INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERSQUATTING: HOW IT FOUL PLAYS THE SOCIETY

AUTHORED BY - KANIKA CHANDAK
& PROF. SHIVANGI SINHA

ABSTRACT

Cybersquatting, also known as domain squatting, is the unethical practice of registering, trafficking in, or using a domain name with the intent of profiting from the goodwill of a trademark belonging to someone else. This deceptive practice can lead to confusion and financial harm for both businesses and consumers and dilute the brand value. This paper will provide an overview of cybersquatting, including its types, aspects, and legal measures taken to combat it, this includes providing resources and guidelines for businesses and individuals to understand their rights and take proactive measures to protect their trademarks in the online space. Additionally, it will discuss the role of domain name dispute resolution mechanisms and international efforts like Uniform Domain Name Dispute Resolution (UDRP) administered by the World Intellectual Property Organization (WIPO) and organization like ICANN to prevent and address cybersquatting in the contemporary digital landscape as collaboration between legal entities and international organizations also involves promoting education and awareness about cybersquatting and its impact on trademark rights.

KEYWORDS: Cybersquatting, domain name, trademark, intellectual property.

INTRODUCTION

With the rapid advancement in technology and the increasing interconnectedness of our digital world, cybercrime has become a significant global threat. It encompasses a wide range of illegal activities, including hacking, identity theft, phishing, malware attacks, online scams, and much more for financial gain to political activism, espionage, or simply causing mayhem and chaos.

Out of all, one of the cybercrime is Cybersquatting. It is a practice in which individuals or entities register internet domain names that are trademarked by others with the intention of profiting from

ISSN: 2582-6433

them or damaging the reputation of the brand. Cyber squatters often use these domain names to redirect traffic to their websites for commercial gain through pay-per-click advertising, phishing scams, or other illicit activities. The practice has become increasingly prevalent in recent years, as the internet has become a critical platform for business and commerce and thus, poses significant challenges to trademark owners, businesses, and individuals seeking to protect their online identities and intellectual property.

TYPES OF CYBERSQUATTING

1. **Typo squatting**

It is also known as URL hijacking, is a form of cybersquatting that involves registering domain names similar to popular or commonly accessed websites in order to redirect traffic to other websites, potentially for malicious purposes such as spreading malware, phishing, or capturing user data. This practice takes advantage of typographical errors or misspellings made by users when typing website URLs into their browser.

2. **Identity theft**

It occurs when someone wrongfully obtains and uses another individual's personal information, such as their name, Social Security number, credit card information, or other identifying details, for fraudulent purposes. This can include opening unauthorized credit accounts, making purchases, or conducting other financial transactions in the victim's name, causing significant harm to their financial and personal well-being. Identity theft is a serious crime and can have long-lasting effects on the victim's credit history and financial stability.

3. **Name Jacking**

It typically refers to the act of registering internet domain names that are similar to established brand names, famous individuals, or popular products. This practice can lead to confusion among consumers and can be used for various purposes, such as selling the domain name to the legitimate owner at an inflated price, diverting web traffic intended for the legitimate site to a different site, or tarnishing the reputation of the targeted brand or individual. Name jacking can potentially infringe upon trademarks and intellectual property rights.

4. **Reverse Cybersquatting**

It refers to the situation in which a trademark owner is wrongly accused of cybersquatting by an

ISSN: 2582-6433

individual or entity that has a generic or descriptive domain name that happens to match the trademark. The trademark owner may attempt to claim the domain name through legal or aggressive means, accusing the domain owner of cybersquatting, when in fact the domain owner registered the domain for legitimate reasons. This concept represents a role reversal of the typical cybersquatting scenario, where the accused domain owner is not in fact engaged in bad faith registration or use of the domain.

ASPECTS OF CYBERSQUATTING

Cybersquatting encompasses several aspects that contribute to its nature and impact. Here are some of the key aspects of cybersquatting:

1. **Domain name infringement**: Cybersquatting involves the registration of domain names that are identical or confusingly similar to existing trademarks or well-known brand names. This infringes upon the intellectual property rights of legitimate trademark owners and can cause confusion among internet users.

2. **Unauthorized profit**: Cyber squatters often aim to profit from the domain names they register by engaging in activities such as pay-per-click advertising, selling the domain names at inflated prices, or using them for fraudulent purposes. They take advantage of the value and reputation associated with established brands.

3. **Brand dilution and dilution of reputation**: By registering domain names that are similar to established brands, cyber squatters can tarnish the reputation and dilute the distinctive nature of the original trademark. This can lead to loss of consumer trust and negatively impact the brand's image.

4. **Missed business opportunities**: Cybersquatting can prevent legitimate trademark owners from utilizing their brand name effectively online. This may result in missed business opportunities, loss of web traffic, and reduced online presence.

5. **Legal implications**: Cybersquatting is considered illegal in many jurisdictions and is subject to various laws and regulations. Trademark owners can take legal action against cyber squatters to protect their rights and seek remedies, such as domain name recovery, damages, and injunctions.

ISSN: 2582-6433

6. **International ramifications**: Cybersquatting is a global issue, and the internet's borderless nature makes it challenging to enforce trademark rights consistently across different jurisdictions. This aspect complicates legal proceedings and requires international cooperation to combat cybersquatting effectively.

7. **Prevention measures**: To combat cybersquatting, organizations and individuals can employ various protective measures, such as monitoring domain registrations, securing trademark registrations, using defensive domain name registrations, and actively enforcing their trademark rights.

Cybersquatting poses significant challenges to trademark owners, businesses, and individuals seeking to protect their online identities and intellectual property. Understanding these different aspects of cybersquatting is vital in developing effective strategies to prevent and address this form of online infringement.

PREVENTIVE MEASURES

Preventive measures for cybersquatting include:

1. **Trademark registrations**: Register your trademarks to establish legal rights and make it easier to defend against cyber squatters. Trademark registration is the legal process of officially recording a logo, symbol, word, phrase, or design that distinguishes and identifies a product or service. Through trademark registration, the owner gains exclusive rights to use the trademark in connection with the specific goods or services it represents. This process typically involves submitting an application to the appropriate government authority, such as the United States Patent and Trademark Office (USPTO) in the United States, and once approved, the trademark is protected under intellectual property laws, allowing the owner to take legal action against unauthorized use or infringement by others.

2. **Domain name registrations**: There are several types of domains, including:

1. ***Top-Level Domains (TLDs):*** These are the highest level of domain names in the hierarchical Domain Name System (DNS). Examples include .com, .org, .net, .gov, .edu, and country-code TLDs like .us, .uk, .de, and .jp.
2. ***Country-Code Top-Level Domains (ccTLDs):*** These are specific to particular countries

ISSN: 2582-6433

or geographic locations, such as .uk for the United Kingdom, .de for Germany, .ca for Canada, and .jp for Japan.

3. ***Generic Top-Level Domains (gTLDs):*** These are generic domain extensions that are not tied to a specific country. Examples include .com, .org, .net, .info, .biz, and newer gTLDs like .app, .blog, .guru, and .company.
4. ***Second-Level Domains:*** These are the part of the domain name that comes before the top-level domain, such as "example" in www.example.com.
5. ***Subdomains:*** These are subdivisions of a domain that are often used to organize and navigate to different sections of a website. For example, blog.example.com and shop.example.com are subdomains of the domain example.com.

Secure variations of your domain name and trademarks to prevent cyber squatters from registering similar domains. It is the process of acquiring and registering a unique internet domain name for a specific period of time, typically one year or longer. This process involves the selection of a domain name, checking its availability, and then completing the registration through a domain name registrar, which is an accredited organization or service that manages the reservation of domain names. Once registered, the domain name becomes an exclusive online address for the registrant, enabling the establishment of a website and the use of personalized email addresses. The registration also provides ownership rights and control over the domain name, including the ability to modify its settings, renew the registration, and transfer it to another registrar if needed.

3. **Monitoring**: Monitoring domain refers to the practice of regularly observing and tracking domain name registrations, as well as associated web content, to identify any unauthorized or potentially infringing activity. This includes keeping an eye on new domain registrations that may be similar to your own domain or trademarks, as well as monitoring the content and activity on those domains. Monitoring domains is an essential proactive measure to protect intellectual property, prevent cybersquatting, and identify potential trademark infringements or unauthorized use of your brand online. Regular monitoring can help to detect and address issues in a timely manner, reducing the risk of damage to your brand reputation and intellectual property rights.

ISSN: 2582-6433

4. **Using SSL Certificates:** SSL (Secure Sockets Layer) certificates are cryptographic protocols that provide secure communication over a computer network, particularly ensuring secure transactions, data transfer, and logins. These digital certificates establish an encrypted link between a web server and a browser, offering secure connections and protecting sensitive information from being intercepted by malicious parties. When installed on a web server, an SSL certificate initiates the padlock icon and HTTPS protocol, signifying to users that the site is secure and their data is encrypted. SSL certificates help enhance trust and security for websites, assist in preventing unauthorized access to sensitive information, and contribute to overall online security.

5. **Defensive domain registrations**: Defensive domain registration refers to the practice of registering domain names that are similar to a company's brand or trademark in order to prevent potential misuse or unauthorized use by others. This can include registering common misspellings, abbreviations, or variations of the brand's domain name in order to protect the company's online presence and reputation. Defensive domain registration is a proactive measure that businesses and organizations take to safeguard their intellectual property and prevent potential infringement or cyber-squatting.

6. **Check web address for confirmation of authenticity:** Checking the address bar to confirm a URL involves verifying the web address displayed in the browser's address bar to ensure that it matches the expected or intended website URL. This includes reviewing the domain name, the presence of secure (HTTPS) connection indicators, and the absence of suspicious characters or misspellings that could indicate a fraudulent or phishing website.

   By confirming the URL in the address bar, users can validate the authenticity of the website they are visiting and reduce the risk of falling victim to phishing scams, malicious websites, or other online threats. This practice helps users ensure they are accessing legitimate websites and enables them to make informed decisions about the safety and security of their online interactions.

7. **Domain name dispute resolution procedures**: The Domain Name Dispute Resolution Procedure refers to the process established by the Internet Corporation for Assigned Names and Numbers (ICANN) for resolving disputes over domain names. This procedure

ISSN: 2582-6433

is primarily used to address cases of cybersquatting, trademark infringement, or other abusive registration practices. The most well-known form of domain name dispute resolution is the Uniform Domain Name Dispute Resolution Policy (UDRP), which provides a streamlined process for resolving conflicts over domain names. Under the UDRP, trademark holders can file a complaint against a domain registrant if they believe the domain name has been registered and used in bad faith. A neutral panel of arbitrators or mediators then evaluates the case, considering factors such as the similarity of the domain name to the trademark, the registrant's rights and legitimate interests in the domain name, and the domain's registration and use in bad faith. Other domain dispute resolution procedures may include specific rules and guidelines established by individual domain registries or agreements between parties involved in the dispute. These procedures are designed to offer a relatively efficient and cost-effective means of resolving domain name issues outside of traditional court litigation.

LEGAL FRAMEWORK IN INDIA

In India, the legal framework regarding cybersquatting is primarily governed by the Information Technology Act, 2000, and the amended Information Technology (Amendment) Act, 2008. These laws provide provisions to address cybersquatting and domain name disputes.

Under the *Information Technology Act*, cybersquatting is addressed through provisions related to unauthorized access, data theft, and fraudulent activities. Specifically, *Section 66* of the Act deals with computer-related offenses, which can encompass actions related to cybersquatting. Furthermore, the *amended Information Technology (Amendment) Act, 2008* includes provisions for the punishment of cybersquatting and related offenses, along with the establishment of authorities for regulating and adjudicating domain name disputes.

In addition to these acts, Indian trademark laws play a crucial role in addressing cybersquatting. *The Trademarks Act, 1999*, plays a vital role in safeguarding intellectual property rights (IPR) and empowering trademark owners to take legal action against cyber squatters. Here's how the act contributes to protecting trademark owners from cybersquatting:

1. ***Ownership and Protection***: The Trademarks Act, 1999, provides a legal framework for the registration, ownership, and protection of trademarks in India. It grants exclusive rights to trademark owners to use their marks in the course of trade and renders

ISSN: 2582-6433

unauthorized use by others, including cyber squatters, an infringement of the trademark owner's rights.

2. ***Grounds for Legal Action***: Under the Act, trademark owners have the legal grounds to take action against cyber squatters who register domain names that are identical or deceptively similar to their trademarks, leading to confusion among consumers or dilution of the distinctiveness of their marks.
3. ***Remedies for Infringement***: The Act offers remedies to trademark owners in cases of infringement, including seeking injunctions, damages, and orders for the transfer or cancellation of domain names registered in bad faith by cyber squatters.
4. ***Protection of Goodwill and Reputation***: By enabling trademark owners to pursue legal action against cyber squatters, the Trademarks Act safeguards the goodwill and reputation associated with the trademarks, preventing unauthorized parties from exploiting the goodwill and reputation of established brands through abusive domain registrations.

Overall, the Trademarks Act, 1999, serves as a crucial legal instrument for protecting the rights of trademark owners and empowering them to take effective legal action against cyber squatters, thereby contributing to the overall safeguarding of intellectual property rights in the digital space.

Moreover, India is a member of the *World Intellectual Property Organization (WIPO)* and is a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) under the World Trade Organization (WTO), which further strengthens the legal framework for addressing cybersquatting and domain name disputes in several ways:

1. **International Best Practices and Standards**: By being part of WIPO and TRIPS, India is exposed to international best practices and standards related to intellectual property rights, including domain name management and protection. This exposure allows India to align its legal framework with globally accepted principles and facilitates the adoption of measures to address cybersquatting in line with international standards.

2. **Access to Dispute Resolution Mechanisms**: WIPO provides dispute resolution services for domain name disputes through its Uniform Domain Name Dispute Resolution Policy (UDRP). As a member of WIPO, India can utilize these services for resolving domain name disputes, offering a recognized and efficient mechanism for addressing

ISSN: 2582-6433

cybersquatting cases.

3. **Legal Harmonization and Cooperation**: Membership in WIPO and participation in TRIPS promote legal harmonization and international cooperation in intellectual property matters. This fosters collaboration between India and other nations in addressing cybersquatting and domain name disputes, allowing for consistent enforcement of intellectual property rights across borders.

4. **Enhanced Enforcement Capabilities**: Participation in TRIPS strengthens India's legal framework by providing mechanisms for enforcing intellectual property rights, including provisions related to cybersquatting. This facilitates the implementation of effective measures to prevent and address domain name abuses, enhancing the protection of trademark owners and promoting a more secure online environment.

India's membership in WIPO and its participation in TRIPS contribute to the development of a robust legal framework for addressing cybersquatting and domain name disputes by incorporating international standards, accessing dispute resolution mechanisms, fostering legal harmonization, and enhancing enforcement capabilities. This ensures that India is equipped to effectively tackle issues related to abusive domain name registrations and protect the rights of trademark owners in the digital space.

Overall, the legal framework in India encompasses both general cybercrime laws and specific provisions related to intellectual property rights, providing avenues for addressing cybersquatting and protecting trademark owners from abusive domain name registrations.

LEADING CASE LAWS IN RELATION OF CYBER SQUATTING

1. One of the leading cases related to cybersquatting is the case of ***Telstra Corporation Ltd v. Nuclear Marshmallows (1999).*** In this case, the Australian telecommunications company Telstra sued the registrants of several domain names, including "telstra.org," alleging that they were engaging in cybersquatting and attempting to profit unfairly from Telstra's trademark.

ISSN: 2582-6433

The court ruled in favor of Telstra, acknowledging that the domain names were registered in bad faith and used in a manner that could cause confusion among consumers. The judgment emphasized the importance of protecting established trademarks in the online domain and highlighted the adverse impact that cybersquatting can have on the reputation and commercial interests of legitimate businesses.

2. ***Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd. (2004):*** In this case, the plaintiff, Satyam Infoway, alleged that the defendant's registration of the domain name "satyaminfoway.net" amounted to cybersquatting and trademark infringement. The court ruled in favor of Satyam Infoway, recognizing the domain registration as an act of cybersquatting and a violation of the plaintiff's trademark rights.
   The court's decision emphasized the importance of protecting established trademarks in the online domain and highlighted the adverse impact that cybersquatting can have on the reputation and commercial interests of legitimate businesses.

3. ***The WIPO arbitration case of Julia Fiona Roberts v. Russell Boyd (2000).*** In this instance, the actress Julia Roberts filed a complaint under the Uniform Domain-Name Dispute-Resolution Policy (UDRP) against the registrant of the domain name "juliaroberts.com." The WIPO panel found in favor of Julia Roberts, concluding that the domain name was registered and used in bad faith, and that the registrant had no legitimate rights or interests in the domain.

4. ***Tata Sons Limited v. Manu and Ors (2011):*** Tata Sons, the holding company of the Tata Group, filed a case against the defendants for registering domain names containing the word "Tata," alleging that it constituted cybersquatting and trademark infringement. The court upheld Tata Sons' claim, ruling in favor of the plaintiff and highlighting the unauthorized use of the Tata trademark as evidence of cybersquatting.

5. Another prominent case is ***Yahoo! Inc. v. Akash Arora & Anr(1999):*** The court came to the conclusion that Akash Arora was responsible for the infringement of the “Yahoo” trademark and issued a restraining order against him based on the theory that he was engaging in cybersquatting by using a domain name that was confusingly similar to that of Yahoo INC. while also providing services that were comparable to those provided by Yahoo INC. The reasoning for this judgement was that the reputational value of a

ISSN: 2582-6433

company is heavily dependent on its name and trademark, which is particularly true in the case of Yahoo Inc. Accordingly, it was decided that the word "Yahoo" had built up its reputation, and that the defendant needed to stop using the domain name "yahooindia.com" permanently. This was because it was determined that the word had gained its reputation. Yahoo Inc. was awarded the right to prevent others from passing off its products.[1]

These cases demonstrate the significance of protecting trademarks in the digital space and the legal recourse available to trademark owners to combat cybersquatting under Indian law. The judgments underscore the importance of safeguarding intellectual property rights and the adverse consequences of cybersquatting on legitimate business. They also highlight the role of dispute resolution mechanisms, such as the UDRP, in addressing instances of cybersquatting and protecting the interests of trademark holders.

CONCLUSION

Cybersquatting refers to the unauthorized registration or use of domain names that are similar to or identical to established trademarks or brands, with the intent to profit from the association with those brands. It can lead to consumer confusion and damage the reputation of legitimate businesses. To combat cybersquatting, laws and regulations have been put in place to protect intellectual property rights, and many businesses have also employed strategies such as monitoring and enforcement to protect their brands online and by being vigilant and informed, internet users can reduce their risk of falling victim to cybersquatting schemes and other online scams. However, cybersquatting remains a significant issue, and continued vigilance and proactive measures are necessary to address this ongoing challenge.

[1] Yahoo! Inc. v. Akash Arora & ANR(1999) Delhi HC (no date) Khurana and Khurana. Available at: https://www.khuranaandkhurana.com/2023/07/10/yahoo-inc-v-akash-arora-anr1999-delhi-hc/ (Accessed: 13 January 2024).