L Rev 283.

26 Andrew Clemson, A Practical Guide to the Law of Domain Names and Cybersquatting (Law Brief Publishing, 2019).

27 info, .org, .pro, .cat, .jobs, .mobi, .pro, .travel etc.

28 Clemson (n 26).

resolution system called Nominet DRS (DRS) for resolving disputes related to .uk ccTLD. This feature can be identified as an attractive aspect of the DNS policy in the UK.

5.1.2 Court action

As previously mentioned, courts rely on existing trademark laws and common law principles of passing off rather than introducing new statutes when addressing the emerging issue of cybersquatting.

5.1.2.1. Trademark law

The Trademarks Act 1994 is the key statute that governs the registration, protection, and enforcement of trademarks in the UK. Particularly, Section 10 of the Trademarks Act deals with the infringement of registered trademarks. This section specifically requires that the infringer "uses in the course of trade" a sign that is similar or identical to the trademark owned by someone else. At first glance, this could pose a challenge concerning cybersquatting because the cyber squatter may not actively "use" the trademark rather 'stockpile' it, awaiting payment from the trademark owners.[29] Moreover, unlike a "sign" in trademark law, a domain name may not be used to distinguish between a product or service, and it is unlikely to cause confusion among consumers if it is warehoused after its registration, until released for a fee.[30] Nevertheless, the Courts, through their interpretation of the Trademarks Act, 1994, have managed to encompass cybersquatting within the purview of trademark infringement.

This can be observed in *British Telecommunications v. One in a Million*,

[29] *British Telecommunications* (n 25).

[30] J. Thomas McCarthy, 'Trademarks, Cybersquatters and Domain Names' (2016) Vol. 10, Iss. 2. DePaul Journal of Art, Technology & Intellectual Property Law (JATIP),231.

which was one of the early British cases that addressed the practice of "cyber-squatting".[31] The defendant, in this case, was a dealer in Internet domain names, who acquired registrations for several prestigious names like 'virgin.com' and 'tandy.com' with the purpose of subsequently selling them to their rightful owners at a higher price. The Court held that the defendants being domain name dealers, the use of trademarks within their business to inflate the value of domain names and obtain payment from the trademark owner, constituted, "use in the course of trade", as outlined in section 10(4) of the Trademarks Act. Therefore, the Court considered the defendant's almost future act of selling the domain name to a 3rd party to be an imminent threat to the plaintiffs' rights. The court further found that this has established the requirement of "likelihood of confusion".

Similarly, in *Tesco v. Elogicom***,** despite the defendants not using the domain names to redirect traffic to their own websites or to sell any goods or services of their own, the Court ruled that the unauthorised use of a trademark within a domain name could still constitute a service provided to the public.[32] Accordingly, the Court held that the mere registration of a domain name similar to an already registered trademark satisfies the criteria for trademark infringement under section 10(4) as it pertains to "use in the course of trade".

5.1.2.2. Passing off

In the *One in a Million* case, the Court further determined that the mere registration of a domain name could constitute passing off.[33] This is due to the false representation that could arise, suggesting that the domain

[31] *British Telecommunications* (n 25).

[32] *Tesco v. Elogicom* [2007] FSR (4).

[33] *Telecommunications Plc & Ors v One in a Million Ltd & Ors* [1998] EWCA Civ 1272.

registrant is associated with the brand owner. The Court further viewed such similar or identical Domain names containing well-known brands as "instruments of fraud" because any actual use of them as domains would inevitably lead to passing off.[34] One significant precedent set by the Court in this case was that the registration of a trademark belonging to someone else, with the aim of capitalising on its reputation could lead to a passing-off claim under common law.[35]

In *Vertical Leisure Limited v Poleplus Limited* [2014] EWHC 2077 (IPEC**),** the Court addressed conduct by the defendant in a manner similar to the previous case.[36] Although the Court did not find any trademark infringement, it acknowledged the passing off resulting from the defendant's action.

5.1.3 Registrar takedowns

In this method, the trademark owner may directly contact the registrar of the abusive domain and request its takedown without resorting to any judicial or quasi-judicial procedure. Upon discovering that the domain may violate any terms outlined in its registration agreement, the registrar has the discretion to remove the domain. However, such takedowns are typically reserved for the most severe cases and should not be employed for instances of "normal" cybersquatting or other actions that may constitute bad faith.[37]

---

34 ibid.

35 ibid.

36 *Vertical Leisure Limited v Poleplus Limited* [2014] EWHC 2077 (IPEC).

37 Clemson (n 26).

5.2 The USA

In the context of addressing trademark disputes in domain names, the USA offers both avenues of litigation and alternate dispute resolution methods to trademark owners. A notable aspect of the legal landscape in the USA involves the Anti-Cybersquatting Consumer Protection Act (ACPA), specially designed for addressing cybersquatting. In addition, the following alternate dispute resolution methods provide further remedies for victims of cybersquatting.

5.2.1 Alternative Dispute Resolution Methods

In relation to generic Top-Level Domains (TLDs), trademark owners can seek remedies through mechanisms like the Uniform Domain-Name Dispute-Resolution Policy (UDRP) and the Uniform Rapid Suspension System (URS). Neustar, with the approval of the Department of Commerce, has developed and implemented the usTLD Dispute Resolution Policy and Rules (usDRP), which is aligned with the UDRP, specifically for addressing disputes related to the usTLD.[38] The usDRP procedure is administered by approved dispute resolution providers, namely the American Arbitration Association (AAA) and the National Arbitration Forum (NAF).[39] This involves a procedure that is more informal than the litigation route and accepts claims of foreign trademark owners as well. Furthermore, the panel decisions would be binding upon the parties unless court action is commenced within 10 days.[40] When legal proceedings are initiated before or during a usDRP administrative

[38] Torsten Bettinger and Allegra Waddell, *Domain Name Law and Practice an International Handbook* (2nd edn, 2015) 1006.

[39] ibid, 1011.

[40] ibid, 1013.

proceeding, the usDRP Rules give sole discretion to the administrative panel to decide whether to suspend or terminate the administrative proceeding or proceed with a decision.[41] A trademark owner can use the above-mentioned alternative dispute mechanisms to seek remedies such as the cancellation or transfer of the abusive domain name.

5.2.2 Court Action

The USA has introduced a key piece of legislation named the Anti-cybersquatting Consumer Protection Act (ACPA), which is solely dedicated to cybersquatting.[42] In cases of trademark infringements related to cybersquatting, the ACPA establishes the right to sue a cybersquatter and to seek redress under the Lanham Act (the US trademark Act) as a trademark infringement. This has provided victims of cybersquatting with a range of remedies, including injunctions, damages, and attorney's fees, in addition to the traditional remedies of transferring or taking down the domain name.[43]

Before the existence of a distinct law for cybersquatting, the issue was tackled only through the Lanham Act, which was amended by the Federal Trademark Dilution Act of 1995.[44] The FTDA defines dilution as "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

41 ibid,1026.

42 Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d).

43 Thomas J. Curtin, "The Name Game: Cybersquatting and Trademark Infringement on Social Media Websites" (2010) 19 J. L. & Pol'y https://brooklynworks.brooklaw.edu/jlp/vol19/iss1/13 accessed on 20th March 2024.

44 Federal Trademark Dilution Act, 15 U.S.C. § 1127.

(2) the likelihood of confusion, mistake, or deception".[45] This established a federal cause of action for the dilution of famous marks, which can occur through either "tarnishment" or "blurring".[46] In the case of *Hasbro, Inc. v. Internet Entertainment Group, Ltd.,* an instance of dilution by tarnishment in cybersquatting emerged. The Court determined that the well-known trademark "Candyland", associated with a children's board game, was diluted by tarnishment, as the defendant had used "candyland.com" for a website displaying sexually explicit content.[47] In *Toys "R" Us, Inc. v. Akkaoui*, a case with similar facts, the Court likewise found that the defendant's cybersquatting resulted in dilution due to tarnishment.[48] Meanwhile, blurring arises when distinguishing a clear difference between entities becomes challenging.

In some cases, the Court has expanded its interpretation of dilution beyond blurring and tarnishment, especially where the cybersquatter does not use the reserved domain name as a trademark in public, distinguishing any goods or services or causing no confusion among the public. This was identified in the two landmark cases of *Intermatic v. Toeppen* and *Panavision v. Toeppen*, where the Court ruled that Toeppen's intention to hold the domain name ransom for financial gain constituted a "commercial use", sufficient to trigger the Dilution Act.[49] [50] The Court reasoned that it would discourage potential customers of Panavision, if they could not locate its website by typing "panavision.com", rather were forced to search

45 ibid.

46 Thomas (n 43).

47 *Hasbro, Inc v Internet Entertainment Group, Ltd* 40 U.S.P.Q. 2d 1479 (W.D. Wash. 1996).

48 *Toys "R" Us Inc. v. Akkaoui,* 40 U.S.P.Q.2d (BNA) 1836 (1996).

49 *Intermatic Inc. v. Toeppen,* 947 F. Supp. 1127 (ND Ill. 1996).

50 *Panavision International v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

across hundreds of websites. This dilutes the value of “Panavision”. Accordingly, “discouragement” becomes a new form of dilution which “stretched” the meaning of “commercial use” to catch cybersquatter. Hence the judicial interpretation has significantly broadened, leading to the recognition of cybersquatting in certain instances, even in the absence of any commercial use. In *Planned Parenthood Federation of America, Inc. v. Bucci***,** the defendant's intention was not to sell the domain name but to use it to express views opposing those of the plaintiff. Despite that, the court found the defendant liable for trademark infringement.[51] The above uncertainty regarding the scope of cybersquatting highlighted the need for a dedicated law concerning trademark claims in cybersquatting cases, which ultimately led to the enactment of the Anti-Cybersquatting Consumer Protection Act.

Nevertheless, even after the enactment of the Anti-Cybersquatting Consumer Protection Act (ACPA), there have been instances where courts recognised gripe sites that have no direct commercial use, as violating trademark rights. For example, in *Bosley Medical Institute v. Kremer*, the defendant (Kremer) registered a domain name that associated a trademark owned by a medical institute named Bosley. Subsequently, the defendant used the said domain name to share negative remarks about the trademark owner. The District Court dismissed the action, reasoning that the defendant’s act was noncommercial. The said decision was reversed by the Ninth Circuit Court of Appeals. The court held that,

> “The district court erred in applying the commercial use requirement to Bosley's ACPA claim. Rather, the court should

[51] *Planned Parenthood Federation of America, Inc. v. Bucci*, 42 U.S.P.Q. 2d 1430, 1441 (S.D.N.Y. 1997).

> confine its inquiry to the elements of the ACPA claim listed in the statute, particularly to whether Kremer had a bad faith intent to profit from his use of Bosley's mark in his site's domain name".[52]

This reflects the underlying intention of the judiciary to deter abusive domain names, by adopting a broader interpretation of trademark law.

5.3 India

Currently, India has not adopted any legal framework to address cybersquatting. Therefore, most cases related to cybersquatting have been dealt with under the Trademark Act, 1999, and the common law passing off. In addition, to traditional litigation, Indian law offers several alternate dispute mechanisms that provide quick and efficient remedies against cybersquatting.

5.3.1 Alternate Dispute Mechanisms

In India, disputes related to generic TLDs are resolved under international dispute resolutions such as Uniform Domain-Name Dispute-Resolution Policy (UDRP) and the Uniform Rapid Suspension System (URS). Meanwhile, the National Internet Exchange of India (NIXI) oversees disputes involving the .in top-level domain, through the Indian Domain Name Dispute Resolution Policy (INDRP).[53] This mechanism provides remedies for any domain violation related to the .in ccTLD, within 30

[52] *Bosley Medical Institute, Inc. v. Kremer,* 403 F.3d 672, 682 (9th Cir.2005).

[53] Nisha Dhanraj Dewani and others, Handbook of Research on Cyber Law, Data Protection, and Privacy (Hershey PA ,2022) 130.

days of filing a complaint.[54] The complainant must meet the requirements given in paragraph 4 of the INDRP, which align with the three UDRP requirements.[55] Arbitration proceedings will be conducted by an arbitrator appointed by the registry, in accordance with the Dispute Resolution Policy as well as the Arbitration and Conciliation Act of 1996 (ACA).[56] The registration agreement requires registrants to adhere to the INDRP. Therefore, if a registrant is found to have violated the agreement, the domain name may be cancelled or transferred to the rightful trademark owner. This policy further allows the registrar to freeze the domain name during a pending INDRP or court action.[57]

In *YouTube LLC v. Rohit Kohli*, the domain name www.youtube.in was held to be an infringement of trademark and directed to transfer the domain after payment to the registry.[58] Similarly, in *Vodafone Group Plc v. Rohit Bansal***,** the arbitrator found that the registration of the domain name "vodafone.co.in" had been done in bad faith and ordered the domain to be transferred to its rightful owner.[59]

5.3.2 Court Action

When pursuing litigation, most cases related to cybersquatting have been addressed under the Trademark Act, 1999, and the common law principle of passing off.

---

54 'Cybersquatting Laws in India' https://www.estartindia.com/knowledge-hub/blog/cybers quatting-laws-in-india accessed 25th March 2024.

55 S Mukharji, 'Passing Off;Internet Domain Names;Domain Name Disputes;Trademark Law;Infringement;Cyber Squatting' (2004) 13 Journal of Intellectual Property Rights.

56 The Arbitration and Conciliation Act, 1996 (26 of 1996).

57 Torsten Bettinger, Allegra Waddell *Domain Name Law and Practice An International Handbook* (2nd edn, 2015) 509.

58 *YouTube LLC v. Rohit Kohli* INDRP/42.

59 *Vodafone Group Plc v. Rohit Bansal* INDRP/052.

5.3.2.1. Trademark Law

As per Section 29 (5) of *the Indian Trade Marks Act, 1999,* using a registered trademark as a trade name, part of a trade name, or a business name, or part of the business name belonging to a business concerning goods and services would amount to an infringement of a trademark. The court in *Titan industries Ltd. vs Prashanth Kooraptti & Ors* widely interpreted the trademark protection afforded by the above provision for the 1st time.[60] It held that domain names are entitled to the same protection as a trademark, affirming the plaintiff's rightful claim. This approach was similarly followed in *Rediff Communication v. Cyberbooth*, when recognising the domain name as a trademark.[61]

Moreover, the Trademark Act has introduced several criminal sanctions related to trademark violations, which could be applicable in cases of cybersquatting. Sections 103 and 104 of the Trademark Act, 1999 penalize applying false trademarks or descriptions and selling goods or services that bear false trademarks or descriptions, respectively.

5.3.2.2. The law of passing off

The remedy of passing off is a remedy under the law of tort that prevents a person from misrepresenting that his goods or services are affiliated with another.[62] This remedy enforces unregistered trademark rights if several conditions exist, such as the reputation of the victim's trademark, misrepresentation by the infringer, and the injury or loss caused to the

[60] *Titan Industries Limited v. Prashanth Koorapati and others*, III AD Delhi 545, 90 (2001).

[61] *Rediff Communications LTD, v Cyberbooth* (AIR 2000 Bom 27).

[62] India has recognized "passing off" with the Delhi High Court decision in *N.R. Dongre vs. Whirlpool* Corporation where it was held that a company cannot sell its goods under the pretend as another company and sell goods.

victim's business. Further, to seek a remedy, prior domain registration is not required. The first case in India, *Yahoo Inc. V. Aakash Arora & Anr*., which dealt with cybersquatting, was given the remedies of passing off. The Court held that the defendant's action was "an effort to trade on the fame of Yahoo's trademark."[63] Similarly, the Court in *Satyam Infoway Ltd v. Sifynet* Solutions has dealt with cybersquatting issues under the law of passing off.[64]

In addition to trademark law, and passing off principles, some provisions in the Information Technology Act of 2000 and the Indian Penal Code of 1860 can be applied to address cybersquatting. Therefore, section 66 of the Information Technology Act of 1999 makes it an offense to commit any dishonest or fraudulent act described under Section 43, which is punishable by imprisonment for a maximum of 3 years, a fine of up to INR 400,000 or both.[65] [66] Further, Section 66A penalizes anyone who conveys "grossly offensive" or "menacing" material through a computer resource or a communication device. Meanwhile, Section 469 of the IPC stipulates that forgery is punishable with imprisonment of up to three years as well as a fine.[67]

---

63 *Yahoo! Inc. v. Akash Arora and another*, 1999 Arb. LR 620.

64 *Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd* 2004 (3) AWC 2366 SC.

65 Information Technology Act of 1999, s 43.

66 ibid, s 66.

67 A person found forging with the intent to harm the reputation of any party or knowing that the document forged will be used for that purpose, shall be punished with imprisonment of either description for a term that may extend to three years, as well as a fine.

5.4 Sri Lanka

In Sri Lanka, no specific legislation can be found in relation to cybersquatting. Except for a few unreported incidents, where owners of reputable trademarks in Sri Lanka had to reach settlements with the cybersquatter, not many cases were found that dealt with cybersquatting.

Nevertheless, it is pertinent to note that the existing legal framework concerning trademark law can be utilised to address potential cybersquatting issues that may arise in the future. The LK Domain Registry (LKNIC) is the independent organisation to register LK domains in Sri Lanka that coordinates and manages several agents who engage in the registration of certain domain names (open second-level domains).[68] This provides no independent dispute mechanism, yet a trademark owner whose rights are being affected or threatened by cybersquatting, may have several alternate dispute mechanisms to seek remedies in addition to the traditional litigation avenue.

5.4.1 Alternative Dispute Resolution Methods

In cybersquatting cases that involve generic top-level domains (gTLDs), trademark owners may have the remedies of getting the abusive domain name, cancelled or transferred in the case of success of the administrative proceedings. Numerous cases involving generic top-level domains have been resolved through the WIPO Arbitration and Mediation Centre, with one party being Sri Lankan.[69]

---

[68] Under the .lk cc TLD, there are two types of second-level domains: closed second-level domains managed directly by LKNIC, and open second-level domains managed by registered agents of LKNIC.

[69] *Tata Sons Pvt. Ltd. v. Victor TSB*, Case No. D2021-1084; *Accenture Global Services Limited v. Janaka De Silva,* Case No. D2020-0481; *Industrias Romi S.A. v. Renown SC,* Case No. D2001-1217; *Manchester City Football Club Limited v. Vincent Peeris,*

In relation to .lk ccTLDs, the Domain Name Dispute Resolution Policy of the LK Domain Registry may be relevant. Unlike in the UK, USA, and India, the LK Domain Registry has not introduced an independent dispute resolution mechanism. Apparently, LK Domain Registry has affirmed its non-liability for disputes between registrants and third parties. However, trademark owners can still pursue arbitration as an alternative to litigation. Further, it should be noted that, upon successful proof of trademark rights, the registrar may take down or transfer the abusive domain name.[70] Nevertheless, the registry does not provide a mechanism similar to the "whois" service in the UK, which could assist trademark owners in identifying potential cybersquatters for legal action.

It is pertinent to note that LKNIC lists several names that will not be registered in their registration policy, including trademarks of other parties and prohibited business names. Despite the said restriction, there is uncertainty as to how such filtering takes place, especially where registration is carried out by agents. Furthermore, the registry has prohibited the resale of domain names to a 3rd party.[71] This may primarily act as a restriction that may help to curb possible cybersquatting, as the violation of the policy terms may result in the cancellation of the domain name.

Renown SC, Case No. D2009-0686, *Facebook, Inc. and Instagram, LLC v. Lasantha Wickramasinghe*, *EntsL / Deepika Priyadarshinie, EntsL,* Case No. D2018-1761; *Fenix International Limited v. Dilshan Omantha,* Case No. DTV2022-0006.

70 'Domain Registry Policy' https://www.domains.lk/domain-registration-policy/ accessed 25 March 2024.

71 ibid.

5.4.2 Court Action

When making trademark claims through litigation, trademark law and law related to unfair competition in Sri Lanka under the Intellectual Property Act No. 36 of 2003 (hereinafter referred to as IPA) would be quite more relevant. While registered trademarks are protected under section 121, unregistered trademarks may still have legal protection under provisions relating to unfair competition and common law actions of passing off. Moreover, despite the lack of explicit recognition, the Computer Crimes Act No. 24 of 2007 may also be applicable to special instances of cybersquatting.

5.4.2.1. Trademark Law

Section 101 of the IPA defines the term "trademark" as "any visible sign serving to distinguish the goods of one enterprise from those of another enterprise".[72] Hence, the function of distinguishing goods is essential to recognising a sign as a trademark. The term "goods" has been defined as "anything which is the subject of trade, manufacture, or merchandise and includes services". In this context, the term "subject of trade" can be understood to encompass a range of assets beyond traditional goods or services. Therefore, domain names, including those stockpiled after registration, can be interpreted as constituting a trademark, although they do not refer to specific goods or services.

Section 170 of the IPA provides the trademark owner with several remedies, including injunctive reliefs, declarative reliefs, removal of marks, recovery of profits and damages, etc. Furthermore, under section 184, criminal sanctions may apply if the willfulness of the trademark

[72] Intellectual Property Act No.36 of 2006, s 101.

infringer can be established along with the act of infringement. Section 186(1)(a) criminalizes the act of forging marks, while section 186(2) criminalizes the sale, display, or possession of goods or things with a forged or misleading trademark.[73] Hence, the IPA not only provides civil remedies but also allows parties to seek criminal remedies under the same Act.

5.4.2.2. Unfair Competition Law

In *Hexagon Pvt Ltd. v Australian Broadcasting Commission*, unfair competition was recognized as, "an extension of the doctrine of passing off, or, possibly, a new and independent cause of action".[74] The laws related to unfair competition are provided by section 160 of the IPA.

Section 160 (1)(a) stipulates that, "Any act or practice carried out or engaged in the course of industrial or commercial activities, that is contrary to honest practices shall constitute an act of unfair competition".[75] An act contrary to honest practices amounts to a wider scope of activities that may allow for action against the infringer, in a potential cybersquatting scenario. In addition, section 160 of the Act outlines specific instances where an act is deemed contrary to honest practices. This includes causing or being likely to cause confusion, damaging another's goodwill or reputation, misleading the public, and discrediting another's enterprise or activities. Therefore, despite the absence of separate legislation in Sri Lanka to address cybersquatting, the existing laws may offer a substantial level of trademark protection in cybersquatting cases.

---

73 ibid, s 186 (1)(a) s 186(2).

74 *Hexagon Pvt Ltd. v Australian Broadcasting Commission* (1975) 7 ALR 233 13.

75 Intellectual Property Act n 72 s 160 (1)(a).

5.4.2.3. Computer Crime Act No 24 of 2007

The Computer Crime Act (hereinafter referred to as CCA) is a piece of legislation specially crafted to address cybercrimes in Sri Lanka. While cybersquatting is considered a cybercrime, the CCA does not specifically recognize cybersquatting within its scope. Nevertheless, section 5 of the CCA prohibits engaging in any activity that results in an unauthorized modification or damage or potential damage to any computer or computer system or computer program. Although the act of cybersquatting does not directly modify, damage, or bring potential damage to any computer, or system, or program, the above provision of the CCA can be applied in special instances of cybersquatting, where the squatted domain is used for malicious activities, such as hosting phishing websites or distributing malware that can harm computers, or systems, or programs belonging to the users.

6. SUGGESTIONS

The current provisions in Intellectual Property Act No. 36 of 2006 may offer substantial protection against the emerging challenges of cybersquatting in Sri Lanka. Nevertheless, it is recommended that amendments be introduced in line with the Anticybersquatting Consumer Protection Act (ACPA) in the USA to extend protection beyond the current provisions of traditional trademark law and unfair competition law in the Intellectual Property Act (IPA). This would involve recognizing cybersquatting as long as the domain name was registered in bad faith, even if it is not intended for commercial purposes. Moreover, explicit provisions need to be introduced to strengthen the trademark owner's position. These provisions could include allowing the transfer of websites, enabling trademark owners to claim attorney's fees and damages in cases where the registrant is found guilty of cybersquatting. In addition, the lk domain name

registry should introduce a formal independent dispute resolution mechanism with a clearly defined procedure similar to that of the UK, USA, and India. Moreover, the registry needs to implement a “whois” service, as in the UK domain registry, which could aid trademark owners in pursuing action by helping them detect potential cyber-squatters. The Computer Crime Act should also be amended to recognize cybersquatting as a cybercrime and to impose criminal liabilities on individuals who register domain names in bad faith. The above suggestions concerning Sri Lanka's legal framework and domain name policy may further strengthen the safeguard against cybersquatting.

7. CONCLUSION

The emerging threat of cybersquatting has raised several legal challenges for trademark owners in the digital era. In some instances, cybersquatting may not amount to a trademark violation, due to it not fulfilling the traditional criteria of trademark law. The USA has introduced a separate piece of legislation to overcome this dilemma, while the UK and India have stretched the interpretation of their trademark laws to deter cybersquatting. Sri Lanka is relatively new to the challenges posed by the emerging trend of cybersquatting. The Intellectual Property Act No. 36 of 2006 presents a potential solution to cybersquatting threats in Sri Lanka. Furthermore, alternative dispute resolution mechanisms such as the UDRP introduced by ICANN, those introduced by domain name operators in the country, and existing ADR methods such as arbitration, will provide quick and efficient remedies to trademark owners in cases of cybersquatting. Nevertheless, it is necessary to enhance Sri Lanka's existing trademark law and improve the domain name dispute resolution policy while taking into account the suggestions from other jurisdictions, as discussed earlier.