Cybersquatting: A Multiplying Con

Shikhar Rusia

BBA LLB 3rd Year, Semester: VI, PRN: 2004030420, Division: B, Roll No: 10, Subject: Cyber Law
Bharati Vidyapeeth (Deemed To Be) University
New Law College, Pune

ABSTRACT: Cybersquatting is a cybercrime which is wide spreading at a very alarming rate and people are not even aware of it. Although people who are using technology as a part of their life are facing issues relating to it unknowingly. This research paper tends to discuss about cybersquatting and its types along with recognition and remedies available to it. It compares remedies available in global world with remedies available in India. It consists of some Indian case Laws. The conclusion of the analysis has been drawn on the basis of primary data collected through the survey conducted by me.

1. INTRODUCTION:

The largest trend now sweeping the internet is domain names. It is standard practise for businesses to have domain names so that they can be quickly recognised by their trademarks. A consumer may desire a relationship with a lot of businesses, but this is not physically viable. The domain names enable customers to locate and get in touch with the business. Domain names and trademarks are connected.[1]

The bad faith registration of internet domain names is known as cybersquatting, which is a kind of domain name trademark infringement. The perpetrators of this offence will buy, sell, or utilise a domain name for a website that inadvertently comprises a protected trademark or service mark. This activity is being taken with the intention of making money off of customer goodwill associated with a well-known brand. Cybersquatting is classified as trademark infringement by definition. However, there are some definite distinctions between the two. For example, not all digital infringements are considered cybersquatting. One instance is when unsuitable listing techniques are applied on Amazon. Although there has been infringement, no domain name was registered in bad faith.[2]

The Indian courts have defined "cybersquatting" as "an act of obtaining fraudulent registration with a purpose to sell the domain name to the lawful owner of the name at a premium" by referring to the term provided in the Manish Vij v. Indra Chugh case decided by the Delhi High Court[3].

When a person or business registers a domain name that is the same as or confusingly similar to a trademark of another party with the intent to sell it for profit. This practise is called "Cybersquatting." The person doing cybersquatting is known as cybersquatter. A cybersquatter violates the trademark owner's basic right to use its trademark in this way. As a result of the decline in domain name pricing and the rise of several top-level domains (.biz, .cn, .mob, and most recently.in). The Cybersquatters have made a lot of illegal income. Cybersquatters then sell the domain to the person or business who owns a trademark that has been utilised in the domain name as a form of ransom in order to gain illegal money. The domain name in question cannot be registered in the name of the owner of the trademark since it has already been registered by another person.[4]

2. WHAT IS CYBERSQUATTING?

Cybersquatting is the practise of registering or utilising a domain name to make money off of a company name, a person's name, or a brand.[5]

According to this definition of cybersquatting, domain squatting occurs either as an act of extortion or as an attempt to steal customers from a competitor. However, it's possible that a domain was registered with good intentions. It wouldn't constitute cybersquatting in this instance. In other words, even if the name is already in use, domain squatting does not happen when a legitimate business name is registered without any malice.

The cybersquatter has a range of bad faith options at their disposal. These could range from offering the owner the chance to buy the domain at an exorbitant price to selling comparable goods on the infringing website. Several factors will be taken into account by courts and international organisations when determining whether bad faith activities have taken place. These factors include the following:

- Does the domain name fall under the alleged cybersquatter's intellectual property rights?
- Does the domain name fall under fair use or have a non-commercial use?
- Did the cybersquatter attempt to sell the domain name without prior good faith intent?
- Was there intent to dilute or harm a registered trademark?
- Did the alleged cybersquatter use intentionally misleading contact information?[6]

[1] Ipleaders; https://blog.ipleaders.in/cybersquatting-position-india/ (last visited February 05, 2023; 11:38 PM).
[2] Mandour Law; https://www.mandourlaw.com/cybersquatting/ (last visited February 06, 2023; 12:23 AM).
[3] Manish Vij v. Indra Chugh, AIR 2002 Del 243.
[4] Ipleaders, supra note 1, at 02.
[5] Fortinet; https://www.fortinet.com/resources/cyberglossary/cybersquatting (last visited February 05, 2023; 10:23 PM).
[6] NOLO, https://www.nolo.com/legal-encyclopedia/cybersquatting-what-what-can-be-29778.html (last visited February 05; 10:58 PM).

2.1 HISTORY OF CYBERSQUATTING?

Cybersquatting has dramatically expanded over the past few years and has a terrible impact on those who possess intellectual property rights (IPR). Cybersquatting is the use, sale, or registration of a popular, already-existing domain name with the intention of reselling it to the rightful owner at a profit. We are all aware that businesses must now have an online presence in order to succeed in the modern world.

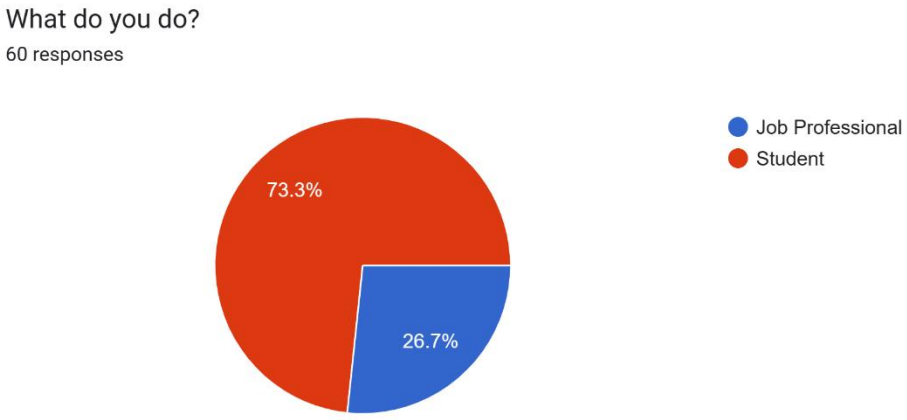
The phenomenon that came to be known as cybersquatting began at a time when most firms were not educated of the internet's market prospects. Several creative people registered as domain names of well-known businesses, with the goal of selling the names back to the businesses when they eventually wake up. The cybersquatter "victims" were Samsung, Fry's Electronics, Hertz, and Avon. Opportunities for cybersquatters are dwindling rapidly, as most businesses now know that a high priority is to nail down domain names.[7] The behaviour that has come to be known as "cybersquatting" first appeared when the majority of businesses were still ignorant of the lucrative potential available online. Some enterprising individuals registered popular company names as domain domains with the intention of selling the names back to the organisations once they realised what they were doing. Among the "victims" of cybersquatters were Panasonic, Fry's Electronics, Hertz, and Avon. Opportunities for cybersquatters are gradually dwindling as more and more companies realise how important it is to secure domain names.

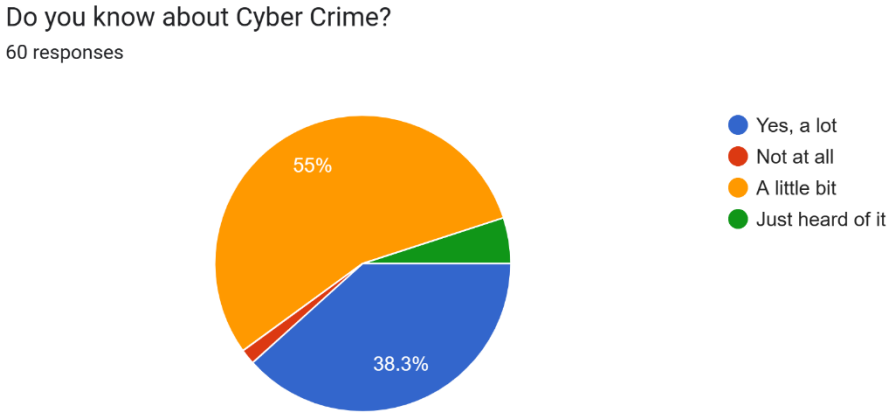
The reach of cybersquatting laws expanded to social media platforms as they gained popularity. It can be challenging to tell traditional trademark infringement from cybersquatting in these circumstances. For instance, it would be conventional infringement to use a branded name to boost search results for another product. Cybersquatting, on the other hand, is claiming to be or represent a brand.

2.2 ANALYSIS ON THE BASIS OF PRIMARY DATA

I have conducted a survey regarding cybersquatting among the students and job professionals of today's generation to know that how many people who are already literate, are aware about cybercrime and specifically cybersquatting. The survey was conducted among 60 people out of which 16 were job professionals and 44 were students. Out of the 60 people who all are educated and are of today's generation there are just 55% people who knows a little bit about cyber-crime and if we talk about cybersquatting just 35% people knows about it, most of the people has faced the issue of typographical error and also when they are surfing over internet, they see similar domain names for one website.

The data of survey has been attached by way of pie charts.

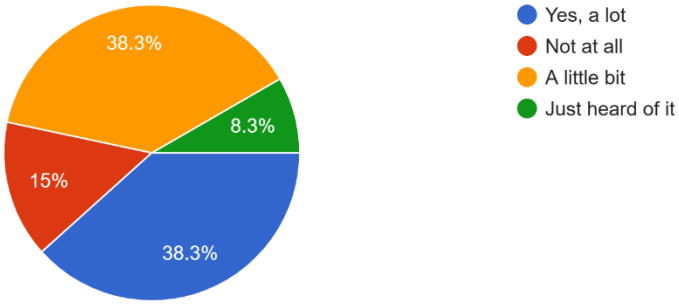




[7] Muskaan Punia, *Cybersquatting*, INDIAN LAW PORTAL, (July 1, 2020) https://indianlawportal.co.in/cybersquatting/.

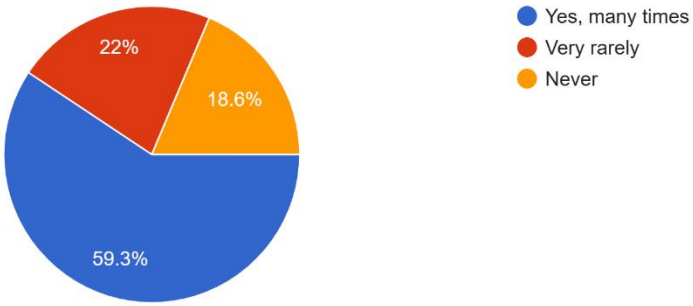
Do you know about domain name?

60 responses



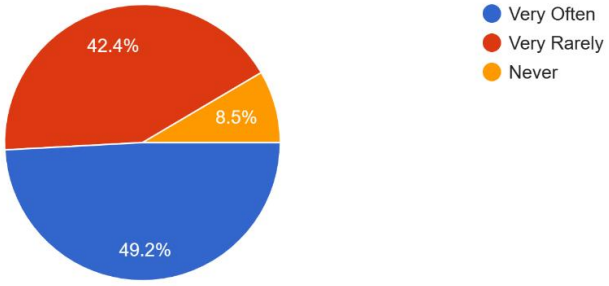
Have you ever seen two different websites with almost similar domain names?

59 responses



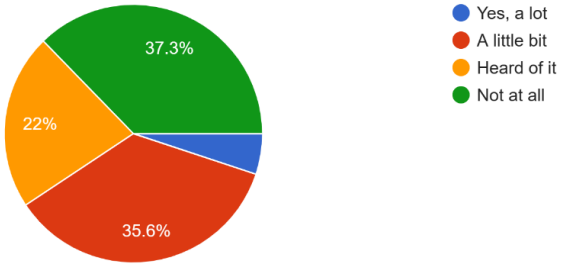
Have you ever faced typographical errors?

59 responses



Do you know about cybersquatting?

59 responses



By the data received after survey I analysed that cybersquatting is such an unnoticed crime that even people who are educated and getting affected are not aware of, and the problem is to recognise the cybersquatting, also it is very important for us to know about such crimes and the remedies to it.

2.3 HOW TO RECOGNIZE CYBERSQUATTING?

How do you know if the domain name you want is being used by a cybersquatter? Follow these steps to find out.[8]

- Check where the domain name takes you. As a general rule, first check to see if the domain name takes you to a website. If it does not take you to a functioning website, but instead takes you to a site stating "this domain name for sale," or "under construction," or "can't find server," the likelihood increases that you are dealing with a cybersquatter. The absence of a real site may indicate that the domain name owner's only purpose in buying the name is to sell it back to you at a higher price.
- Of course, absence of a website does not always mean the presence of a cybersquatter. There may also be an innocent explanation and the domain name owner may have perfectly legitimate plans to have a website in the future.
- If the domain takes you to a functioning website that is comprised primarily of advertisements for products or services related to your trademark, you may also have a case of cybersquatting. For example, if your company is well-known for providing audio-visual services and the website you encounter is packed with ads for other company's audio-visual services, the likelihood is very strong that the site is operated by a cybersquatter who is trading off your company's popularity to sell Google ads to your competitors.
- If the domain name takes you to a website that appears to be functional, has a reasonable relation to the domain name, but does not compete with your products or services, you probably aren't looking at a case of cybersquatting. For example, if your trademark is "Moby Dick" for fine art dealing with whaling, and the website you encounter (www.mobydick.com) is for road cleaning machines, you do not have a case of cybersquatting. You may, under certain circumstances, have a case of trademark infringement.
- Contact the domain name registrant. Before jumping to any conclusions, contact the domain name registrant. To find the name and address of a domain name owner, you can use the "WHOIS Lookup" at whois.net. Find out whether there is a reasonable explanation for the use of the domain name, or if the registrant is willing to sell you the name at a price you are willing to pay.
- Pay, if it makes sense. Sometimes, paying the cybersquatter is the best choice. It may cheaper and quicker than filing a lawsuit or initiating an arbitration hearing.

2.4 TYPES OF CYBERSQUATTING:

i. Typosquatting:

Different techniques can be used to engage in cybersquatting. The most prevalent method, however, is typosquatting, which is accomplished by changing the way the website's domain name was formed. By using this technique, the cyber-squatter can redirect users to a fake or illegal website when they make typing mistakes or errors.[9] The basic goal of typosquatting is to change a domain's original spelling by adding or removing digits, characters, or periods. Additionally, it involves altering the order of the letters or words within a domain. Typosquatting is the practise of profiting on possible errors.

Typosquatting, often known as "false URLs," takes advantage of customer typing errors made when attempting to access websites. This frequently includes errors or typical misspellings of trademarked terms. When using this technique, infringers frequently construct a bogus website to go with the domain address. This may mislead customers about the origin of the goods they're buying. Different top-level domains may also be used by cybersquatters to pressure trademark owners into purchasing the website.[10]

Examples:

- Eliminating the “dot” from the domain name. i.e., wwwfacebook.com.
- Misspelled the website name such as www.facbook.com.
- Website’s domain name expressed in a different way, such as facebook.org.
- Registering starbucks.org if it hadn’t been registered by the trademark owner.
- Attempting to sell any top-level domain featuring “starbucks” after having no intent to legitimately use the website.
- Registering potential misspellings or typos for starbucks.
- Linking starbukcs.io to a website that sells competing coffee products.

ii. Identity Theft:

Because someone can exploit a company's identity to generate a comparable Uniform Resource Locator, cybersquatting can also be used for identity theft (URL). A user visiting that company's website might instead land on the bogus site. At that time, the cybersquatter effectively hijacked the target's digital identity.

Consider a scenario in which your business recently announced a partnership with another company but you have yet to buy a URL. Sky Computing is the name of your business, and Reach Digital is the business you are collaborating with. You issue a press release announcing that the joint venture will be known as Sky Reach.

Then, a cybersquatter can register "skyreach.com" online in order to take advantage of this "opportunity." You discover that the URL you desire is already taken when you register it. This is against the law, and you can request that the domain "skyreach.com" be transferred to either your business, the business with which you have a partnership, or the joint venture.[11]

[8] NOLO, supra note 6, at 03.
[9] Swarit Advisors; https://swaritadvisors.com/blog/cybersquatting-in-india/ (last visited February 05, 2023; 01:30 AM).
[10] Mandour Law, supra note 2, at 02.
[11] Fortinet, supra note 5, at 03

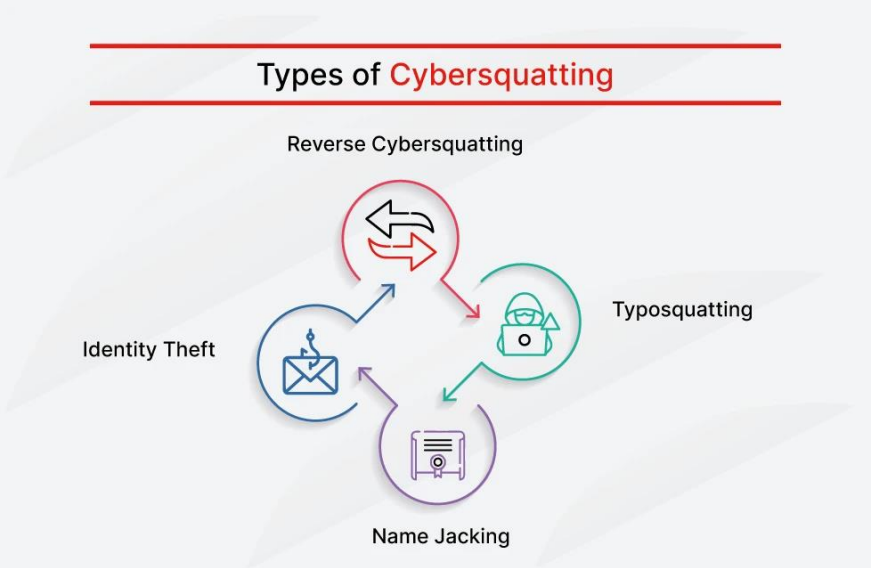
iii. Name Jacking:

In the United States, personal names may be trademarked in certain situations. This only usually happens if they've developed a secondary significance in the marketplace (such as Madonna or Beyoncé). The Anti-Cybersquatting Consumer Protection Act may not always apply to name jacking because it is a complicated area of the law. On social media, name jacking can also occur. Even without a registered domain name, creating a profile that represents a celebrity or well-known person may be considered cybersquatting. Given the abundance of fan sites now online, this is another grey issue. If the website starts selling illegal goods, that might be called cybersquatting.

iv. Reverse Cybersquatting:

Reverse domain name hijacking (RDNH), commonly referred to as reverse cybersquatting, is a tactic that resembles cybersquatting in several aspects. Reverse domain hijacking is a little different from cybersquatting, which is the act of buying a domain name that contains a trademark with the intention of profiting from that trademark. It occurs when a person or company falsely asserts that she, he, or it is the owner of a trademark before unjustifiably attempting to seize your genuine domain name.

Consider the case where you registered the domain name IndustrialChemicals.com. It is possible for someone to launch a company called Industrial Chemicals and then accuse you of cybersquatting by utilising their name. They actually intend to exploit ACPA to facilitate their own cybersquatting.



Along with the above mentioned four types of cybersquatting there is one more type of cybersquatting known as **Renewal Snatching.**

v. Renewal Snatching:

Renewal snatching, a practise of registering a specific domain name of a website when the original owner of the website fails to renew the domain name registration, is one way that cybersquatting may occur. Since the registration of domain names is valid for a certain amount of time, the owner must have it renewed when it expires. If the domain name is not registered before it expires, someone may purchase it. When a domain name's registration expires, cybersquatters might purchase it and resell it to the legitimate owner at a higher price.

Since domain name registration is only valid for a set amount of time, cybersquatters rely on trademark owners' frequent failure to renew their domain registrations. If the owner doesn't renew the domain registration before it expires, another party may then purchase the domain name. A domain name will be squatted as soon as it becomes accessible. Renewal Snatching is the name given to this action.[12]

2.5 LEGAL SCENARIO IN CASE OF CYBERSQUATTING:

- **US Anti-Cybersquatting Consumer Protection Act, (ACPA) of 1999**

With the introduction of this legislation, the goal was to protect distinctive brand name owners from online squatters. The injured party has two choices:

i. can use the International System of Arbitration by the Internet Corporation of Assigned Names and Numbers, or
ii. to bring legal action against the cybersquatter under the provisions of the Anti-Cybersquatting Consumer Protection Act (ACPA) (ICANN).

In court cases, the issue of jurisdiction is always present. The location of the plaintiff, defendant, or the service provider through which the name is registered should be the trial's venue, according to the courts.

The WIPO Arbitration and Mediation Centre has initiated action to establish an online system for the management of commercial disputes concerning intellectual property. This is a special type of dispute resolution method that is developed to be utilised for both document exchange and evidence filling. The service is reasonably priced and effective. Online arbitration is used in this technique. A trademark owners might attempt to reclaim a site that has been illegally occupied through an arbitration procedure offered by the World Intellectual Property Organization, a copyright agency of the United Nations. 1823 complaints were submitted to WIPO in

[12] Swarit Advisors, supra note 10, at 08.

2006, a 25% increase over 2005's total. According to a report from 2007, 84% of cases brought since 1999 ended in the complainant's favour. It is an organisation with the expertise to create a balanced system that is simple to use.[13]

The Uniform Domain Name Dispute Resolution Policy (UDNDRP), a policy for resolving domain name disputes, was adopted and put into effect by ICANN in 1999. Due to this international policy, arbitration rather than litigation is used to resolve disputes. An action can be brought by any person who complains (referred to by ICANN as the "complainant") that:

- a domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights
- the domain name owner has no rights or legitimate interests in the domain name, and
- the domain name has been registered and is being used in bad faith.

For the complainant to succeed, each of these requirements must be proven. The domain name will be deleted or transferred to the complainant if they win their case. However, the UDNDRP does not provide for financial remedies. The ICANN website contains information on how to file a complaint.[14]

A usual first step in trademark action involving cybersquatting is to write a cease-and-desist letter. This is your chance to let the violator know that their actions are against your rights and that they will probably face legal consequences.

Include the following details, if possible:

- All contact information from IP owner and domain registrant.
- Demand that cybersquatting end and website be transferred.
- Demand that no further cybersquatting activities take place.
- Proof that the sender has exclusive rights to the trademark in question.
- Explanation of further legal action that may take place.
- Deadline for a reply (usually 10 days).

After this, it may be reasonable to file trademark lawsuit under the Anti-Cybersquatting Consumer Protection Act if the infringing behaviour doesn't stop. When this happens, the cybersquatter frequently tries to settle the matter right away or decides not to fight back in court at all, which would result in a default judgement.

You can also submit a UDRP Complaint using ICANN's Uniform Domain Name Dispute Resolution Policy. Compared to ACPA litigation, this administrative process is frequently quicker and less expensive. Cybersquatters are frequently ordered to cancel or transfer domain ownership as a result of plaintiffs' success in court. Sadly, UDRP complaints do not result in monetary awards; the sole prize is the transfer of the domain name.

The Federal Trademark Dilution Act (FTDA), which took effect in 1999, was the primary tool for combating cybersquatting. After the Anti-Cybersquatting Consumer Protection Act was passed, this changed (ACPA). The law established a legal basis for suing cybersquatters, enabling trademark owners to take control of a domain and perhaps collect damages.

Often these types of cases are handled through the Internet Corporation for Assigned Names and Numbers (ICANN). To sue under the ACPA, plaintiffs must prove the following:

- The alleged cybersquatter intended to profit from bad faith registration.
- Defendant registered, used or trafficked in a domain name that is either…
- Confusingly similar or identical to an existing distinctive identifier.
- Confusingly similar, identical or dilutive of a famous identifier.
- The trademark belongs to specific organizations mentioned under U.S. Codes 18 and 36.

Plaintiffs may be awarded injunctive relief, legal costs, and damages that ranging from $1,000 to $100,000 per domain name if their claims are successful in federal court. Many of the same arguments available to other alleged infringers are also available to website owners. For example, if someone registered the name KodakComplaints.com and posted unfavourable reviews of KODAK® items, they would satisfy the first two requirements. They are unlikely to be charged with cybersquatting, though, as their intention is to criticise rather than profit.[15]

- **Aids available to victims of Cybersquatting in India**

In India, there is no cyberlaw that would address the issue of cybersquatting. However, these claims have been heard by Indian courts in accordance with the Trademarks Act of 1991. The victims in this situation have access to two different types of assistance: The Remedy of Violation: This includes managerial remedies, civil remedies (such as account profit and ruling damages), and criminal remedies (such as the suspect's imprisonment) (like the ban on import of invading copies). Only if the domain name of the website has been registered by the genuine owner under this Act is this form of remedy permitted under the Trademark Act.

The Passing-Off Remedy: This remedy entails the true owner applying for an injunction to prevent use of the domain name by another business or person. No prior registration for a domain name is necessary if the injured party wants to use this remedy.[16]

There is no domain name protection law and cyber squatting cases are adjudicated in India under the Trade Mark Act, 1999. The Uniform Domain Name Dispute Resolution Policy (UDRP) procedure, designed by ICANN, is primarily used to settle disputes concerning registrations made in bad faith. WIPO was created as a means of promoting the protection, use, and distribution of intellectual property around the world and is the top organisation accredited by ICANN to conduct domain name dispute resolution services under the UDRP. India is one of the 171 nations that make up the WIPO.

An individual can lodge a complaint before ICANN approved administrative dispute resolution service providers under Rule 4(a) that:

[13] iPleaders, supra note 1, at 02
[14] Nolo, supra note 6, at 03
[15] Mandour Law, supra note 2, at 02.
[16] Swarit Advisors, supra note 10, at 08.

- The domain name shall be "identical or confusingly similar to a trade mark or service mark" over which the claimant has rights.
- The owner / registrant of the domain name has no right or legitimate interest regarding the domain name.
- Domain name is registered and used in bad faith.

India has also established its own registry under the name IN Registry with the help of the National Internet Exchange of India (NIXI), where the.IN Dispute Resolution Policy is used to resolve domain name disputes (INDRP). The Indian Information Technology Act of 2000's pertinent provisions and generally accepted concepts were taken into consideration when developing the strategy. The IN Domain Name Dispute Resolution Protocol (INDRP) and INDRP are the protocols that govern how disputes are resolved under the IN Registry. These rules outline the manner in which a lawsuit, associated costs, correspondence, and the relevant process will be filed.

The Hon'ble High Court of Delhi held in **Aqua Minerals Limited vs. Mr. Pramod Borse & Anr**[17] that until and unless a person has a legitimate reason for why he wants to register a particular domain name, there will be no interference drawn that the aforementioned person preferred to trade under the name of the trade name he had chosen for registration or as a domain name because it was an existing name with a common prestige and popularity at immense.[18]

SOME INDIAN CYBER-SQUATTING CASES:

Yahoo! Inc. v. Akash Arora

It is the first case that was reported in India regarding cybersquatting. In this case, plaintiff was a registered owner of the domain name "yahoo.com". He obtained an interim order which restrained the defendants from dealing the name "yahooindia.com" or any other trademark similar to the trademark of the plaintiff.

Tata Sons Ltd Vs. Ramadasoft

In this case, the defendant had a domain name registered in the name of Tata. It was held in this case that domain names not only involve addresses but also the trademarks of the companies. The domain names in this case, were similar to the plaintiff's trademark and that the defendant had used the names with mala Fide intentionThese facts entitled the defendant to transfer the domain names in the favor of the plaintiff.

Sbicards.com vs. Domain Active Property Ltd.

The administrative panel, in this case, said that defendant an Australian entity had a registered domain name which was registered with the mala Fide intention and it could have attracted attention from the public because of its affiliation to SBI Cards products and services.[19]

3. CONCLUSION AND OPINION:

Cybersquatting is the unethical and unlawful practice of buying a domain name with the intent of profiting from someone else's trademark. It is done by creating a similar domain name and attracting traffic to your duplicate site. Cybersquatting is the act of purchasing, selling, or utilising a domain name with the purpose of making money off of the reputation of another person's brand. It usually refers to the practise of acquiring domain names that incorporate the names of already-existing companies with the intention of selling the names to such companies for a profit. In cybersquatting, a domain name is licenced, sold, or used with the intention of making money off of someone else's trademark. Typically, this refers to the practise of purchasing domain names that contain the names of real companies with the goal of reselling the names to other companies for a profit. The majority of the time, a cybersquatter will purchase a domain name that is similar to the name of a well-known company or celebrity in order to profit from on-site advertisements or try to sell the domain to the trademark holder at a premium price. The chance for cybersquatters, however, arises when a copyright holder forgets to renew their domain registration, allowing cybersquatters free to pounce and register their already existing domain for themselves.

There are various types of cybersquatting namely:

a) Typosquatting
b) Name jacking
c) Identity Theft
d) Reversal Cybersquatting
e) Renewal Snatching.

There is no active law as such for this cybercrime in India, on the basis of data received by survey it has been drawn people are unaware about this crime even they are suffering. Since many cybersquatting sites always try to trick our computers into sending our private details or attempting to install malicious software on your device, it is vital that you have the proper vulnerability management in place before you go to investigate. A controlled protection company will help you secure your personal data and your business from phishing malware and other threats. One of the easiest and by far the most important moves here is choosing multiple top-level domains and building a page on them all. It could be shockingly successful to assign a name on many domains like.com,.org or one of the other top tier domains like.me domain.

Customers of a legitimate business may suffer fraud, data theft, or other types of harm as a result of cybersquatting. By doing this, the company runs the risk of being held liable or, at the very least, losing the trust of customers and investors.

Cybersquatters can create a site that looks similar to a company's in order to communicate with its target audiences without even having to breach the company's Domain Name System (DNS).

Perhaps more worrisome is the chance that a worker will click on a link in an email that appears to have been sent by the company. Employees who do this risk exposing the company's computer systems to viruses or outside attack.

[17] Acqua Minerals Limited vs Mr. Pramod Borse & Anr, AIR 2001 Delhi 463.
[18] Indian Law Portal, supra note 8, at 04.
[19] iPleaders, supra note 1, at 02