Journal of Intellectual Property Studies Vol. VII(2), October 2023 pp.85-100

TYPOSQUATTING AND ITS IMPACT UPON INTELLECTUAL PROPERTY IN CYBERSPACE: A LEGAL STUDY

JYOTIRINGA PUZARI*

ABSTRACT

In 1982, the American-Canadian writer William Gibson coined the term 'cyberspace'. He described cyberspace as "the creation of a computer network in a world filled with artificially intelligent beings". Now popularly known as the Internet, 'cyberspace' has undergone significant evolution since its inception. We have witnessed that online technology has substantially advanced and simultaneously global e-commerce has exponentially developed. However, with this development, newer forms of cybercrime have come to the surface. One such example is the relatively unknown practice of 'typosquatting'. Typosquatting, identified as 'URL hijacking', can be understood as a practice in cyberspace that involves the use of a domain name similar to a well-known brand or trademark. This practice actually aims to deceive users into visiting a fraudulent website instead of the legitimate ones, wherein their personal and sensitive information is put at the risk of theft and harm.

This research paper examines the issue of typosquatting in the context of intellectual property rights in the cyberspace. It explores the legal and ethical implications of this practice and highlights the challenges faced by IPR holders in protecting their rights in the online environment. The paper argues that typosquatting poses a significant threat to IPR, and that there is a need for a more comprehensive legal framework to address this issue, especially in India. It also suggests various measures that IPR holders can take to protect their rights and prevent the spread of typosquatting. Ultimately, this paper emphasizes upon the need for a collaborative effort between IPR holders, policymakers, and internet service providers in India to combat the issue of typosquatting and aims at securing the online environment and protecting intellectual property rights in the cyberspace.

I. INTRODUCTION

The Internet was initially intended to be a decentralized network for communication and information exchange like Advanced Research Projects Agency Network ["**ARPANET**"], the pioneer project of the US Department of Defence in the 1960s. ARPANET 'decentralized' architecture relied on a distributed yet inter-connected design of computers and devices wherein

* LL.M. (specialisation in IPR), National Law University and Judicial Academy, Assam.

multiple servers are robustly connected with each other to transmit data and offer a resilient communication network,[1] but it has now developed into a vital infrastructure for international trade, social engagement, and communication. In recent years, there has been a shift towards using the Internet for commercial purposes, transforming the nature of businesses, services and transactions, like 'digitalized marketing'. The marketing landscape has changed, and the old-style physical marketplace has paved the way for electronic commerce, commonly termed as 'e-commerce'. As a result, many companies have achieved success in their online businesses and commercial services.[2] But over time, competition grew among businesses to attract customers and to expose their businesses over the Internet. These companies placed great emphasis on customer usage to their websites, and they sought to differentiate their products by using 'trademarks', which not only signify quality but also aid in building brand recognition (through the use of 'brand-names'). Thus, using domain names as trademarks began to help "businesses to create a strong presence on the Internet".[3]

Domain names, generally user-friendly names, are unique addresses used by internet surfers/ users to name and give identity to one's website, including commercial websites. For example, *Myntra*, which is a popular Indian website known for providing the service of online shopping of clothing apparel, footwear, lifestyle products etc. Thus, domain names act as equivalents of trademarks.[4]

However, with such technological advancements in the cyberspace, new opportunities have opened doors for criminals to exploit the resources of the Internet, including intangible human creations such as a 'domain name'. People attempt to take advantage of domain names owned by other owners by using them inappropriately to gain benefits and profit from the positive reputation already associated with the name. One such way includes the practice of 'typosquatting', as a way of 'domain-mimicry', which can detrimentally impact a brand's reputation and introduce complications for both the business and its website(s). For instance, a false website which imitates a legitimate business's website by using slight alphabetical variations in their website's name can

---

[1] Vijay Kanade, *What is ARPANET? Definition, Features, and Importance*, SPICEWORKS, (Sep 12, 2023), https://www.spiceworks.com/tech/networking/articles/what-is-arpanet/#:~:text=The%20architecture%20of%20ARPANET%20was,dedicated%20phone%20connections%20between%20them.

[2] Jalaj Agarwal & Gracy Bindra, *Domain Name Disputes and the rising threat of Cybersquatters,* 6 IJLS, 1, 1 (2020).

[3] Dara B. Gilwit, *The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement,* 11 WASH. U. J. L. & POL'Y, 267, 267 (2003).

[4] Chadha & Chadha Intellectual Property Law Firm, *Domain name and Trademark rights in India*, LEXOLOGY, (Mar. 21, 2023), https://www.lexology.com/library/detail.aspx?g=daaafca2-6a68-4134-bd29-27aa941a1f03#:~:text=For%20infringement%3A%20Any%20person%20violating,section%2029%20of%20the%20Act.

create confusion and distrust among consumers as well as dilute the brand's online presence and its reputation in the long run through its misleading and malicious content.

Typosquatting refers to the act of registering domain names that resemble existing ones but have minor spelling mistakes or typos. Individuals involved in typosquatting exploit these errors to redirect people to their own websites, which may contain harmful or malicious content as well as advertisements. In terms of intellectual property rights ["**IPR**"], typosquatting can be seen as a type of trademark infringement that can harm the reputation and goodwill of a trademark owner. These "typo-squatters" register domain names that closely resemble trademarked names or brands and utilize them to confuse consumers or divert traffic away from the legitimate website. As a result, the trademark owner may experience financial losses and damages to their reputation. Furthermore, typosquatting poses a risk to consumers, who may unintentionally visit websites hosting malware or engage in fraudulent activities. Fraudulent websites often employ subtle variations in legitimate domain names, such as omitting or adding a letter or modifying the domain extension.

In recent times, typosquatting has had significant adverse effects on the cyberspace. One of these is the potential for financial losses to both individuals and businesses that unknowingly enter sensitive data such as login credentials or credit card details on fraudulent websites. Furthermore, when typosquatters misappropriate the names of legitimate companies with well-known brands, it damages their reputation, which eventually costs them money and undermines customer trust. Additionally, typosquatting can facilitate the spread of other cybercrimes, such as phishing and ransomware attacks. Cyber-criminals can use typosquatting to disseminate malicious software or direct unsuspecting users to phishing websites where they can extract sensitive information or infect the user's device with malware. Apart from these cybercrimes, this practice clearly infringes upon the intellectual property rights of a person who has actually registered a 'domain name' after following all necessary legal procedures. Therefore, this sub-form of 'cybersquatting' should be given due notice and laws should be made to respond against this malicious practice.

In India, there is no law in existence to combat this evil practice of typosquatting; there are no specific provisions under the Information Technology Act, 2000[5] to deal with typosquatting.[6] The

[5] Information Technology Act, 2000, No. 21, Act of Parliament, 2000 (India).
[6] Madhavendra Singh, *Typosquatting- An Evil in Cyberspace*, LIVELAW (Mar. 21, 2023), https://www.livelaw.in/columns/typosquatting-cyberspace-cybercrimes-cybersquatter-201029#_ftn2.

only remedy is to bring an action under the Trade Marks Act, 1999.[7] Moreover, there are only a few countries, such as United States of America ["**US**"] that criminalises the act of 'typosquatting' *per se*.[8] The enforcement of laws and regulations prohibiting typosquatting vary across jurisdictions and it can be difficult to pursue a legal action against typosquatters who operate in countries with weaker or non-existent provisions against such a practice in their laws relating to intellectual property.[9]

Hence, it is important to understand and discuss how IPR can be secured in the cyberspace from such new, yet lesser-known cyber-threats and further aid in the protection of the interests of domain-name owners.

II. TYPOSQUATTING OF DOMAIN-NAME: FROM THE LENS OF INTELLECTUAL PROPERTY LAW

The violation of IPRs in the cyberspace has also emerged as a major concern due to the proliferation of 'cyber technology'. Therefore, safeguarding online content and creations has become quite imperative in present times. It is crucial to acknowledge that "domain names" are more than just names assigned to websites belonging to different businesses or organizations; they serve as valuable business identifiers that play a vital role in enhancing the visibility and reputation of the respective business entity.[10] Having a domain name today has become an essential aspect for any business that engages in digital operations or maintains a presence on the internet, and so does its legal protection.

A. Domain Name as an Intellectual Property

Domain names are user-friendly web addresses that are designed to be memorable and easily accessible for internet users when trying to locate a specific website. These addresses are intended to be comprehensive, memorable, and simple to use.[11] Every internet website has its own unique IP address, and the web server uses a domain name system to translate a domain name into the corresponding numerical IP address in order to access a website. In simpler terms, a domain-name can be understood as the address of a website on the Internet. So, the name that one writes in the web-browser to visit a website is the 'domain name'. For instance, to access the popular social-

[7] Trade Marks Act, 1999, No. 47, Act of Parliament, 1999 (India).
[8] SINGH, *supra* note 5.
[9] *Id.*
[10] Tejaswini Kaushal, *Domain Name as Intellectual Property: An Analysis,* LEGALLY FLAWLESS (Mar. 29, 2023), https://legallyflawless.in/domain-name-as-intellectual-property-an-analysis/#need_for_domain_names.
[11] *Id.*

networking site 'Facebook', one has to type "facebook.com" on the web-browser which is the domain-name.

There is a significant difference between trademark and domain name. A trademark is a symbol or design that is visually recognizable and is used to differentiate one company's products or services from another's. This may include elements such as colour schemes, packaging, and the shape of products. A domain name, on the other hand, is the word-text that people enter into their web browsers to access a particular website. Additionally, while trademark law prohibits the use of deceptively similar marks, there is no such prohibition in domain-name registration. Even minor variations of existing domain names can be registered without issue. This implies that a domain-name can be registered which may closely resembles an existing one and it is easily allowed just because it may have slight alterations or changes in it from the existing one.[12] Snehlata Singh in her paper[13] illustrated that there is a possibility of existence of "www.abcd.com" and "www.ab-cd.com" as two different registered domain-names.

In India, the judicial interpretation of domain-names as 'trademarks' under the Trade Marks Act, 1999 proves that these domain names are indeed intellectual property which should not be infringed by others, without the consent or license of the proprietor.

Companies use domain names to differentiate their products and services from their competitors, as well as to advertise them and strengthen customer loyalty. These names are more than just addresses; they function as trademarks by indicating the source of a business. If another individual uses a similar name, design, or pronunciation of an existing trademark in a way that misleads the public, it is a form of violation of the trademark holder's rights. This act constitutes infringement. This not only damages the reputation of the trademark holder, but also provides an unfair advantage to the infringing business.

The first instance in which an Indian court granted trademark safeguarding to domain names was the case of *Titan Industries Limited v. Prashanth Koorapati and Ors.*[14] The plaintiff received a favourable ruling from the Delhi High Court, which ordered an *ex parte ad interim* injunction prohibiting the

[12] Himanshi Jain*, Everything's Gone Digital, and So Did Infringers: Domain Name Disputes*, 3 DME JL 27, 28 (2022).
[13] Snehlata Singh, *Conflicts between Trademarks and Domain Names: A Critical Analysis,* SSRN (2011), https://dx.doi.org/10.2139/ssrn.2045222.
[14] Titan Industries Limited v. Prashanth Koorapati and Ors, Delhi High Court Suit No. 179 of 1998.

defendant from using the trade name "*Tanishq*" or any other name that would be confusingly similar and cause the plaintiff's business and products to be passed off as their own.

In the case of *Satyam Infoway Ltd v. Sifynet Solutions*[15] the appellant (Satyam Infoway Ltd.) claimed to have registered several domain names with the word '*Sify*' prior to the respondent. Their claim centred on the contention that the use of a similar domain name by the respondent was leading to confusion in the minds of potential customers, thereby constituting a violation of their intellectual property right. The Supreme Court of India acknowledged that there is no specific law in India that addresses the resolution of disputes related to domain names and therefore, in the absence of a specific legislation, the matter was resolved in the court by applying general principles of trademark law and the passing-off doctrine. However, even though the Trade Marks Act may not provide sufficient protection for domain names, it does not imply that they cannot be legally safeguarded under the laws concerning passing-off., as mentioned in the Trade Marks Act.[16]

Another significant Indian case is that of *Tata Sons v. The Advanced Information Technology Association*[17] wherein World Intellectual Property Organization ["**WIPO**"] held that the term "Tata" was a distinguished name associated with superior merchandise. Since it was a surname and lacked any literal interpretation, Internet Corporation for Assigned Names and Numbers ["**ICANN**"] granted the transfer of the domain name to Tata Sons after WIPO ruled in their favour. This statement has been rephrased to avoid plagiarism.

B. Typosquatting as trademark infringement

Typosquatting can amount to trademark infringement for several reasons.

1. First, consumer confusion may result from the registration and usage of a domain name that is confusingly similar to a brand, leading them to believe that they are accessing the official website of the trademark owner. This can damage the reputation and goodwill of the trademark owner, and potentially lead to financial losses if consumers are misled into making purchases on a fake website.
2. Secondly, typosquatting can dilute the distinctiveness of a trademark by creating a situation where multiple websites are using similar domain names, which can make it more difficult for consumers to identify the legitimate website associated with the trademark. The exclusive right

[15] Satyam Infoway Ltd v. Sifynet Solutions, (2004) 6 SCC 145.
[16] *Id.*
[17] Tata Sons v. The Advanced Information Technology Association, WIPO Case No. D2000-0049.

of the trademark owner to use their trademark in commerce may ultimately be weakened as a result.

3. Additionally, typosquatting can also be seen as a form of cyber-squatting, which is the practice of registering a domain name with the intention of profiting from the resale of the domain name or by using the domain name to engage in online activities that infringe upon the trademark owner's rights.

III. TYPOSQUATTING IN THE EXISTING LEGAL FRAMEWORK

It is well-established that 'typosquatting' refers to the act of a person registering a domain name that bears a resemblance to an established brand by making slight changes to the spelling. For instance, an example can be registering a fake website named "goglee.com" imitating the popular website "google.com". This practice shall be considered as infringement. Another possibility is the creation of a fake website with identical logos and colour schemes. As a result, fraudsters utilise these websites to force people to buy their products, increasing traffic and propagating malware.[18] In many countries, typosquatting is illegal under their existing trademark and unfair competition laws. Typosquatting remains a problem on the Internet and the legal frameworks in place are meant to combat it in any form.

A. United States of America

The distinction of enacting the first thorough cybersquatting regulation belongs to the United States. In 1999, the Congress passed the Anti-Cybersquatting Consumer Protection Act [**"ACPA"**]. However, prior to this Act, there was no specific clause dealing with cybersquatting. Prior to the adoption of the ACPA, trademark owners frequently used the Federal Trademark Dilution Act ["**FTDA**"], commonly known as the Lanham Act, which was passed in 1995, to bring legal actions against domain name registrants. The landmark case of *Panavision International LP v. Toeppen*[19] somewhat aided the drafting of the ACPA, which was done to prevent trademark infringement in the cyberspace. In this particular case, the plaintiff won the case, with the court determining that the defendant had violated the plaintiff's rights by registering domain names as 'www.panavison.com' and 'www.panaflex.com', and displaying images of the Pana Valley. This was because the plaintiff's business was focused on tourism and relied on the internet to attract customers.[20]

[18] JAIN, *supra* note 10, at 30.
[19] Panavision International LP v. Toeppen, 141 F.3d 1316, 1326 (9th Cir. 1998).
[20] *Id.*

The ACPA was introduced to extend the Lanham Act (15 U.S.C.) by safeguarding individuals and owners of distinctive trademarked names from cybersquatting. If cyber-squatters are located and the US courts have jurisdiction over the case, the ACPA's trademark provision can be utilized. To succeed under this provision, the plaintiff must demonstrate the following:

(a) The disputed mark is well-known or has a unique quality;
(b) The domain name is the same as or resembles a distinctive or famous mark in a confusing manner, or
(c) Harms the image of a well-known mark; and
(d) The registrant acquired, used, or sold the domain name with an intention to unjustly profit from the plaintiff's mark.[21]

The ACPA, however, also facilitates the mechanism of serving justice to the defendants who are unable to be located or who are outside of the Court's personal jurisdiction (as per the *in rem* provision).[22]

In the landmark case of *Morrison & Foerster v. Wick,*[23] the claimant was the rightful holder of the trademark "Morrison & Foerster". The defendant, on the other hand, had registered two domain names, "morrisonfoerster.com" and "morrissonandfoester.com". After a court hearing, it was determined that the defendant's domain names were nearly indistinguishable from the claimant's trademarked name. Additionally, the court also found that the defendant had caused harm to the claimant's reputation by displaying racist slogans and hyperlinks on their web pages, thereby damaging the claimant's goodwill. The court's decision reflected on how typosquatting of a popular domain-name harms the business and goodwill of the original domain name-owner.

It is concerning that a common Dispute Resolution Policy for ".us domain names" does not exist in the US jurisdiction, due to the absence of a centralized entity managing the domain name space. The United States Dispute Resolution Policy ["**USDRP**"] allows for the cancellation or transfer of "us domain names" that violate the complainant's trademarks,[24] while the United States Nexus Dispute Policy ["**USNDP**"] ensures that all ".us domain name registrations" have a strong connection to the United States.[25]

[21] Anti-Cybersquatting Consumer Protection Act of 1999, 15 U.S.C §1125(d)(1)(A).
[22] Anti-Cybersquatting Consumer Protection Act of 1999, 15 U.S.C § 1125(d)(2).
[23] Morrison & Foerster v. Wick, 94 F. Supp. 2d 1125 (D. Colo. 2000).
[24] DISPUTE RESOLUTION POLICY (last visited Mar. 29, 2023), http://www.neustar.us/policies/docs/usdrp.pdf.
[25] NEXUS DISPUTE POLICY (last visited Mar. 29, 2023), http://www.neustar.us/policies/docs/nexus_dispute_policy.pdf.

The Truth in Domain Names Act, 2003 ["**TDNA**"] is another important legislation under which "using a misleading internet domain name to trick someone into accessing pornographic material is considered a criminal act".[26] Individuals who break the 'law' may be penalized with a monetary fine and/or imprisonment for a maximum term of two years. However, if an individual has the intention to deceive a minor, the penalty may increase to a monetary fine and/or imprisonment for a maximum term of four years.

John Zuccarini is one of the notorious 'typosquatters' and the first person to ever be charged with offences violating the TDNA. He allegedly made $1 million per year by registering thousands of domain names that were common misspellings of popular Web sites.[27] Zuccarini has faced many lawsuits, and due to multiple violations of the ACPA, has been obligated to hand over around 200 domain names to the legitimate copyright and trademark owners. His typosquatting was so extensive that the Federal Trade Commission ultimately obtained a permanent injunction against him. As per the complaint filed against him, Zuccarini kept up numerous websites with names that were commonly misspelled versions of famous domain names, and he continued to host pornographic content on these sites. Additionally, some of his websites were misspelled versions of websites that were popular among children. Zuccarini was later sentenced to two and a half years of imprisonment in February, 2004.[28]

B. International Framework

ICANN happens to be a significant entity in this regard. Established in 1998 by the US government, ICANN currently operates as the supervisor of the global Domain Name System, administering and regulating domain names, IP addresses etc. One noteworthy event occurred on October 24, 1999, when the ICANN implemented a policy called the Uniform Dispute Handling Policy ["**UDRP**"].[29] The main objective of the UDRP is to create a structure to solve disputes that arise between registrants or domain name holders and third parties who assert a prior interest in the domain name. This policy has proved to be an economical and effective way of combating cyber squatters and other related issues. Organizations that have been approved by ICANN conduct the UDRP implementation. The most prominent organization that provides UDRP

[26] The Truth in Domain Names Act of 2003, 18 U.S.C. § 2252B.
[27] *Id.* at 145.
[28] CNN TECHNOLOGY (last visted Mar. 30, 2023), http://edition.cnn.com/2003/TECH/internet/09/03/trick.names/index.html.
[29] *Uniform Domain Name Dispute Resolution Policy*, ICANN (last visited Mar. 30, 2023), http://www.icann.org/ udrp/udrp-policy24oct99.htm.

services is the WIPO. ICANN-accredited registrars can sell domain names, and ICANN supervises the domain name registration system, which includes setting standards and criteria for all accredited registrars. ICANN is in charge of coordinating and maintaining the domain name system, as well as assigning IP addresses and distinguishing domain names.[30]

The UDRP makes it mandatory for any individual or entity that registers a domain name through an ICANN-accredited domain registry to utilize the policy.[31] The primary objective of formulating this policy was to address conflicts that may arise between owners of domain names and trademarks. The first UDRP dispute was centred on the case of *World Wrestling Federation Entertainment Inc. v. Michael Bosman,*[32] which served as the inaugural instance of such a case being resolved. The litigation was initiated by the US-based Federation against Bosman, who resided in California. It revolved around Bosman's registration of the domain name 'www.worldwrestlingfederation.com'.

There are currently six dispute resolution organizations that are permitted to accept complaints made in accordance with the UDRP's complaint procedure. The WIPO is considered to be the most popular domain name dispute resolution platform. In a certain case,[33] the WIPO ruled in favour of Google Inc. wherein Google Inc. won the case against an Indian teenager, Herit Shah, in 2009 for typosquatting. Shah had registered the domain name googblog.com, which Google claimed was too similar to its trademark and could confuse users. WIPO ruled in favour of Google on May 15, 2009, and directed Shah to transfer the domain name to Google Inc. since the company had been actively using the domain.

While the UDRP has been effective in many cases, it is not without its flaws. The UDRP policy only applies to disputes over domain names registrations and does not address broader issues such as trademark infringement or 'typoquatting'. The UDRP process is often criticized for lacking transparency.

C. Position of India

There is no specific legislation in India that addresses the resolution of conflicts related to cybersquatting or other disputes over domain names in a direct manner. The Information

[30] EKTA SOOD & VIBHUTI NAKTA, CYBERSQUATTING: NEED FOR PROTECTION OF DOMAIN NAMES IN THE REALM OF CYBERSPACE, IGI Global 120, 126 (2022).
[31] *Id.* at 127.
[32] World Wrestling Federation Entertainment Inc. v. Michael Bosman, 1 N.C.J.L. & Tech. 3 (2000).
[33] Google Inc. v. Herit Shah, Case No. D2009-0405.

Technology Act, 2000, the primary law that criminalizes cybercrime, makes no mention of typosquatting. It is also important to note that the cybersquatting cases are decided through the principle of passing off and infringement, as contained in the Trade Marks Act, 1999. The Indian courts have, therefore, been active in resolving cases relating to cyber-squatting under these laws. In 1999, India's first cyber-squatting case was brought to court between *Yahoo! Inc. and Akash Arora & Anr.*[34] Yahoo! Inc., the plaintiff, owned the well-known brand "Yahoo!" and the domain name "Yahoo.com." However, the defendants registered a similar domain name, "YahooIndia.com," which had a similar format and colour scheme and provided similar services to the plaintiff. The Delhi High Court used the law of passing to prohibit the defendant from using the domain name. The court ruled in favour of the plaintiff, stating that the defendant's domain name was misleadingly similar, intended to deceive the public and take advantage of Yahoo Inc.'s reputation.

The case of *Rediff Communication v Cyberbooth & Anr,*[35] another significant case relating to typosquatting, was decided by the Bombay High Court. The defendants had registered a domain name "radiff.com" which was similar to the plaintiff's domain name "rediff.com". The court ruled in favour of the plaintiff, as the defendant's domain name had the potential to cause confusion between the two distinct entities. The court also recognized the importance of domain names as valuable assets that need to be protected.

It is therefore, the need of the hour, to incorporate provisions in the existing laws or far better, come up with a *sui-generis* law dealing with cybersquatting and typosquatting. Having a specialized legislation focused on cybersquatting can offer more precise guidelines on what constitutes cybersquatting, making it simpler for affected parties to take legal action. Besides, such legislation could establish a conflict resolution mechanism for more expedient and affordable resolution of cybersquatting as well as typosquatting disputes.

IV. MAPPING INDIA'S APPROACH TOWARDS TYPOSQUATTING: THE ROAD AHEAD

Although there is no exclusive, separate law in India that addresses typosquatting, the existing legal framework offers several legal options and remedies to tackle typosquatting through different provisions in the cyber[36] and trademark[37] law. However, this is not adequate enough and it does not narrow down the need of a 'comprehensive and effective *sui-generis* law' to address the growing

[34] Yahoo! Inc. v. Akash Arora & Anr., (1999) IIAD Delhi 229.
[35] Rediff Communication v. Cyberbooth & Anr, (1999) 4 BomCR 278.
[36] Information Technology Act, 2000, No. 21, Act of Parliament, 2000 (India).
[37] Trade Marks Act, 1999, No. 47, Act of Parliament, 1999 (India).

concerns over the offence(s) and disputes concerning typosquatting of domain names. Typosquatting creates consequences that can result in dilution of a trademark or a brand, loss of revenue, and damages to the legitimate owner's reputation. Furthermore, typosquatting can also result in the violation of the trademark holder's sole entitlement to utilize their trade mark and in this manner; this practice poses a serious threat to the integrity and value of IPR.

Given the increasing prevalence and rising trend of instance of typosquatting in India, enacting a dedicated law to address it would offer improved legal clarity and certainty for both the offenders and the aggrieved parties. This law could encompass a definition of typosquatting, as well as penalties, fines, and other legal actions. Additionally, it could outline a system for settling disputes related to typosquatting. Nevertheless, it would be essential to approach this legislation with care and consultation with different stakeholders, especially the users, before implementation. The rising overlap between trademark and domain name systems has had certain detrimental effects that need to be mitigated as soon as possible.

The Indian laws are facing certain challenges related to this issue. The Trade Marks Act of 1999 doesn't include any particular provisions that expressly define or address anything related to domain names, nor does it outline the criteria and procedure for protecting domain names from a trade mark infringement. Moreover, the Act's authority doesn't extend beyond Indian borders, meaning it can't provide adequate protection in case of infringement outside India. Additionally, the Information Technology Act, 2000 doesn't adequately address domain name disputes related to trademark infringement or prevent typosquatting. In this context, the Indian legislators can draw parallels to the particular US laws countering cybersquatting and accommodate the legal provisions on similar lines.

The Trade Marks Act, 1999 can be revised to accommodate provisions relating to cybersquatting and its different forms, including typosquatting. The first step should be the express and exclusive inclusion of 'domain-name' in the ambit of the definition of Trade Mark.[38] Sec. 11 of the Trade Marks Act, 1999 which deals with grounds for refusal of registration of a trade mark, can be amended to the extent that the instance of existence of an identical or confusingly similar trademark in the same class of products or services in the offline market can be acknowledged a relative ground for a domain name's refusal to be registered as a trademark.[39] The same law can be

[38] Trade Marks Act, 1999, § 2 (m), No. 47, Act of Parliament, 1999 (India).
[39] Manthan Agarwala & Simran Kang, *Cybersquatting India: Genesis & Legal Scenario,* 4 IJLMH 740, 756 (2021).

changed to add a new clause that outlaws different types of cybersquatting as a result of trademark infringement. It is crucial to define cybersquatting and typosquatting in detail during the domain name registration procedure in order to achieve this. This would be similar to the Anti-Cybersquatting Consumer Protection Act's *in rem* clause.[40] India can adopt a legal provision that enables trademark holders to take legal action against domain names directly rather than the owners of domain names if the owners cannot be located or if personal jurisdiction over them cannot be established.[41] With this inclusion, the trademark will not be limited as 'territorial' in nature. Moreover, in order to prevent fraudulent and erroneous domain name claims, the registration must be cancelled, and activities committed in 'bad faith' must be dealt with, as strictly as possible.[42]

The Information Technology Act, 2000 can also be amended to bring about necessary changes and accommodations in the law to address the issue of typosquatting in a strict sense. Amendments can be made on similar lines with the US Act,[43] restricting and imposing penalties on individuals who deliberately employ deceptive internet domain names with the intention to mislead people, particularly minors, into accessing explicit or pornographic material. The Act could be amended to increase the damages that can be awarded to victims of typosquatting. This would act as a deterrent to typosquatters and provide greater compensation to the victims of typosquatting. Moreover, the registration of domain name procedure could be made stricter by requiring domain name registrars to verify the identity of applicants and then implement the rules of registration. If a person is found guilty of "typosquatting" by an Indian court, the penalties may also be included. In other words, along with civil remedies (injunction orders, accounts of profits etc.) significant criminal remedies can be made available under the amended Act against typosquatting and the court can sentence offenders (including repeated offenders) to imprisonment and fine depending upon the gravity of the offence.

However, India could also take a different *sui-generis* approach in its initiative towards 'combating' the offence of typosquatting. As mentioned earlier, the first step towards creating a *sui generis* law for typosquatting would be to define the term clearly in the legislation. This would ensure that the scope of the law is well-defined and that it covers all relevant activities. The second step may be putting up a 'domain name dispute resolution mechanism' to settle disputes related to

[40] Anti-Cybersquatting Consumer Protection Act of 1999, 15 U.S.C §1125(d)(2).
[41] Manthan, *supra* note 36, at 756.
[42] Jalaj Agarwal & Gracy Bindra, *Domain Name Disputes and the Rising Threat of Cybersquatters*, 6 IJLS 1, 13 (2020).
[43] The Truth in Domain Names Act of 2003, 18 U.S.C. § 2252B.

cybersquatting and typosquatting. The legislation should include penalties for typosquatting, which should be strong enough to deter individuals or companies from engaging in such activities. The penalties could include fines, imprisonment, or both. One way for India to align its laws and regulations with international standards regarding cybersquatting and typosquatting is by working together with global organizations like WIPO to create effective strategies and recommendations. This collaboration would enable India to establish the best practices that are in line with the world's expectations. A watch-list of frequently misspelt terms and phrases that typosquatters frequently target can be made by the Indian Registry. This can help domain name registrars and trademark owners identify potential cases of typosquatting and take appropriate action. The *sui-generis* Indian law can establish a National Domain Name Dispute Resolution Center that would provide a central location for resolving domain name disputes. This Center could be staffed by experts in the domain of intellectual property law, domain name registration, and alternative dispute resolution mechanisms, including online mediation process to resolve such disputes.[44]

Instead of the lenient 'first-come-first' basis of registration, the procedure can be elaborated in the *sui-generis* law in a comprehensive yet strict manner. The domain name registration process is a critical aspect of preventing cybersquatting and typosquatting. Some points can be considered to be included which will aid in creating a robust and secure domain-name registration process:

(a) The requirement of ownership details as proof during registration procedure.
(b) Adopting a verification process for registrants/ applicants.
(c) Creating a clearing-house for Trademarks to allow trademark owners to register their trademarks and receive alerts when someone tries to list a new domain name that resembles their trademark.
(d) Administrative panels should be set up to regulate the domain name registration process and administer the allotment of Second Level Domain Names which tend to be identical or closely similar to 'existing names'.[45]

India can draw parallels from the US law on cybersquatting which mandates that cybersquatting can only be established if the domain name's registration, trafficking, or utilization has been carried out with malicious/ bad intent to profit.[46] In a similar vein, India may contemplate incorporating a criterion into its legislation that provides to ensure that only malevolent behaviours and malicious criminal intent are subject to criminal penalty. This could serve to establish clear distinctions

[44] JALAJ, *supra* note 39, at 14.
[45] *Id.* at 14.
[46] Anti-Cybersquatting Consumer Protection Act of 1999, 15 U.S.C. § 1125(d)(1)(A)(i).

between lawful domain registration and intentional actions aimed at deceiving or causing harm to internet users. By outlining precise criteria for determining criminal responsibility in instances of typosquatting, Indian legislation could enhance its ability to tackle and discourage malicious conduct while also protecting legitimate online practices. The ACPA has certain provisions that provide a safe haven for intermediaries, such as domain name registrars, to shield them from any responsibility for cybersquatting committed by their customers/ clients.[47] India could also take into account the inclusion of 'safe harbour provisions' in its legislation to safeguard intermediaries. This would mean that intermediaries like domain-registrars or Internet service providers in India will not be held responsible for the illicit Internet activities carried out by their customers or clients, as long as they meet the necessary conditions and procedures, The safe harbour provision strikes a balance between holding the actual wrongdoers accountable and protecting those who provide services. After all, the aim of the law is to promote fairness, justice and effectiveness.

Regarding legal awareness, there is potential for collaboration between law schools, legal aid clinics, domain name registrars, Internet service providers, and other industry stakeholders to increase the understanding of the law and encourage adherence to it. This may involve establishing guidelines for registering and managing domain names, as well as offering training and educational opportunities for industry professionals. Additionally, India can prompt industry stakeholders to report any instances of legal violations and cooperate with law enforcement during investigations. The aim of India's *sui-generis* law on deceitful domain names (typosquatting) should be to safeguard internet users against deception or fraud perpetrated through such domain names, and to foster a more dependable and secure online environment.

V. CONCLUSION

Typosquatting is a deceitful scheme. This practice has the potential to cause significant harm to both individuals and businesses, as it could tarnish the reputation of authentic brands and jeopardize the security of unsuspecting users.

Eventually, typosquatting has emerged as a profitable business for cyber-criminals over time, with some individuals earning millions of dollars annually. Due to the significant revenue generated by typosquatting, the current legal penalties may not be sufficient. The legal system's reliance on civil litigation has been ineffective in deterring typosquatters and aspiring typosquatters, as a single court ruling does not result in their bankruptcy or the removal of all infringing domain names or

[47] Anti-Cybersquatting Consumer Protection Act of 1999, 15 U.S.C. § 1125(d).

the payment of substantial monetary damages. It is due to the fact that the profits incurred from use of deceptive domain names are really huge and offenders generally operate under multiple identities which enable them to continue their illicit business of registering new domain names. Therefore, considering the criminal intent, typosquatting should be considered a serious criminal offence and punishment should be given accordingly. This paper aims to highlight the general public's lack of knowledge and concern about this type of offense. Furthermore, there is currently no specific legislation in India especially, to address the issue of 'typosquatting'. In India, it is only deemed a violation of Trademark law, enabling companies to seek legal redressal against persons or organizations that engage in this activity. But countries such as the United States have put in place laws for protection against typosquatting, a form of cybersquatting. This should inspire India s well, to come up with a *sui-generis* law dealing against the offence of 'typosquatting'. Moreover, the Indian Domain Name Dispute Resolution Policy could be amended, and certain unnecessary arbitration procedures could be removed to enable a smoother process of litigation.

Overall, it is crucial for individuals and companies to recognise the risks posed by typosquatting and to implement measures to safeguard themselves against this form of cybercrime. This involves keeping an eye on domain name registrations vigilantly, instead of a lenient 'first-come-first-served' basis and then take legal action against fraudulent domain names that resemble their own brand names which will enable the authentic brand-owner/ proprietor to safeguard their intellectual property rights. Remaining vigilant and taking appropriate precautions can help to prevent the harmful effects of typosquatting and establish a safer online-environment.