REGULATION OF CYBERSQUATTING: AN ANALYSIS OF THE LEGAL FRAMEWORK IN INDIA, THE UK AND THE USA

Shriyaa Zubin*

ABSTRACT

With the internet's fast expansion and growth, it is now essentially impossible to find a business that doesn't have an online presence. A website or any other form of internet presence is increasingly commonplace for businesses, and those who don't are surely considering acquiring one. It's simple to see why using the internet to advertise one's products or services is convenient and quick. Therefore, having a website for your company is essential. However, since the registration of a domain name is done on a first-come, first-served basis and without the necessity for any documentation of the name's commercial use, anybody can do so, even if the name is the brand name or registered trademark of another. This has now given rise to an issue known as 'Cybersquatting' in which dishonest people prematurely register names that are confusingly similar to other people's trademarks in order to make money, deceive others or damage the reputations of the actual owners of the trademarks or names. This article aims to dive deeper and analyse the Legal Framework around the world.

INTRODUCTION

Cybersquatting is the practice of buying, illegally selling, or using a web domain with the intention to profit from the reputation of another party's work. The practice typically includes registering domain names that are similar to or the same as well-known brands or corporate names in order to lead traffic to a website or sell the domain name back to the actual owner for a higher price. Moreover, cybersquatters may exploit domain names to spread viruses or engage in dishonest practices like phishing. Cybersquatting is frequently illegal and may result in the infringer being subject to legal action. Businesses and trademark owners may protect themselves from cybersquatting by filing their domain names, trademarks, and other intellectual property with the appropriate authorities and keeping a lookout for instances of

*BBA LLB, FIRST YEAR, SYMBIOSIS LAW SCHOOL, PUNE.

infringement. Any lawful trademark owner who lacks their own domain may let a competitor use it.[1]

Only first-come, first-served domain name registrations are approved. Cybersquatting is the practice of marketing or renting a name that is perplexingly close to a trademark. Finding strategies to encourage the spread of intellectual property on the Internet while preventing its illegitimate use has become harder legally in recent years. The act of "cybersquatting" started with the invention of domain names. Due to the fact that not all business owners are tech-savvy, a rival organisation could acquire their trade name and then try to sell it to the legitimate trademark owner as a domain name. Brand jacking, also known as cybersquatting, first became a problem in the 1990s, a time when the internet was a widely followed global trend. "Cybersquatting" refers to the practice of registering a fictitious domain name with the intention of later selling it to the name's legitimate owner for a profit. This domain name is too close to an offline registered brand or person's name, which weakens it or makes it confused.[2]

Cybersquatters are motivated by money. Such a trademark holder is willing to pay a premium price to acquire the domain name since, due to their similarities, any harm or annoyance caused by the latter may be traced back to the owner of the original brand.[3]

Domain Name:

Domain names might be far more expensive than real estate. For instance, fb.com was purchased by Facebook for USD 8.5 million. Thieves, as well as companies, are drawn to domain names because of their high value. Since it damages a company's image and reputation, domain name theft can pose significant problems for businesses. This is due to the possibility of using a stolen domain name in connection with illegal activities, including the distribution of pornographic content, downloading malware, and sending spam. In this context, one of the past ICANN CEOs noted that while spam and malware may be more immediately dangerous threats, domain hijacking may nevertheless have a significant negative impact on a company.

Phishing, identity theft, and fraudulent domain name purchases are the three major techniques that criminals employ to steal domain names. The next sections go into further depth about

[1] SCC Online, Domain Names and Cybersquatting in IP Laws, CNLU LJ (8) [2018-19] 229, http://www.scconline.com.eu1.proxy.openathens.net/DocumentLink/gqW4kDTo
[2] S&A Law Offices India: Cyber Squatting Laws In India https://www.mondaq.com/india/trademark/208840/cyber-squatting-laws-in-india accessed on 2nd September
[3] ibid

these three techniques as well as the safeguards against them. It is vital to offer broad guidance on how to prevent domain name theft before moving on to examine those procedures. First and foremost, it is advised to work with trustworthy domain name registrars. Some unidentified registrars might not help their customers if their domain name is stolen. It's also possible that certain registrars deliberately participate in domain name theft. The "locking" function offered by the majority of domain name registrars should be used, too. Finally, routine domain name portfolio monitoring provides a prompt response in the event of a theft, which may ultimately result in the successful recovery of a stolen domain name. The transmission of bogus communications that appear to have been issued by the domain name registrar is one popular method of phishing domain name theft. The notification can inform the domain name holder that he has to reactivate his account on the domain name registrar's website. A screenshot of an actual email sent by a criminal to a person whose identity will be kept secret is seen in the image below. The person sent his personal information to the thief who stole a domain name since he was unaware that the email was bogus. The thief then "sold" the domain name to a Chinese customer who claimed to have bought it legally and not to be aware of any illicit activity.

By employing techniques other than phishing, a domain name thief may be able to get private information about the victim. Such methods may involve access to paper documents, accessing publicly available private information, guessing a weak password, or "shoulder surfing". The latter phrase describes the practice of watching individuals while they interact with computers, ATMs, or other electronic devices. The fraudster may immediately access the victim's domain name account after getting the victim's personal information.

One must take several precautions to prevent identity theft, such as creating secure passwords, keeping private information off the Internet, turning on social network privacy settings, and shredding any personal information-containing documents before throwing them away. The registrar will likely absolve itself of any liability in the event that a fraudster steals a domain name using the personal details of a domain name owner. Sometimes, scammers get in touch with domain name owners and ask to buy their names. The con artists may offer highly alluring pricing to entice the owners. When the domain name's owner agrees to sell it, the scammer also promises to pay after getting the domain name. If the seller concurs as well, the scammer obtains the domain name and then vanishes. The process of recovering a stolen domain name is sometimes made more difficult by its repeated sale to different customers. One must employ

the services of reputable escrow providers to avoid fraudulent domain name purchases. These companies gather, keep, and disburse the money associated with domain name transactions. Although domain name theft is a serious problem in the e-commerce industry, recovering a stolen domain name may be difficult and expensive. A stolen domain name, MLA.com, which was moved to a registrar in the Bahamas in May 2013, was recovered after 19 months and around USD 15,000 by the owner of an advertising firm.[4] Because it was difficult for customers to contact the firm, it suffered considerable revenue losses. In another instance, a domain name theft cost the owner of ShadesDaddy.com USD 50,000 in missed revenue. It's like your house has been robbed, said the owner, who was also forced to fire six of his eight employees.

Thus, ICANN and national governmental agencies must devise a method to make it easier for domains that have been stolen to be recovered. The implementation of an online dispute resolution like ICANN's Unified Domain Name Dispute Resolution Policy (UDRP), which will be applicable especially to the settlement of issues relating to domain name theft, may be one such method. Such a process will enable domain name owners to regain control of their domain names without needing to file legal claims. Another, even more creative strategy is the establishment of a crowdsourced online dispute resolution system for stolen names comparable to eBay's Community Court. With the use of eBay's Community Court, issues involving sellers' ratings that were posted on eBay might be settled by community members serving as jurors. By enabling representatives of the domain name registrars to settle such conflicts collaboratively, the notion behind eBay's Community Court may be applied to disputes involving domain theft.[5]

The most effective way to protect the ownership of a domain name is prevention, at least until the emergence of a fresh and ground-breaking approach to dispute resolution about domain name theft. According to this article, there are three categories into which preventive methods may be divided: phishing prevention measures, identity theft prevention measures, and domain name fraud prevention measures. If these precautions are fully understood, domain name owners will be able to avoid fraudsters' traps and maintain control of their domain names for a very long time.

[4] SCC Online, Domain Names and Cybersquatting in IP Laws, CNLU LJ (8) [2018-19] 229, http://www.scconline.com.eu1.proxy.openathens.net/DocumentLink/gqW4kDTo, accessed on 5th September
[5] ibid

How cybersquatting may be a challenge for a company:

A strong online presence is essential for business success in the modern digital era. To attract customers, promote their goods or services, and increase brand awareness, businesses spend a lot of money creating and maintaining websites. However, a dangerous practice known as cybersquatting, which may have significant and frequently sneaky repercussions on organisations, is lurking in the virtual shadows. Cybersquatting, also known as domain squatting, is the practice of registering, purchasing, or otherwise making use of a domain name with the intention of making money off of the reputation of another person's brand. This practice usually entails the registration of domain names that are eerily similar to well-known trademarks, brand names, or prominent website addresses. Cybersquatters frequently do this in the hopes of either profiting from online traffic created by visitors who unintentionally visit their site or selling the domain to the legal trademark owner at a premium price. Brand dilution and misunderstanding are two of the most immediate and harmful repercussions of cybersquatting on enterprises. Customers may unintentionally end up on cybersquatters' websites believing they are dealing with the actual company when they register names that closely resemble legitimate brands. This perplexity may breed distrust, annoyance, and a poor impression of the real brand. Customers might come across improper information, phishing scams, or fake goods, all of which could damage their confidence and loyalty. Additionally, cybersquatters purposefully register domain names linked to well-known brands or frequent misspellings or typos of such names. They, therefore, distract visitors from the trustworthy website. It can result in online strategy failure, brand dilution, lost web traffic, financial consequences, reputational harm, and increased marketing spending. Cybersquatters frequently target prospective rookies in the hopes of making money off of their popularity in the future. In conclusion, cybersquatting poses a serious risk to companies operating in the digital era. It is crucial for companies of all sizes to safeguard their online reputation and brand integrity. In the continuous struggle against this stealthy yet sneaky danger to corporate success in the digital sphere, vigilance, legal redress, and proactive domain management are crucial weapons.

Let's assume that someone makes the decision to establish a website and invests effort, energy, and resources into it for Google Ad Words and search engine optimisation to grow and drive visitors to the site. The website will act as the company's online address if it is successful in growing in popularity and significance for the enterprise. Imagine finding out after reading all of this that a tonne of identical domain names, including every imaginable misspelling or

typographical error of that domain name, have been acquired by cybersquatters. As it is usual for individuals to type domain names incorrectly, which results in these misspelled domain names and eventually the competitor's website, each of them has been registered since they will each see a sizable amount of traffic as a result of the popularity of the competitor website. These potential customers or leads might not be in great numbers, but it is still possible that they could find their way to the Cybersquatters website, and one cannot control the information on a squatter's website.[6] Visitors to competing websites or mechanically generated web pages with promoted pay-per-click links are regularly directed by cybersquatters. These websites might include wagering, obscene, phishing, or other offensive material. The primary issue is that the domain name is tied to the websites, and as was already indicated, the links are almost certainly to the rival website. However, since Google Ad Words automatically inserts advertising on linked websites, including cybersquatter websites, the links may even lead to the owner's own website if the website is connected to it. The owner will ultimately have to spend to have his or her own clients led back to the website. Also, it's possible that customers might become distracted and visit a rival's website, costing you a crucial client.[7]

We may thus draw the conclusion that the subject of cybersquatting is more persistent the more web presence and online income someone has.

REGULATION OF CYBERSQUATTING AROUND THE WORLD

India

Presently, no law in India specifically mentions resolving issues with cybersquatting or other domain name conflicts. The Trademarks Act of 1999, which protects the use of trademarks in domain names, is not extraterritorial. It doesn't provide sufficient domain name protection. According to the Supreme Court, domain names should have the maximum amount of legal protection under the passing-off statutes. This legislation was developed by judges in India, and all the High Court's unanimously agreed on it. The Supreme Court chose and authorised this statute. In Indian courts, conflicts over domain names are rather rare. Few recorded judgements involving domain name conflicts have been made, and Indian case law has not yet been established. However, since Internet usage is increasing in the nation at an astounding

[6] SCC Online, Trademark Infringement Through Cybersquatting : Law and Policy : A Study of Udrp and Indian System, CNLU LJ (6) [2016-17] 33, accessed on 7th September 2023 http://www.scconline.com.eu1.proxy.openathens.net/DocumentLink/04YQ0TS8
[7] ibid

rate, Indian courts will undoubtedly see domain name conflicts in the future. A dispute involving a purposeful trade-off of the similarity between the domain name and another well-known brand is referred to as infringement. The registrant then runs a company that is similar to that of the trademark holder in an effort to capitalise on the reputation of the trademark holder. In these circumstances, regardless of whether the infringement took place as Internet domain names or in any other context, the use of the mark (domain name) would be prohibited by the current trademark law.

Indian Laws:

Justification for Action When it came to the Indian domain name situation, the Satyam Infoway Ltd v. Sifynet Solutions (P) Ltd judgement nailed it back in 2004. It should be noted that the Indian Information Technology Act, 2000 and the Trade and Merchandise Marks Act, 1958 (together referred to as the "TM Act") do not address domain name disputes. Indian Courts thus treat these disagreements according to the "passing off" criteria. In N. R. Dongre v. Whirlpool, the courts stated that "a man may not sell his own products on the pretence that they are the property of another man," which is the basis of the case of passing off. One person tries to make money off of another's reputation in a certain profession or industry by passing off, which is a type of unfair commercial competition. A passing-off lawsuit is directly governed by tort law, common law of rights, or case law. The Act solely lists the procedures to follow and applicable remedies; it makes no attempt to define passing off. Unfortunately, the Trademark Act does not contain any provisions under which the crime of cybersquatting may be prosecuted. The Indian Courts have, therefore, been adhering to the passing off principle, the rules and regulations of the WIPO, and the UDRP in the absence of any such provision.[8]

Drafting a new law in India that specifically addresses domain names is urgently needed.

The United States

The United States is recognised for passing anti-cybersquatter legislation before any other country in the globe. According to Anahid Chalikian, "the courts have addressed the issue of cybersquatting by applying traditional trademark infringement and dilution principles to claims

[8] Live Law, https://www.livelaw.in/columns/cybersquatting-domain-name-protection-under-trademark-law-209573, accessed on 7th september 2023

submitted by cybersquatting victims. Congress passed the Anti Cybersquatting Consumers Protection Act (ACPA) in November 1999. However, it has shown that trademark law is insufficient for safeguarding brand owners online. To put it another way, federal trademark statutes like the Lanham Act and the Federal Trademark Dilution Act ("FTDA") created the most palatable remedies for trademark owners who were the victims of cybersquatting before Congress passed the ACPA. Since trademark laws like the Lanham Act and the FTDA protect all of them, there are several methods to deal with the cybersquatting phenomenon under American law. The sections that follow describe the "ACPA's" legal principles for dealing with cybersquatting. The first piece of legislation to stop cybersquatting was being debated in Washington. American legislators eventually realised that registrations for cybersquatting operations posed a threat to domestic consumers, global consumers, and e-business in general. They also realised that this dangerous inclination needed to be countered with a novel strategy. On the other hand, the new law that was being submitted to stop cybersquatting through the legislative process was rejected by the White House. However, the U.S. Senate decided it was important to address the uncertainty surrounding the application of trademark law, including the Lanham Act and the ACPA, unexpected judicial opinions, and significant legal costs required to combat cybersquatters. For instance, the FTDA was thought to be the main tool trademark owners utilised to battle cybersquatters. In other words, the only way to resolve a domain name dispute through the legal system prior to the adoption of US anti-cybersquatting laws was to file a case for trademark infringement or dilution. The owner of a well-known mark may obtain an injunction "against another person's commercial use in commerce of a mark or trade name if such use commences after the mark has become well-known and results in dilution of the distinctive nature of the famous mark".[9]

United Kingdom

As a common law country like the US, the UK also bases its laws on previous court decisions. The protection of trademarks registered in the UK, including cybersquatting activities, is governed by the UK Trademarks Act of 1994, as amended. No legislation covering these actions expressly has been adopted by the nation. The UK Trademark Act does not specifically offer legal protection for unregistered trademarks, in contrast to the US Lanham Act. On the other hand, if a trademark is being used in the course of trade or commerce but has not yet been

[9] Sunando Mukherjee, "Passing off in Internet Domanins- A legal Analysis https://nopr.niscpr.res.in/bitstream/123456789/4731/1/JIPR%209%282%29%20136-147.pdf accessed on 7th September 2023

registered, it is feasible to stop usage by a "third party" who is infringing by making a claim under the ground of "passing off." However, proving the validity of this claim is more challenging than proving trademark infringement. The common law tort of passing off and infringement of a trademark in violation of statute have emerged as the two most important grounds for a lawsuit. A tort for the unlawful use or registration of a domain name connected to a trademark or cybersquatting activity is not recognised in the UK, nevertheless. The UK Trademarks Act 1994, as amended, and the passing off offence are typically used by English courts when making judgements about cybersquatting activities. Take the Harrods case, which used the recognisable brand "Harrods" and resulted in the first cybersquatting ruling from an English court. The passing off and trademark infringement allegations were resolved by the English court. The bulk of the plaintiffs, who were trademark owners, asked for compensation and an order compelling the trademark infringement to stop imitating their mark or destroying its reputation. The court attempted for many years to apply equity principles to the litigation that was filed before it in line with the English trademark structure. Commercial interests lobbied for a framework for trademark registration, but a new strategy was needed. As a result, in 1875, the UK Trademarks Registration Act was adopted. This law served as a model for both the UK Trademark Act of 1994 and the UK Trademark Act of 1938. However, decisions made by English courts—which typically use the UK Trademarks Act 1994, as modified—apply common law principles to situations involving cybersquatting. Therefore, to stop cybersquatting, trademark owners may file a trademark infringement case under UK trademark law. The court acknowledged that there was no dominant authority or control over the internet and that it was difficult to deal with cybersquatting activities within the confines of trademark law. As a result, it struggled to decide how to rule in the case. The defence claimed that despite the defendant owning a variety of domain names, none of them had ever been utilised in the conduct of commerce or enterprise involving goods or services. The appellants are selling domain names that are confusingly similar to registered trademarks, the court determined after accepting a "passing off" trademark infringement argument under article 10(3). The origin is shown through the domain names. Because of this, they registered after all. Additionally, they will be added to the services provided by the registrant, a domain name trader. "There is only one plausible reason why someone who was not a member of the Marks & Spencer Plc group might want to use such a domain address, and that is to pass oneself off as a member of that firm or his products as being theirs," the court said. Therefore, disputes involving cybersquatting may be settled through traditional claims of trademark infringement or even the passing-off tort, as in the "One-in-a-Million" case. Nevertheless, there are a variety of remedies

available in cases of trademark infringement and passing off, such as injunctions to prevent the use of the brand without permission, verdicts and damages, or an account of earnings.[10]

CONCLUSION

In conclusion, companies and trademark owners face serious difficulties in the digital era as a result of the practice of cybersquatting. By registering names that are misleadingly similar to well-known brands or trademarks, cybersquatters, motivated by the possibility of financial gain, frequently cause customer confusion and damage the reputation of genuine firms. This practice has an impact on both established enterprises and start-ups trying to build an internet presence. Cybersquatting can take many different forms, such as the selling of domain names with misleadingly similar spellings, the dissemination of malware and phishing scams, and the rerouting of web traffic to rival websites or potentially dangerous material. Cybersquatting may have negative effects on a brand's reputation and credibility that go beyond financial losses. Businesses and trademark owners must take preventative actions and maintain vigilance to resist cybersquatting successfully. These precautions include collaborating with trustworthy domain name registrars, making use of domain locking tools, and putting regular domain name portfolio monitoring into practice. In order to avoid identity theft, which may be used by cybersquatters, people should be careful while revealing information in the digital space and take precautions to secure their identity. A country's efforts to combat cybersquatting through the legal system may differ from another. The Anti-Cybersquatting Consumer Protection Act (ACPA) was passed in the US in order to give trademark owners legal remedies. In the meanwhile, the UK handles cybersquatting claims using common law principles and trademark regulations. India has a weaker legal system, and domain name conflicts are frequently resolved using the passing-off concept. This highlights the necessity for particular legislation to address the problem fully. Furthermore, creative methods for streamlining the recovery of stolen domain names should be investigated by national government organisations and international organisations like ICANN. The procedure might be sped up, and the cost to trademark owners reduced by implementing online dispute resolution processes designed for domain name theft cases.

[10] Us Trademark Statute office gov, https://www.uspto.gov/sites/default/files/trademarks/law/Trademark_Statutes.pdf accessed on 8th September 2023

Cybersquatting continues to be a problem for companies and owners of trademarks, necessitating a multidimensional strategy that includes preventative measures, regulatory frameworks, and international collaboration to secure online identities and maintain brand integrity in the digital sphere. Dealing with cybersquatting will remain a crucial problem for both companies and the government as the internet develops.