# CYBERSQUATTING AND DOMAIN NAME PROTECTION IN CYBERSPACE: A LEGAL ANALYSIS

**Vartika Sisodiya[*] Dr. Seema Gupta[*]**

## INTRODUCTION

In recent decades, the internet has come to dominate the world, which has led to the creation of risks that are associated with the digital era. Over the past few years, the Internet has been employed for business purposes, which has led to a change in the way organizations operate. Numerous firms have effectively developed their company and commerce positioning services online as a result of the evolution of marketing trends and the paradigm shift from traditional marketplaces to online commerce.[1] Domain names under the trademark law are becoming increasingly important as the prevalence of cyberspace in commercial transactions increases.

A digital address that enables an organization or an individual to be identified by other people who use the Internet is referred to as a Domain name. Domain names are used primarily to identify and locate the many computers, users, files, and resources that are accessible via the Internet.

The problem arises when a large number of people claim ownership of the same name, which is explicitly forbidden by the legislation governing trademarks. It is common for trademark law to be defined by its restriction on the use of registered trademarks. This is because the use of registered trademarks has the potential to cause confusion among prospective customers regarding the identity and validity of the supplier of the goods or services.[2] The resolution of disputes between computer users who are acquiring domain names for the Internet and the owners of registered trademarks has been accomplished through the utilisation of this. Cyber-squatting, typo-squatting, mega-tagging, and renewal snatching are some of the negative consequences that are associated with trademarks that have arisen as a result of the transition to the online platform.

[*]LLM, UNIVERSITY INSTITUTE OF LEGAL STUDIES, CHANDIGARH UNIVERSITY.
[*]ASSOCIATE PROFESSOR, UNIVERSITY INSTITUTE OF LEGAL STUDIES, CHANDIGARH UNIVERSITY.

[1] N.S. Gopalakrishnan, *Domain Name Disputes and the Indian Law: Issues and Solutions*, 45 JILI 187, 192 (2003)

[2] K. Venkataraman, *Legal Challenges in the Age of Cyber Squatting*, 4 SCC J 28, 34 (2011).

**1. [3]Toeppen v. Panavision International L.P. (1998)**

The domain name panavision.com was registered by cyber squatter Dennis Toeppen, who tried to sell it to Panavision for $13,000. By registering the name in bad faith, Panavision claimed that Toeppen was engaging in cyber-squatting and filed a lawsuit against him.

Despite the fact that the website did not use the trademark in a conventional sense (i.e., providing services or goods), the U.S. Court of Appeals for the Ninth Circuit determined that Toeppen's acts violated the Federal Trademark Dilution Act. The court observed that Toeppen acted in bad faith since his main goal was to extract money from Panavision.

This case was among the first to demonstrate that, even in the absence of active usage, cybersquatting can reduce a trademark's value, highlighting the significance of registering a domain in good faith.

**2. The Farm of Sporty Sportsman's Market, Inc. v. L.L.C. (1999) [4]**

Sporty's Farm registered the domain sportys.com, which is a name that is similar to the well-known trademark "Sporty's" held by Sportsman's Market, Inc. Claiming that Sporty's Farm had registered the domain in bad faith to interfere with Sportsman's Market's operations, Sportsman's Market filed a lawsuit for infringement.

In accordance with the Ant cybersquatting Consumer Protection Act (ACPA) of 1999, the U.S. Court of Appeals for the Second Circuit determined that Sporty's Farm had registered the name in bad faith and mandated that Sportsman's Market obtain the domain.

Because it used the ACPA to transfer a domain from a bad faith registrant to a legitimate trademark proprietor, this case was crucial. It reaffirmed the idea that domain names are protected against squatting and can be considered intellectual property.

**3. Privacy Ltd. v. Facebook, Inc. (2010)**

Facebook filed a lawsuit against a gang of cybersquatters who used the "Facebook" brand to register domain names such as facebooksearch.com, facebookstuff.com, and facebooklogin.com. Facebook asserted that these domains were created to mislead users and

[3] Panavision Int'l L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998).
[4] Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489 (2nd Cir. 2000).

profit from the positive perception of its brand.

The court decided in favour of Facebook, concluding that the defendant's attempt to capitalize on Facebook's trademark was an act of bad faith. The cyber squatters were compelled to pay damages, and Facebook received the domains.

The case highlighted how crucial it is to protect domain names that bear similarities to well-known trademarks, especially in order to avoid customer misunderstanding and damage to a business's reputation.

### 1.1 TRADEMARK AND DOMAIN NAME SYSTEM

A trademark is legally defined as a unique sign, symbol, word, phrase, design, or combination that identifies and differentiates the goods or services of one entity from those of others in the market. It functions as a mark of origin, signifying the source of the goods or services, and assures a specific standard of quality linked to the brand. According to the Trade Marks Act, 1999 and in alignment with international agreements such as the Paris Convention and TRIPS Agreement, a trademark confers into its owner exclusive rights to utilize the mark in relation to designated products or services.

JLRJS Journal of Legal Research and Juridical Sciences

It enables the owner to prohibit the unlawful utilisation of identical or deceptively similar marks by others, which could mislead consumers or undermine the brand's image.[5] A trademark must possess distinctiveness (the ability to differentiate the goods/services of one entity from those of another) and non-deceptiveness (it should not mislead consumers regarding the nature, quality, or origin of goods/services). [6]Trademarks may be registered for legal protection, granting the owner statutory rights to enforce their mark and pursue remedies in instances of infringement. Unregistered trademarks possess specific rights under the common law idea of passing off, safeguarding the goodwill linked to the mark.
In legal circumstances, a trademark is delineated and safeguarded to promote equitable competition, avert customer confusion, and protect the intellectual property rights of enterprises.[7] Every single web page has its own unique address, which not only provides a visual representation of the company's identity but also distinguishes it from other businesses

[5] Ashwani Kr. Bansal, *Trademark Law in the Cyberspace: Domain Names and Trademark Conflicts*, 45 JILI 77, 80 (2003).
[6] V.K. Unni, *Protection of Domain Names under Trademark Law: Indian and International Perspective*, 50 JILI 65, 68 (2008).
[7] Pavan Duggal, *Cybersquatting and the Indian Trademark Law*, 56 JILI 198, 201 (2013)

operating in the same industry. It is no longer necessary for users of the Internet to type lengthy IP addresses in binary format because domain names make it easier for them to remember, recognise, and access websites via the Internet.[8] The term "domain name" refers to a unique identifier for a website and is composed of three different components. The initial section, which is known as the third-level domain, is comprised of the letter "www," which indicates that the website is connected to the World Wide Web and may be accessed through internet search engines. In most cases, the second component is referred to as the second-level domain name. This component encompasses the distinguishing name of the company, such as "Facebook," and is considered to be the most important component. [9]The final part is known as the top-level domain name, and it can be composed of a variety of categories, including generic code, country code, special top-level domain names, or restricted usage domain names. The acronyms ".in" for India and ".jp" for Japan are examples of country codes that are used to identify certain nations.

When a company chooses generic domain names, such as ".com," ".org," or ".edu," it indicates that it is not deploying its domain name to a particular category of organisation. This type of deployment is overseen by the Internet Corporation for Assigned Names and Numbers, which is more often known as ICANN.

Examples of top-level domain names that are considered to be specialised include ".legal" and ".app." In spite of what their designation suggests, restricted top-level domain names, such as ".arpa" and ".biz," are not available to everyone.

When it comes to domain names of this kind, the allocation technique varies from one instance to the next. It is possible that the allocation may take place on a first-come, first-served basis, or that a company that has documented business interests would be given priority when it comes to obtaining a domain name that corresponds to its business name.[10] As the landscape of e-commerce continues to evolve, domain name systems continue to retain a significant amount of importance, and the disputes that they cause are nearly unlimited because of this, it is necessary to establish a regulatory authority that is specifically designated because the domain name plays such an important part in determining the origins of a product, it is

[8] Akhil Prasad, *Domain Name System: The Interface with Trademark Law*, 55 JILI 234, 239 (2011).
[9] Manisha Singh & Varun Sharma, *Domain Names and Cyber-Squatting: A New Arena in Trademark Law*, 22 Delhi L. Rev. 167, 169 (2000).
[10] Ashwani Kr. Bansal, *Trademark Law in the Cyberspace: Domain Names and Trademark Conflicts*, 45 JILI 77, 80 (2003).

imperative that it be treated with the same level of significance as a trademark in terms of legal protection and recognition. Failure to do so could lead to trademark infringement.[11] Products can be uniquely identified through the use of trademarks, which have also developed into a way of digital branding for a great number of businesses throughout the world. For the purpose of attracting more users to their websites, businesses sometimes combine two languages, a variety of typefaces, and colour schemes in order to create elaborate and distinctive domain names. These domain names serve as an essential tool for communication in the context of economic transactions. [12]It is possible for two people from different countries to own a single trademark for a product or service in the physical world. On the other hand, in the digital world, a domain name is solely owned by one person and can be used to represent not just a single product or service but also an entire company that is involved in a wide variety of products and services.

## 1.2 DOMAIN NAMES AND THEIR SIGNIFICANCE

Domain names are crucial as they represent the initial step in establishing a website. [13] A domain name serves as the web address that individuals utilise to locate your site. For instance, if you intend to initiate a fashion blog, you must acquire a domain name that embodies the subject, such as "www.fashionblog.com." Domain names hold significance for several reasons:

JLRJS
Journal of Legal Research and Juridical Sciences

An exceptional domain name enhances brand development and increases recognition among prospective clients. [14] An effective domain name is memorable and conveys the nature of your organization. For instance, "www.amazon.com" is memorable and indicates that the site offers things for sale online. Consequently, individuals seeking products for online purchase are more inclined to recall and access Amazon.

A memorable domain name will enhance website traffic by facilitating easier discovery. Furthermore, an exceptional domain name can enhance your SEO (search engine optimization) initiatives, as it constitutes one of the ranking criteria considered by search engines. With a custom domain name, you may establish personalized email addresses that incorporate

[11] Akhil Prasad, *Domain Name System: The Interface with Trademark Law*, 55 JILI 234, 239 (2011).
[12] S.K. Verma, *Intellectual Property Rights in Cyberspace: Trademark Issues*, in V.K. Ahuja (ed.), *Cyber Law: Contemporary Issues and Challenges* 97 (Oxford Univ. Press, 2009).
[13] Arpita Kapoor, *The Intersection of Domain Names and Trademarks: Judicial Trends in India*, in S.K. Verma (ed.), *Law and Technology* 155, 158 (LexisNexis, 2013).
[14] P. Mehta, *The Global Evolution of Domain Name Disputes: Implications for India*, 11 Journal of Intellectual Property Law & Practice 567, 570 (2016).

your domain[15]. This appears significantly more professional than utilizing a complimentary email provider such as Gmail or Yahoo. For instance, if your domain name is "www.fashionblog.com," you may establish an email address like "info@fashionblog.com." This fosters confidence with prospective clients and demonstrates your professionalism as a business.

Domain names are crucial since they facilitate the discovery of your website by users[16]. For instance, Google's domain is google.com. Without a domain name, individuals would encounter challenges in locating your website. Establishing a store in a mall without signage would impede potential customers from locating it.

### 1.3 DOMAIN NAME AND CYBER-SQUATTING

The connection between cybersquatting and domain names is around the illegal registration and misuse of domain names with the intention of utilizing trademark-related intellectual property rights. [17]In order to capitalise on the positive associations people have with a registered trademark or a popular brand, some people register, trade, or use domain names that are either identical to or confusingly close to those marks. This practice is known as cybersquatting. This behaviour is seen as an infringement on trademark rights and has the potential to confuse consumers or dilute the brand.[18]

JLRJS Journal of Legal Research and Juridical Sciences

Cybersquatting is considered trademark infringement in the eyes of the law when someone uses a domain name in a way that makes customers wonder where the goods or services are coming from, gives the impression of affiliation or endorsement when none exists, or tries to blackmail the legitimate owner of the trademark by offering to sell the domain for too much money. These regulations are in place to prevent the public from being misled or to violate the rights of trademark owners.

#### Legal Definition of Cyber Squatting

In India, the principal legislation addressing cybersquatting is the Trademarks Act of 1999 and the Information Technology Act of 2000. Nevertheless, the legislation includes some

[15] Manisha Sinha, *Domain Names and Trademark Law: A Comparative Study*, 12 JIPR 18, 21 (2007).
[16] Dr. K. Shivashankar, *The Role of ICANN in Domain Name Management*, in Manoj Kumar (ed.), *Internet Governance and Legal Perspectives* 89, 91 (Eastern Law House, 2012).
[17] yoti Pandey, *The Legal Dimensions of Cybersquatting in India*, 52 JILI 147, 150 (2010).
[18] K.N. Chaudhary, *Domain Name Disputes and Intellectual Property Rights*, in S.K. Verma & Raman Mittal (eds.), *Legal Dimensions of Cyber Space* 115 (Indian Law Institute, 2004).

ambiguous sections and omissions, which diminish its efficacy in addressing situations related to cybersquatting. India presently has a dedicated legislative framework addressing this issue, unlike several other countries, including the United States, which has explicit laws, such as the Anti-cybersquatting Consumer Protection Act (ACPA), to combat cybersquatting.

Trademark owners encounter considerable risk from cybersquatting, which can lead to substantial financial losses, reputational harm, and diminished consumer trust. In the case of Tata Sons Ltd. v. Manu Kosudi & Ors, the defendants registered several domain names incorporating the renowned trademark "TATA." The Delhi High Court, in its ruling favouring Tata Sons, considered the defendant's malevolent intent to unlawfully benefit from the registered goodwill of the Tata trademark.

In the lack of a definitive legislative framework, the sole legal remedy to address cybersquatting in India is via interpretations and precedents. Ian J. Lloyd, Information Technology Law 257 (7th ed., Oxford University Press, 2014). With the progression of the digital era, the demand for comprehensive, holistic, and contextually pertinent legislation regarding cybersquatting is becoming increasingly urgent. The legal framework and precedents established by Indian courts concerning cybersquatting will be examined in the subsequent sections. A.K. Koul, "Cybersquatting: Legal Implications and Challenges," 45 JILI 82, 85 (2003). Although cybersquatting may initially seem to be a technological or financial issue, it is fundamentally a crucial aspect of intellectual property rights by safeguarding these rights in the digital domain.

JLRJS Journal of Legal Research and Juridical Sciences

India has the ability to cultivate an environment that is conducive to innovation, competition and the growth of digital technology.

**Cyber Squatting Through Advertising**

Cybersquatting[19] via advertising transpires when individuals or entities register domain names that are identical or deceptively similar to established trademarks or brand names, intending to profit from the resulting confusion.

Cybersquatters generally derive income from advertising strategies such as pay-per-click

[19] Sivakumar Reddy, *Cybersquatting and the Domain Name Dispute Mechanism: A Legal Perspective*, 2 SCC J 17, 21 (2010).

(PPC) advertisements or affiliate marketing. [20]Cybersquatters exploit user uncertainty, particularly through typographical errors or minor modifications in domain names (such as incorporating a descriptive term or utilising an alternative top-level domain), to redirect internet traffic intended for legitimate enterprises. When visitors arrive at these deceptive sites, they may inadvertently click on the advertisements, generating revenue for the cybersquatter.

This technique adversely affects legitimate trademark owners by redirecting traffic and potential customers away from their official websites, resulting in diminished revenue and brand dilution.

Furthermore, consumers who inadvertently access these sites may link the substandard or irrelevant material on the cybersquatter's page to the real brand, thus tarnishing the company's reputation.

[21]Notwithstanding legal structures like the Uniform Domain Name Dispute Resolution Policy (UDRP) and statutes such as the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA) aimed at mitigating these problems, cybersquatters persist in using advertising networks and privacy safeguards for profit. Enforcement is complicated by evasion strategies, including concealing registrant identities using privacy services or rapidly re-registering domains under alternate names. Thus, although legal frameworks are in place, cybersquatting via advertising continues to be a persistent and expanding issue in the digital realm.[22]

Cybersquatting employs advertising by utilising deceptive domain names to earn income through diverse advertising strategies, including pay-per-click (PPC) and affiliate marketing. Cybersquatters acquire domain names that closely resemble established companies or trademarks, aiming to divert traffic from individuals who inadvertently access their websites. These visitors may enter a slightly misspelt variant of the brand's URL or a similar name, directing them to the cybersquatter's site instead of the authentic one.

Upon arriving at the cybersquatter's website, it is generally inundated with advertisements, frequently presented via advertising networks such as Google AdSense or other platforms.

[20] Madhavi Divan, *Facilitating Brand Hijacking through Cybersquatting: A Legal Analysis*, 45 JILI 85, 90 (2003).
[21] Manish Kumar, *The Impact of Cybersquatting on E-Commerce and Advertising*, in P. Ishwara Bhat (ed.), *Law and Social Transformation* 195 (Eastern Book Company, 1st ed., 2009).
[22] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 135 (HarperCollins, 2018).

These advertisements may pertain to a specific brand or alternative competitive products.[23] Whenever a user clicks on an advertisement, the cybersquatter generates income via PPC models, capitalising on the ambiguity and misdirected traffic. Occasionally, the advertisements may direct visitors to further misleading or detrimental websites, further taking advantage of individuals who believe they are interacting with a reputable company.[24] Cybersquatters frequently seek to optimize traffic without offering substantive content or services, depending solely on advertising for money. This monetization approach undermines the legitimate brand by redirecting potential customers and traffic, while also eroding user trust and damaging the business's reputation if people link their experience to the authentic brand. Notwithstanding legal frameworks such as the UDRP and ACPA, these behaviours persist as a prevalent and formidable challenge in the digital realm.

**Cyber Squatting on Social Media Websites**

Cybersquatting on social media platforms, commonly known as username squatting or handle squatting, entails the illicit registration or utilization of a social media username or account that closely resembles a prominent brand, celebrity, or public person. Similar to conventional cybersquatting involving domain names, the objective is to capitalize on the reputation of the trademark owner or a prominent individual by selling the username, deceiving users, or making income through fraudulent endorsements, phishing, or misleading information.[25] The Mechanisms of Cybersquatting on Social Media- During the initial phases of a platform's introduction, or while a brand or prominent figure is in the process of creating its online presence, cybersquatters promptly register usernames that replicate well-known trademarks, corporations, or individuals. These handles (or usernames) are thereafter kept hostage, with cybersquatters demanding compensation for their transfer to the legitimate owner. Occasionally, the squatter may disseminate content that emulates the brand's official messaging, deceiving followers into believing it is a legitimate account, or exploit the account for illicit purposes such as phishing schemes, selling counterfeit products, or endorsing deceptive advertising links.

This technique can substantially undermine genuine brands and prominent individuals,

[23] P. Narayanan, *Trade Marks and Passing Off* 224 (6th ed., Eastern Law House, 2004).
[24] Upendra Baxi, *Internet, Intellectual Property and Cybersquatting*, in V. Gopalakrishnan (ed.), *The Future of Intellectual Property Law* 210 (LexisNexis, 2017).
[25] Anupam Chander, *The New Cyberlaw Framework for Social Media and Domain Names*, in P. Bhattacharya (ed.), *Law and Technology: Emerging Issues* 45 (LexisNexis, 2nd ed., 2020).

resulting in consumer confusion, reputational harm, and diminished trust in official channels[26]. Customers may follow a counterfeit brand account, resulting in the dissemination of misleading information or exposure to scams. Furthermore, when cybersquatters utilize these handles to disseminate spam, harmful material, or deceptive advertising, the authentic brand or individual may be erroneously linked to such activities.

Legal and Platform Responses on Social Media Sites - In contrast to conventional cybersquatting, which may be mitigated by laws such as the Uniform Domain Name Dispute Resolution Policy (UDRP), social media sites implement their own terms of service to counter username squatting. Prominent social media platforms such as Twitter, Instagram, and Facebook implement measures to prevent or address squatting concerns. These policies enable organizations and people to submit complaints or request the release of usernames that violate their trademarks or identities.

The efficacy of these policies differs among platforms, and in certain instances, conflict resolution may be protracted[27]. Trademark holders or prominent people generally must give evidence of their identification and rights to the name, after which the platform will evaluate the case to ascertain if the handle is being misappropriated. Certain instances of cybersquatting on social media may be remedied under trademark legislation, permitting the legitimate owner to pursue legal recourse if the username is exploited in bad faith for profit or to mislead the public.

JLRJS
Journal of Legal Research and Juridical Sciences

## 1.4 CONTEMPORARY CHALLENGES TO DOMAIN NAME PROTECTION IN INDIA

India has had numerous episodes of cyber-squatting historically; nevertheless, the remarkable expansion of digital media and the internet has resulted in an increase in recent occurrences of cyber-squatting.

S. Basheer, Protection of Domain Names in India: Issues and Challenges, 45 JILI 89, 93 (2003). Currently, India lacks laws that particularly tackle domain name disputes, including policies on cyber-squatting. The Indian Trademarks Act, of 1999 lacks explicit protections safeguarding

[26] Tushar Chaturvedi, *Cyber Crimes and Social Media: The Growing Threat of Cybersquatting*, 47 JILI 321, 325 (2022).
[27] Vinod Surana, *The Battle Against Cybersquatters on Social Media: Legal Remedies in India*, 33 Company Law Journal (CLJ) 127, 129 (2020).

domain names from infringing upon trademark rights. Moreover, the statute lacks extraterritorial jurisdiction, thereby failing to offer sufficient protection against violations occurring beyond Indian territory. The stipulations of the Information Technology Act of 2000 are insufficient to address domain name disputes related to trademark infringement and to curtail the practice of cyber-squatting.

The courts in India have vigorously addressed cases of cyber-squatting under the provisions of the passing of the Act. The doctrine of passing off is a tort under common law that has been refined by esteemed courts for application in domain name disputes. This conclusion might be inferred from the ruling in the matter of [Satyam Infoway Ltd. v. Siffynet Solutions Pvt. Ltd., AIR 2004 SC 35 40]. Satyam Infoway Ltd. versus Sifynet Solutions (P) Ltd. The Supreme Court of India asserted that, although there is no specific legislation governing domain name disputes and the Trademarks Act, 1999 is inadequate due to its lack of extraterritorial applicability, domain names in India are protected under the laws concerning passing off to the fullest extent possible.

One of the things that a passing-off action does is to prevent the respondent from misrepresenting their goods or services to the general public as being those of the complainant. This is accomplished by prohibiting the defendant from using the complainant's name or trademark. A complaint is filed in order to protect the public from fraudulent activities and to maintain the goodwill of the person who filed the complaint.

JLRJS Journal of Legal Research and Juridical Sciences

Further elucidation of the significance of this concept may be obtained by examining a number of important instances that have been decided by the Indian courts about this matter: [28]Yahoo! Inc. v. Akash Arora & Anr. was the first case to be filed in India addressing cyber-squatting. This case was filed in January of 1999. It was the plaintiff who was in possession of the well-known trademark "Yahoo!" as well as the domain name "Yahoo.com." The defendants, on the other hand, registered a domain name that is as confusingly similar to or identical to "YahooIndia.com," with a style and colour scheme that are comparable to those of the plaintiff, and they offered services that were comparable to those of the plaintiff.

Through the application of the statute of passing off, the Delhi High Court made it impossible for the defendants to make use of the domain name that was assigned to them. The court decided in favour of the plaintiff, concluding that the defendant's domain name was

[28] Yahoo! Inc. v. Akash Arora, 78 (1999) DLT 285 (Del.).

misleadingly similar, likely to confuse the general public and abuse the reputation of Yahoo Inc. The court's decision was favourable to the plaintiff.

However, it has been observed that with the increasing number of domain name disputes, parties have begun using alternative dispute resolution mechanisms such as arbitration and mediation for the purpose of resolving cases relating to cyber-squatting.

This is despite the fact that the Indian Courts have been fairly active in dispensing cases relating to cyber-squatting and providing adequate relief[29]. Parties, for a variety of reasons, choose to resort to the Unfair Discourse Resolution Process (UDRP) given by the World Intellectual Property Organization (WIPO) and other ICANN-approved service providers rather than the formal litigation system offered by the Indian courts.

## 1.5 EXISTING LEGAL FRAMEWORK AND INTERPRETATIONS BY COURTS

**Legal Frameworks**[30]: The current method for tackling cybersquatting concerns in India is dependent on the interpretation of the Information Technology Act and the Trademark Act. This is because there are no particular statutory measures already in place. Certain measures are included in the Trademark Act that are intended to indirectly address cybersquatting. These provisions are primarily concerned with trademark infringement and passing off.

The illegal use of a registered trademark or a mark that is similar to a registered trademark in a manner that is likely to produce confusion or deceit is considered to be an act of infringement, according to Section 29 of the Trademark Act.

As a consequence of this, in the area of domain names, it is possible that an individual has committed trademark infringement if they register a domain name that is either identical to a registered trademark or deceptively similar to a trademark[31].

Under the circumstances of the case known as Rediff Communication Ltd. v. Cyberbooth & Anr, the Bombay High Court came to the conclusion that the domain name "Radiff" violated the plaintiff's trademark "Rediff." In addition, the High Court decided that in the field of digital technology, a domain name serves not only as an address but also as an identity of the entity,

[29] Rajiv Dutta, *Legal Protection of Domain Names: The Indian Scenario*, 48 JILI 77, 81 (2006).
[30] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[31] Pavan Duggal, *Cyberlaw: The Indian Perspective* 185 (4th ed., Saakshar Law Publications, 2019).

which brings it into alignment with the concept of a trademark.

There is a large amount of ambiguity and inconsistency in the interpretation of the Trademark Act because it does not contain any clear references to domain names or cybersquatting. 'Use in the course of trade' in the context of digital technology is not precisely defined under the Trademark Act, which results in interpretations that are open to interpretation.

It is possible that the provisions of the Information Technology Act, specifically Section 43 and Section 66, which cover unlawful access to computer systems and damage to data, respectively, could be applicable in situations involving cybersquatting. Nonetheless, these policies were largely established to tackle cybercrimes like as hacking, data theft, and virus attacks, thereby reducing their usefulness in cybersquatting situations.

**Interpretation by The Courts:** In order to handle the issue of cybersquatting, the courts in India have applied basic concepts of common law, specifically passing off.

In the case of Yahoo Inc. v. Akash Arora & Anr[32], the court came to the conclusion that the use of a domain name that is confusingly similar to the trademark of the plaintiff could result in passing off. The court ruled that a domain name is more than just an internet address; it also serves as a means of identifying a corporation, and as such, it is entitled to protection under trademark law.

In recent times, the judicial system has been making efforts to broaden the scope of protection enjoyed by trademark law in situations involving cybersquatting.

In the matter of Sholay Media Entertainment & Anr v. Yogesh Patel and Others, the defendant intentionally registered domain names that included the well-known brand "Sholay" with the intention of capitalizing on the goodwill that is associated with the trademark. The court did not agree with the defendant's claim that film titles are not protected and instead ruled in favour of the complainant, who claimed that "Sholay" is a well-known trademark. Although there has been an evolution of existing statutory provisions and court interpretations that offer some relief, these laws and interpretations do not fully address the entire resolution of cybersquatting. As a consequence of the absence of a particular legislative framework, the solutions that are implemented are fragmented and insufficient, and they do not adequately address the

[32] Yahoo! Inc. v. Akash Arora, 78 (1999) DLT 285 (Del.).

fundamental issue.

## 2.1 EVOLUTION OF DOMAIN NAME AND CYBERSQUATTING

### Early Days Of Domain Name (1980s- 1990s)

The concept of domain names emerged alongside the growth of the internet[33]. Initially, domain registration was a straightforward process, and many early internet users registered names without much thought about trademark implications. As businesses began to recognize the importance of an online presence, the demand for domain names surged.

During the initial period of domain names, spanning the 1980s to the 1990s, the internet served predominantly as a resource for academic and governmental research, with the notion of domain names arising to facilitate the simplification of intricate numerical IP addresses utilized for computer identification within the network.

In 1983, Paul Mockapetris created the Domain Name System (DNS), enabling the use of easily recognizable names such as "example.com" in place of numerical sequences. The inaugural domain name, symbolics.com, was registered in 1985.

During this time, domain names were mostly utilized by colleges, governmental entities, and technological corporations. [34]The business utilization of the Internet commenced its expansion in the 1990s following the National Science Foundation's removal of prohibitions on commercial use in 1991. This resulted in the registration of domain names for commercial purposes. The establishment of Network Solutions, Inc. (NSI) as the first entity for domain name registrations and the emergence of .com domains signified the commencement of the commercial internet era. As organizations and individuals increasingly recognized the significance of possessing a domain name, this era also witnessed the initial occurrences of cybersquatting, as speculators registered domain names associated with prominent brands or personalities, expecting the escalating financial worth of online visibility.

### Emergence Of Cyber Squatting (Mid-1990s)

The rise of cybersquatting in the mid-1990s corresponded with the swift commercialization

[33] Mohan Mehta, *Cyber-Squatting and Its Impact on E-Commerce and Trade Marks*, 62 Journal of Indian Law Institute 108, 110 (2020).
[34] K.C. Subramanian, *Legal Framework on Domain Names and Cybersquatting in India: An Analysis*, 9 Indian Journal of Law and Technology 67, 69 (2013).

and growth of the internet[35]. As enterprises and individuals acknowledged the significance of an online presence, domain names transformed into valuable digital assets. Cybersquatters exploited this situation by registering domain names that are identical or similar to established trademarks, corporate identities, or renowned personalities, intending to sell them at inflated prices or capitalize on the brand's popularity for profit.

Trademark owner frequently incurs high costs to recover their domains because of the absence of effective legal mechanisms to deter such practices. [36]The proliferation of cybersquatting resulted in considerable legal challenges, ultimately leading to the enactment of legislation such as the Anti-Cybersquatting Consumer Protection Act (ACPA) in 1999 in the United States, as well as the establishment of dispute resolution mechanisms like the Uniform Domain-Name Dispute-Resolution Policy (UDRP) by ICANN, which offered recourse for trademark proprietors confronting domain name exploitation. This initiated worldwide endeavours to mitigate cybersquatting and safeguard intellectual property on the internet.

By the mid-1990s, opportunistic individuals began registering domain names that mirrored popular trademarks and brand names, aiming to sell these names at inflated prices to the rightful owners[37]. This practice, known as cybersquatting, quickly garnered attention as companies realized the extent of the issue. Notable early cases included the registration of names like "pepsi.com" and "coca-cola.com" by squatters.

JLRJS Journal of Legal Research and Juridical Sciences

## LEGAL FRAMEWORK DEVELOPMENT (LATE 1990s)

In the late 1990s, as cybersquatting proliferated alongside the expansion of the internet, notable advancements in the legal framework were instituted to tackle this issue[38]. The Anti-Cybersquatting Consumer Protection Act (ACPA) was enacted in the United States in 1999, representing a significant advancement in the fight against cybersquatting. The ACPA granted trademark holders a legal recourse to target anyone who registered, utilized, or sold domain names with malicious intent to exploit their established businesses, facilitating lawsuits and

[35] Raju Sharma, *Cyber Squatting: The Domain Name Dispute and Indian Legal Framework*, 49 Indian Bar Review 17, 23 (2021).
[36] Michael Geist, *Domain Names and Internet Governance: A Comparative Study of Country Code Top-Level Domain Policies*, 41 Virginia Journal of International Law 435, 438 (2001).
[37] Satyendra Kumar, *The Evolution of Domain Names and the UDRP Mechanism in India*, 60 Journal of Indian Law Institute 102, 105 (2018).
[38] Praveen Dalal, *Cyber Squatting in India: Legal Perspective*, 15 Journal of Intellectual Property Rights 233, 240 (2010).

potential damages against cybersquatters.

Furthermore, the Internet Corporation for Assigned Names and Numbers (ICANN) established the Uniform Domain-Name Dispute-Resolution Policy (UDRP) in 1999. This international regulation provided a more expedient and economical approach for adjudicating domain name disputes without engaging in protracted legal processes. [39]The UDRP enabled trademark proprietors to reclaim domain names registered in bad faith via arbitration, offering an alternative to legal proceedings. These advancements laid the groundwork for safeguarding intellectual property rights in the digital era and mitigating domain name exploitation.

To address the growing problem of cybersquatting, lawmakers and organizations began to develop legal protections[40]. The **Anticybersquatting Consumer Protection Act (ACPA)** was enacted in the United States in 1999, allowing trademark owners to sue for damages against those who register domain names in bad faith. This marked a significant step in providing legal recourse for companies affected by cybersquatting.

**Introduction Of UDRP (1999)**

In the same year, the Uniform Domain-Name Dispute-Resolution Policy (UDRP) was established by the Internet Corporation for Assigned Names and Numbers (ICANN). The UDRP provided an alternative dispute resolution mechanism for trademark holders, allowing them to resolve domain name disputes more efficiently without going through lengthy court processes. This policy has since been adopted globally and has become a cornerstone of domain name protection.

**Expansion Of Domain Name Registration (2000s)**

As the internet continued to expand, the introduction of new top-level domains (TLDs) and an increasing number of registrars led to a more competitive landscape. This made it easier for cyber squatters to register variations of popular brand names. The proliferation of TLDs also complicated the enforcement of domain name rights.

[39] Gaurav Shrivastava, *Cyber Squatting and Trade Mark Conflicts*, 57 Indian Journal of Law & Technology 32, 35 (2014).
[40] Shubha Ghosh, *Domain Names, Intellectual Property, and Cyber-Squatting: Property, Speech, and Public Policy*, 20 Fordham Intellectual Property, Media & Entertainment Law Journal 199, 201

## 2.2 INTERNATIONAL FRAMEWORK

The global framework regulating domain name disputes primarily addresses conflicts between trademark owners and domain name registrants, particularly in instances of cybersquatting, which involves registering, selling, or utilizing a domain name to profit from another's trademark. The framework comprises several international rules, treaties, and organizations designed to reconcile intellectual property rights with unrestricted Internet usage. The essential elements of this framework comprise:

### Uniform Domain Name Dispute Resolution Policy (UDRP)

The UDRP, overseen by the Internet Corporation for Assigned Names and Numbers (ICANN), serves as the principal worldwide framework for adjudicating disputes concerning generic top-level domains (gTLDs), including .com, .org, and .net[41].

Extent: The UDRP pertains to instances where a domain name is identical or confusingly similar to a trademark, and the domain was registered and utilized in bad faith. [42]

Essential Criteria: To submit a complaint under UDRP, the complainant must demonstrate that the domain name is identical or confusingly similar to a trademark or service mark in which they possess rights.

JLRJS Journal of Legal Research and Juridical Sciences

The domain registrant possesses no valid interests in the domain name. The domain name has been registered and is being utilized in bad faith.

### WIPO Arbitration and Mediation Center

The Role of WIPO: The World Intellectual Property Organization (WIPO) [43] is a primary source of dispute resolution services for UDRP disputes. Additional entities, including the National Arbitration Forum (NAF), also address UDRP complaints. Result: Dispute resolutions generally lead to the transfer of the domain name to the complainant or its cancellation. The UDRP prohibits the awarding of monetary damages.

The World Intellectual Property Organization (WIPO) is a vital entity within the international

[41] David Lindsay, *International Domain Name Law: ICANN and the UDRP* 213 (Hart Publishing, 1st ed., 2007).
[42] Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, 17(3) Info. Soc'y 151, 153 (2001).
[43] World Intellectual Property Organization (WIPO), *WIPO Overview of WIPO Panel Views on Selected UDRP Questions* 2.0, ¶ 3 (WIPO, 2017).

dispute settlement framework. Besides managing UDRP claims, it also offers arbitration, mediation, and expert determination services for both generic and country-code top-level domains (ccTLDs), contingent upon local legislation[44].

The WIPO has established distinct protocols for addressing domain name disputes, especially in instances of cybersquatting, guaranteeing swift and effective resolution without prolonged litigation.

**Country Code Top-Level Domains (ccTLDs):**

The UDRP pertains to gTLDs, whereas WIPO also addresses disputes involving ccTLDs in regions where local domain name authorities have implemented UDRP-like regulations[45]. Numerous country code top-level domains (ccTLDs), such as .uk and .au, possess distinct domain dispute resolution mechanisms, while some choose to adhere to the principles of the Uniform Domain-Name Dispute-Resolution Policy (UDRP).

Dispute Resolution Policies for Country-Code Top-Level Domains (ccTLD) Country code top-level domains (ccTLDs) are domain extensions designated for certain nations (e.g., .uk, .de, .cn), and numerous ccTLD registries have implemented their own dispute resolution processes.

JLRJS Journal of Legal Research and Juridical Sciences

Although certain ccTLDs possess policies akin to the UDRP, a standardized structure regulating ccTLDs does not exist. Each nation may formulate its own regulations, potentially resulting in inconsistency.

**Global Trademark Legislation and Agreements**

International accords are essential for safeguarding trademark rights, frequently central to domain name conflicts. Several significant accords encompass[46]:

The Paris Convention for the Protection of Industrial Property establishes trademark protection across many nations, providing a foundation for domain name holders to defend their rights on an international scale.

[44] S.K. Verma, *Cyber Law and E-Commerce* 189 (Indian Law Institute, 2nd ed., 2003).
[45] Philip S. Corwin, *Balancing the Scales: The UDRP's Flaws and Proposals for Reform*, 67 J. World Intellectual Property 445, 448 (2009).
[46] World Intellectual Property Organization (WIPO), *Introduction to Intellectual Property: Theory and Practice* 120 (Kluwer Law International, 2nd ed., 2004).

TRIPS Agreement (Trade-Related Intellectual Property Rights): The World Trade Organization (WTO) administers TRIPS, which mandates member countries to offer trademark protection, hence indirectly facilitating domain name dispute resolution through the establishment of international trademark enforcement norms.

**Anti-Cybersquatting Consumer Protection Act (ACPA)**

The Anti-Cybersquatting Consumer Protection Act (ACPA) in the United States offers legal remedies for cybersquatting. Although this is a national statute, its ramifications are global, as numerous cybersquatters focus on U.S.-based domains such as .com. Essential Clauses:

The ACPA permits trademark owners to initiate legal action against cybersquatters who register, traffic in, or utilize domain names with malicious intent to exploit another's trademark. It permits courts to mandate the annulment or reassignment of domain names and provides for statutory damages of up to $100,000 per domain name. Although the UDRP is more expedient and cost-effective, the ACPA provides the opportunity for monetary damages, which the UDRP does not permit.

**Prevention of Reverse Domain Name Hijacking**

Reverse Domain Name Hijacking (RDNH) transpires when a trademark owner seeks to unjustly appropriate a domain from a rightful registrant. The UDRP and associated regulations have stipulations to safeguard domain owners from abusive practices. The UDRP stipulates that if a complaint is determined to have acted in bad faith, a claim of reverse domain name hijacking may be asserted, safeguarding the domain owner from the unfair forfeiture of their domain name.

**WHOIS Database and Data Protection Legislation (GDPR)**

The WHOIS database offers public information regarding the registrant of a domain name, essential for adjudicating domain disputes. The implementation of the General Data Protection Regulation (GDPR) in the European Union has limited access to this information to safeguard privacy.

The GDPR's influence on WHOIS restricts access to contact information for domain owners, complicating trademark holders' ability to commence UDRP hearings or pursue legal action

against cybersquatters. This has introduced further issues to the international system, as the data of domain name registrants is less accessible, necessitating new ways to reconcile privacy with dispute resolution requirements.

**Mechanisms for Alternative Dispute Resolution (ADR)**

Alternative Dispute Resolution (ADR) techniques, including arbitration and mediation, are progressively utilized in conjunction with or as substitutes for conventional dispute resolution methods such as litigation or the Uniform Domain-Name Dispute-Resolution Policy (UDRP). The World Intellectual Property Organization provides Alternative Dispute Resolution services to expedite and confidentially resolve conflicts, with mediated solutions typically being more conciliatory and economical.

**ICANN's Registrar Accreditation Agreement (RAA)**

The Registrar Accreditation Agreement (RAA) obligates accredited domain name registrars to adhere to ICANN standards, including compliance with the UDRP. This guarantees that registrars collaborate in securing and transferring disputed domain names upon the issuance of a UDRP verdict.

The RAA mandates that domain registrars adhere to international dispute resolution protocols, thereby offering legal assurance for both domain name registrants and trademark proprietors.

JLRJS Journal of Legal Research and Juridical Sciences

## 2.3 INTERNATIONAL COOPERATION AND CHALLENGES

Collaboration among jurisdictions: International cooperation is essential due to the transnational nature of domain name conflicts. Although ICANN and WIPO offer international frameworks, the implementation of trademark legislation and dispute resolution mechanisms differs across nations.

Emerging Legal Difficulties: With the evolution of the internet, emerging difficulties such as phishing, typosquatting, and blockchain-based domain names (e.g., ENS domains on the Ethereum blockchain) raise legal questions that existing international frameworks may inadequately address. Future revisions to the UDRP and national legislation may be necessary to align with technological advancements.

## 2.4 HOW TO PREVENT CYBERSQUATTING IN THE DIGITAL AGE

To avert domain name and trademark infringement in the digital world, enterprises and individuals had to use various proactive measures[47]:

**Secure Key Domain Names Promptly[48]:** Acquire various domain name alternatives, including diverse top-level domains such as .com, .net, and .org, as well as prevalent misspellings of your brand or trademark to thwart cybersquatters from capitalizing on them.

**Supervise Domain Registrations and Social Media Accounts:** Employ domain monitoring services and social media notifications to identify any new registrations that closely resemble your trademark or brand name, facilitating early identification of any infringements.

**Trademark Registration:** Confirm that your brand name, logo, and other essential assets are formally registered as trademarks in pertinent jurisdictions. This bolsters your legal standing in the event of infringement.

**Employ Legal Instruments[49]:** Leverage frameworks such as the Uniform Domain Name Dispute Resolution Policy (UDRP) or national legislation (such as the Anti-Cybersquatting Consumer Protection Act (ACPA)) to promptly address infringers, including seeking domain transfers or initiating litigation.

JLRJS Journal of Legal Research and Juridical Sciences

**Utilize Brand Protection Services:** Implement specialized tools and services that automate the surveillance and enforcement of your intellectual property rights online, swiftly removing infringing domains or material. Implementing these tactics enables organizations and individuals to significantly reduce the risk of domain name and trademark infringement in the contemporary digital landscape.

## 3.1 CHALLENGES AND LIMITATIONS TO PREVENT CYBER SQUATTING AND DOMAIN NAME PROTECTION

Preventing cybersquatting and safeguarding domain name protection in cyberspace encounters numerous obstacles and constraints, including:

[47] Arvind Datar, *Judicial Approach to Cyber Squatting in India*, 51 JILI 92, 97 (2020).
[48] Arvind Datar, *Judicial Approach to Cyber Squatting in India*, 51 JILI 92, 97 (2020).
[49] Nishith Desai, *Cyber Squatting: Emerging Legal Trends in India*, 57 JILI 73, 78 (2021).

**1. Global nature of the Internet[50]:** The internet possesses an intrinsic global character, characterized by domain names registered across several countries and governments. Legal frameworks vary by country, complicating the enforcement of uniform regulations and the pursuit of legal recourse against cybersquatters operating internationally.

**2. Privacy and Proxy Services:** Numerous cybersquatters utilize privacy and proxy services to conceal their identities, complicating the efforts of trademark holders to trace and identify the individuals responsible for infringing domains. The enactment of privacy legislation such as GDPR has further limited access to WHOIS data, hindering enforcement initiatives.

**3. Financial and Temporal Implications of Legal Proceedings:** Although legal mechanisms like the Uniform Domain Name Dispute Resolution Policy (UDRP) and the Anti-Cybersquatting Consumer Protection Act (ACPA) offer pathways for resolving disputes, engaging in litigation can be costly and protracted, particularly for small enterprises that may not possess the necessary resources to initiate numerous claims.

**4. Expedited Domain Re-registration[51]:** Subsequent to the resolution of a domain dispute, cybersquatters can swiftly re-register a comparable domain utilizing alternative versions or top-level domains (TLDs). This engenders a "whack-a-mole" situation in which trademark proprietors perpetually pursue new violations.

JLRJS Journal of Legal Research and Juridical Sciences

**5. Automated Domain Registration (Domain Tasting):** Certain cybersquatters employ automated methods to register domains en masse or evaluate domains for profitability prior to finalizing their acquisition. This procedure, referred to as "domain tasting," enables individuals to capitalize on lucrative domains while circumventing the expenses associated with permanent registration.

**6. Inconsistent Enforcement by Sites[52]:** Although social media sites and domain registrars possess policies to combat cybersquatting, the enforcement of these policies can be irregular. Platforms may require time to address concerns, or in certain instances, squatters may use loopholes to persist in their operations.

[50] Nishith Desai, *Cyber Squatting: Emerging Legal Trends in India*, 57 JILI 73, 78 (2021).
[51] Satyendra Babu, *Legal Aspects of Cyber Squatting in India* 119 (Central Law Agency, 2016).
[52] S. A. Tiwari, *Prevention of Cybersquatting: A Comparative Analysis of U.S. and Indian Laws*, 46 JILI 81, 85 (2015).

**7. Insufficient Awareness Among Brands[53]:** Numerous enterprises, particularly smaller ones, neglect to secure all pertinent domain name variations, rendering them susceptible to cybersquatting. A deficient comprehension of international domain registration or proactive brand protection methods exacerbates the risk.

**8. Monetization of Infringing Domains:** Cybersquatters can generate revenue via advertising, affiliate marketing, or the sale of counterfeit goods on infringing domains. The prospect of financial profit from these acts motivates them to persist in registering and squatting on domains, despite the possibility of legal repercussions.

## CONCLUSION

Cybersquatting and domain name protection are significant issues in the digital era, as the internet expands and offers new prospects for both legal enterprises and nefarious individuals. Legal instruments such as the Uniform Domain Name Dispute Resolution Policy (UDRP) and national legislation like the Anti-Cybersquatting Consumer Protection Act (ACPA) provide essential resources for trademark owners to address cybersquatting. These procedures allow brand owners to recover infringing domains and safeguard their intellectual property from misuse. Nonetheless, despite these legal remedies, cybersquatting persists, posing continual hurdles for domain name protection.

A principal challenge in adjudicating domain disputes is the internet's worldwide scope and the varying legal norms among governments, which hinder enforcement. Moreover, cybersquatters often employ privacy services to conceal their identity, complicating efforts for trademark owners to identify and pursue action against them. The proliferation of automatic domain registration and the rapidity with which squatters can re-register domains engenders a "whack-a-mole" dilemma, wherein disputes are frequently settled only to resurface in various manifestations.

In conclusion, whereas current legal frameworks offer vital mechanisms for combating cybersquatting, the advancing strategies of squatters and the intrinsic difficulties of the digital environment necessitate ongoing adaptation. To enhance the protection of domain names, enterprises must use proactive strategies, including the early registration of essential domains, vigilant monitoring for infringements, and the application of legal remedies with innovative

[53] Pavan Duggal, *Cyber Law: The Indian Perspective* 135 (4th ed., Saakshar Law Publications, 2020).

technology solutions. Enhancing international collaboration and improving legal frameworks will be essential to addressing these ongoing concerns and guaranteeing effective domain name protection in cyberspace.

JLRJS
Journal of Legal Research and Juridical Sciences