International Journal of Recent Advances in Multidisciplinary Topics
Volume 5, Issue 3, March 2024
https://www.ijramt.com | ISSN (Online): 2582-7839

Cybersquatting: A Comprehensive Analysis of Definition, Facets, and Statistical Trends

Shubham Sanjay Banne*
Student, Post-Graduate Diploma in Intellectual Property Rights, Maharashtra National Law University, Mumbai, India

***Abstract*: Effective regulation is urgently needed to combat the illness known as "cybersquatting," which encourages cyber squatters to prey on vulnerable Domain Name Holders. Cybersquatting is viewed as a menace that has no boundaries given the state of circumstances in the globe today. A lot more has to be done in the Indian legal system to prevent cybersquatting, despite the fact that effective and proactive engagement has been crucial in resolving domain name disputes and setting clear laws in this area, according to several studies. The court must play an effective role by applying the law in a way that best captures the organic essence of the state, rather than relying just on statistics to demonstrate the overall development of any nation's digital infrastructure.**

***Keywords*: Cybersquatting, Domain name squatting, Name-jacking, URL, ICANN, UDRP.**

1. Introduction

Cybersquatting is the practice of maliciously registering, purchasing, or utilizing a domain name. In order to make money off of others, cyber squatters disregard the existence of a trademark. In actuality, the first person to purchase a domain name will get it.

If the business hadn't yet developed a website, a cyber-squatter may purchase brainzz.com with the intention of either using the domain name to drive traffic and make money through advertising, or selling it to brainzz at a later time for a profit. If a business has a good reputation but no website, the company either pays the owner of the domain name to transfer the domain or contact a trademark attorney to start a lawsuit.

The second way is time- and cost-intensive, so trying to buy the domain directly from the cyber squatter is usually the preferred method. Today, opportunities for cyber squatters aren't as common since most businesses make the purchasing of their domain a high priority, especially if they have a strong trademark.

Cybersquatting is defined as registering, trafficking, or using a domain name in bad faith with an intention to profit from the trademark holder's goodwill, as defined by the Anti Cybersquatting Consumer Protection Act, 1999, it is also known as domain squatting. The word comes from the phrase "squatting," which refers to inhabiting an abandoned place or land that is not the squatter's own. Most of the time, the cyber squatter sells the domain name at a premium to the firm or individual who owns the trademark.

2. Aspects of Cybersquatting

A. History of Cybersquatting

"The rising number of alleged cybersquatting cases shows the growing premium placed on domain names by companies and individuals operating in the wired environment" - Francis Gurry

The threat of cybersquatting was raised in the late 1990s when the internet was just becoming a global sensation. Most firms were unconcerned about the commercial and economic potential offered by the internet during this time.

B. Domain Name

A domain name is an Internet resource name that is universally understood by Web servers and online organizations and provides all pertinent destination information.

www.trademarkname.com

- WWW – refers to World Wide Web
- Trademark name - The name that a corporation or an individual chooses for their website, which is usually similar to their trademark and often refers to the company's name
- .com - ".com" is short for "commercial." A site doesn't necessarily have to have a commercial purpose to use. While .in Indicates the country in which the company is based. For instance,' In' designates a corporation based in India; '.ca', on the other hand, alludes to a firm based in Canada.

In India, cases such as "Rediff Communications Ltd v Cyberbooth" have highlighted the importance of a domain name's protection, declaring that "a domain name is more than an internet address and is entitled to the same trademark protection as a brand."

This article critically examines the many types of cybersquatting, as well as the present legal scenario of cybersquatting in India, with relevant examples, instances, and illustrations. In addition, this blog makes recommendations for how the Indian legislature and judiciary should deal with cybersquatting cases.

*Corresponding author: shubhambanne1819@gmail.com

C. Types of Cybersquatting

1) Domain Name Squatting

This is the practice of buying a well-known company's domain name to extort money from the parent firm. In Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd, the respondent obtained the domain names www.siffynet.net and www.siffynet.com, which were confusingly similar to the plaintiff's www.sifynet.com. The Supreme Court held that "Domain names are commercial identifiers, serving to identify and distinguish the firm itself or its goods and services, as well as to define its associated online address".

2) Identity Theft

Domain names are acquired for a fixed period; after which they expire if they are not re-registered. When a domain name expires, a cyber-squatter can use software tools to register it. Alert angling and extension exaggeration are two methods of Domain Name identity theft.

3) Uniform Resource Locator (URL)

Commonly known as Typo squatting. If any typographical errors are made while typing the web URL into the browser, it is forwarded to a substitute website that is utilized by cyber squatters to make money. For instance, Google's typo squatting site Goggle.com installed malware on visitors' computers. The malware displayed pornographic pictures in spam pop-ups and downloaded Spy Sheriff antivirus, which damaged victims' machines.

4) Name-Jacking

In this type of squatting, an individual's name is acquired as a top-level Domain Name.

3. Statistics & Overview

As discussed above from 1999 when act got establish to till date many changes cases occurred which helped to concurrent technical & legislative solutions. So, it is important to take overview of the statistics of Domain Resolution of year 1999 to 2022.

As a research expert in cybersquatting, examining the statistics of domain resolution from 1999 to 2022 reveals intriguing trends. Over this period, there's a noticeable surge in the number of domain ownership changes, particularly in the United States, China, India, and the United Kingdom. In 1999, the landscape was relatively sparse, with only one domain change recorded in the US. However, as the internet became more pervasive, the numbers escalated dramatically. Notably, the United States consistently dominated the scene, showcasing a rapid increase from 949 domain changes in 2000 to a staggering 1351 in 2022. Conversely, India and China exhibited a slower but steady rise, reflecting the growth of their online presence. China, in particular, experienced a significant uptick from 43 domain changes in 2000 to 878 in 2022, indicating its emergence as a key player in the digital realm. Meanwhile, the United Kingdom and India demonstrated fluctuating patterns, influenced by various economic and technological factors. This overview underscores the dynamic nature of cybersquatting activities and highlights the evolving strategies employed by domain owners across different regions.

Also, there is statistics that shows sector wise percentage.

Table 1

Year	NOC in USA	NOC in India	NOC in China	NOC in United Kingdom
1999	1	0	0	0
2000	949	45	43	152
2001	681	16	51	149
2002	425	7	64	132
2003	399	5	76	74
2004	427	7	84	87
2005	547	14	97	125
2006	693	9	88	154
2007	841	22	113	190
2008	838	17	117	175
2009	665	29	168	175
2010	779	30	347	197
2011	786	31	339	178
2012	783	26	501	192
2013	650	29	445	196
2014	670	37	406	202
2015	612	59	412	203
2016	680	34	473	179
2017	758	43	492	185
2018	839	50	466	215
2019	953	32	445	189
2020	1055	36	557	228
2021	1193	66	696	249
2022	1351	82	878	190

Table 2

Sector wise Cybersquatting cases	Percentage
Biotechnology and Pharmaceuticals	9.90%
Banking and Finance	9.40%
Internet and IT	8.80%
Retail	8.10%
Food, Beverages and Restaurants	7.20%
Entertainment	6.50%
Media and Publishing	6.30%
Fashion	6.00%
Hotels and Travel	6.00%
Other	5.30%
Telecom	4.90%
Automobiles	4.40%
Electronics	4.30%
Heavy Industry and Machinery	3.90%
Transportation	3.30%
Sports	2.50%
Insurance	1.80%
Luxury Items	1.70%

Research on cybersquatting trends across various sectors reveals intriguing insights into the prevalence and distribution of such cases. Biotechnology and Pharmaceuticals emerge as the most targeted sector, constituting 9.90% of cybersquatting instances. This sector's vulnerability likely stems from the valuable intellectual property and branding associated with pharmaceutical companies. Following closely behind, Banking and Finance accounts for 9.40% of cybersquatting cases, reflecting the attractiveness of financial institutions as targets for fraudulent activities. Internet and IT companies also face significant threats, with 8.80% of cases directed towards them, underscoring the inherent risks within the digital realm. Retail and Food, Beverages, and Restaurants sectors follow suit, with 8.10% and 7.20% respectively, indicating the broad spectrum of industries affected by cybersquatting. Notably, sectors such as Luxury Items and Insurance experience comparatively fewer incidents, standing at 1.70% and 1.80%, highlighting potential variations in cybercriminals' preferences and strategies. Understanding these sector-wise patterns is crucial for devising

targeted countermeasures to mitigate the impact of cybersquatting across diverse industries.

4. Indian Legal Scenario

The World Wrestling Federation (WWF) sued a Californian individual for registering the domain name "wordwrestlingfederation.com" and offering to sell it to WWF at an inflated price, in the first known case of cybersquatting. The World Intellectual Property Organization (WIPO) decided that the registered domain name was identical to the WWF brand and could cause confusion. The resident was also urged to transfer his or her registration to WWF.

The Anti Cybersquatting Consumer Protection Act of 1999 governs incidents of cybersquatting in the United States. There is presently no legislation in effect in India that addresses or addresses the issue of cybersquatting. In Satyam Info Way Ltd v Sifynet Solutions, the court recognized the lack of legislation in India for cybersquatting dispute settlement. The Indian judiciary, on the other hand, has been proactive in providing remedies in domain name infringement cases.

1. In the case of Yahoo! Inc. v Akash Arora and Anr, where the respondents were using the domain name "yahooindia.com," which was identical to the plaintiff's trademark "Yahoo," one of the most significant verdicts on trademark passing off through domain names were handed down. The respondents, on the other hand, claimed that the services offered did not meet the definition of goods under the Indian Trademark Act. Yahoo, on the other hand, was granted an injunction since web services are regarded as goods worldwide.
2. In the case of Reddif Communication Limited v Cyberbooth and Anr, the respondent had registered the domain name "radiff.com," which was identical to the plaintiff's domain name "reddif.com." The court recognized the domain name as a registered trademark. In this case, the court ruled in favor of the petitioner, finding that a domain name is a valuable company asset.
3. Following in the footsteps of WIPO in the Reddif case and SBI Cards Vs Domain Active Property Ltd, Indian courts have ordered the infringing party to surrender the domain name to the original trademark owners. Tata Sons Ltd. V Mr. Manu Kishori is one of the most notable cases for this, in which the defendant had a domain name registered in the plaintiff's name and was compelled to surrender the name to the plaintiff.

5. Indian Dispute Resolution Policy in India

The Internet Corporation for Assigned Names and Numbers (ICANN) established the Uniform Domain Name Dispute Resolution Policy (UDRP) to resolve disputes over the registration of internet domain names. Further, as India is a signatory to the World Intellectual Property Organization (WIPO), it is required to follow the UDRP process. As a result, India has developed an Indian Domain Name Dispute Resolution Policy (INDRP) with UDRP-compliant standards. INDRP has several provisions that are comparable to UDRP. The following are some of the salient qualities of the same:

- Appointment of arbitrator for disputes regarding domain names.
- Conduction of Arbitration proceedings should be according to the provisions of the Arbitration and Conciliation Act, 1996.
- The Arbitrator in the caseshould pass a reasonable award within 60 days from commencement of arbitration proceedings.
- Arbitrator shall give reasons for the award.

The case of YouTube LLC v. Rohit Kohli, in which the respondent registered the domain name "www.youtube.co.in," was a notable one brought under the INDRP's purview. The trademark in the domain name belongs to a corporation called "YouTube." The Board found that the domain name was phonetically and conceptually similar to the complainant's trademark and hence granted the domain name transfer to the trademark's original owner.

In addition, a few clauses of the Information Technology Act of 2000 and the Indian Penal Code of 1860 may apply in the event of cybersquatting in India. The following are some such provisions:

1. Forgery under Section 469 of the IPC: A person found forging with the intent to harm the reputation of any party, or knowing that the document forged will be used for that purpose, shall be punished with imprisonment of either description for a term that may extend to three years, as well as a fine.
2. Section 66 of the Information Technology Act of 1999: Under this provision, any person who commits any act referred to in section 43 dishonestly or fraudulently is punishable by imprisonment for a term up to three years, a fine up to five lakh rupees, or both.
3. Section 66A: This clause punishes anyone who uses a computer resource or communication device to convey "grossly offensive" or "menacing" material.

6. Discussion

In the realm of intellectual property rights (IPR), cybersquatting emerges as a complex issue encapsulating varied challenges and legal intricacies. Cybersquatting, succinctly defined as the unauthorized registration, trafficking, or utilization of a domain name to capitalize on the reputation and goodwill associated with another entity's trademark, permeates global jurisdictions with its repercussions. Research findings underscore the pervasive nature of cybersquatting, with studies indicating a significant increase in domain disputes over the years, especially in burgeoning digital economies like India and China.

Delving into the Indian legal milieu, it's apparent that while specific legislation dedicated to cybersquatting remains absent, the judiciary has exhibited proactive intervention in addressing disputes. Research indicates a growing trend of courts invoking

trademark laws and principles of unfair competition to provide remedies to aggrieved parties. This judicial stance underscores India's commitment to upholding intellectual property rights and fostering a conducive environment for online commerce.

Furthermore, scholarly studies shed light on the challenges posed by cybersquatting in the Indian context, particularly concerning the enforcement of judgments and the identification of perpetrators operating across international borders. Such research underscores the need for enhanced cooperation between law enforcement agencies and internet governance bodies to effectively combat cybersquatting.

The introduction of the Indian Domain Name Dispute Resolution Policy (INDRP) mirrors India's alignment with international standards, notably the Uniform Domain Name Dispute Resolution Policy (UDRP), in combating cybersquatting through structured arbitration mechanisms. This proactive stance exemplifies India's evolving legal landscape, adapting to the nuances of cyberspace and its attendant challenges.

Moreover, research highlights the efficacy of alternative dispute resolution mechanisms, such as mediation and arbitration, in resolving cybersquatting disputes swiftly and cost-effectively. Collaborative efforts between stakeholders, including trademark owners, domain registrars, and internet service providers, are essential in developing comprehensive strategies to mitigate cybersquatting risks.

Legislative provisions within the Information Technology Act of 2000 and the Indian Penal Code of 1860 furnish additional avenues for addressing cybersquatting activities. However, research suggests the need for periodic review and updates to existing laws to keep pace with evolving cyber threats and technological advancements. In concert with global trends, India continues to refine its approach to cybersquatting, leveraging a convergence of legal frameworks, judicial activism, and international cooperation. Through such concerted efforts, India endeavors to uphold the sanctity of intellectual property rights, foster innovation, and fortify its digital ecosystem against illicit practices, thus contributing to a more secure and equitable online environment.

References

[1] Look, J. J. (1999). The Virtual Wild, Wild West (www): Intellectual Property Issues in Cyberspace—Trademarks, Service Marks, Copyrights, and Domain Names. In the University of Arkansas at Little Rock Law Review, vol. 22, pp. 64, Arkansas: School of Law

[2] Radack, D. V. (1998). Understanding Some Ground Rules in Internet Domain Name Disputes. Journal J.O.M., 50(1).

[3] https://www.upcounsel.com/cybersquatting

[4] https://www.khuranaandkhurana.com/

[5] https://www.wipo.int/amc/en/domains/statistics/