IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Domain name vis-à-vis Trademark in reference to Cyber Squatters

[1]Mausam Thaker, [2]A.K. Tripathi and [3]Ravi Sheth

[1,2,3] Raksha Shakti University, Lavad, Gujarat, India

DOI: https://doi.org/10.26438/ijcse/v7i5.10681075 | Available online at: www.ijcseonline.org

Accepted: 16/May/2019, Published: 31/May/2019

Abstract : Domain name is meant to locate the web address on internet but in today's era domain name has gone very far from the purpose of domain name. Now generally domain names are used to identify the goods and services which a particular manufacture, company and service provider is offering be it offline or online. As per prevalent practices registration of domain name being not as stringent as that of trade marks lead to the practice of cybersquatting. In plethora of judgments Courts have responded positively to have resolved the disputes applying the principles of trade mark and passing off laws. It automatically speaks that domain name and trade mark are different concepts but on the ground of unavailability of the law in pertain to domain name cyber squatters may not be allow to play with the laws. The paper covers lack of laws in India, history of cyber squatters, cyber squatters position in India and working of ICANN and ACPA.

IndexTerms **-** Trademarks, Domain name, Cyber squatters, GTLD, ICANN and ACPA

I. INTRODUCTION

With the advent of the Internet, the world today is witnessing a revolutionary change in the field of communication. To convergent digital environment has the feature of being, in term of costs of delivery, not as related to distance as conventional India. In respect of the internet, a specific feature called logical addressing has been developed which allows the user to reach a graphical or multimedia location where information is delivered to him in an interactive way. Both these issues may have an impact in respect of trade mark protection. The internet seems to have exploded on the forefront of several commercial establishments, organisations, governments and institutions. Showing an Internet address has become very important for almost every organisation. It goes without saying that as the awareness of the internet grows, the number of web sites grow correspondingly. Such growth of web sites has also given rise to a new area of disputes – Domain Name disputes. A Trade Mark can be defined as a distinctive design, picture, emblem, logo or wording affixed to goods for sale to identify the manufacturer as the source of the product. The question that attracts the attention of anybody is, does a Domain name come under the definition of a Trade Mark? The answer is found when both their nature and scope are analysed – under law a Trade Mark is used in commerce to represent a product or a business while on the other hand a Domain name is a word or a phrase registered in the Domain name system. Moreover a Domain Name is not a corollary to the trademark system. Nevertheless, previously decided Domain name disputes have given Domain name as much protection as Trademarks. In Indian stand point on the status of Domain Names is also encouraging as in the Rediff case it was held that a Domain Name is more than an internet address and is required equal protection as Trademark. Further buttressing the strength hold of Domain name in the ever growing scope of e-commerce is the fact that consumers have now begun to attribute Domain names with goodwill, reputation, dependability and brand following similar to that of a Trademark. Cybersquatting is a form of speculation where a domain name is registered with the intention of spelling off the same. Cyber squatting is the preparation so that a person or legal entity books up the trade mark, business name or service mark of another as they have domain name for the reason of holding on to it and then selling the same domain name to someone else for best premium and consideration. Cyber squatters book up domain name of important brands in the hope of earning quick millions. The paper gives an overview of the connection between Trade mark, Domain name and some issues of cyber squatting

II. TRADE MARK

Procedure and Duration of Registration of Trademark.

- When an application for registration is made to the registrar, he may accept or refuse, or refuse after having accepted the same, if the condition so demands. However, one does not get a proprietary right over a mark merely by virtue of applying for the registration of the said mark as his trademark. The accepted applications are advertised and any person who thinks he may be aggrieved by the prospective registration of the trademark, may, within three months make his position known to Registrar in a pre subscribed manner. The registrar shall dispose of the matter after giving both parties an opportunity of being heard.
- Registrar may permit corrections of errors or amendments, if any, in the application on the request of the applicant whether before or after his acceptance of the application.

Having cleared all there decks, the application reaches the registration stage; and if there is no direction from the Central Government to deny registration of the trademark mentioned in the application, the registrar shall register the trademark. Generally, a trademark is owned by only one person, but under special circumstances, two or more persons may also be registered as joint proprietors of a trademark.

- The registration of a trademark is initially made for a period of ten years but may be renewed from time to time by payment of a prescribed fee. Before the expiry of the renewed term, the registrar gives notice to the proprietor to get it renewed for another term by depositing prescribed fees and fulfilling other conditions, if any, mentioned in the notice. If the proprietor fails to comply with the notice and conditions prescribed therein, the registrar will remove the trademark from the register after its present term expires. However, even one year after such removal the said trademark shall be treated as good as a registered trademark, for the purpose of registration of new trademarks.
- When an application for registration of a trademark is advertised, an interested person may oppose the registration by giving in the prescribed form notice to the Registrar, and the Registrar has to decide the case after hearing both the parties. However, when he has arrived at a decision and thus disposed of the case; the aggrieved can make an appeal against it before the Appellate Board. In this respect, the Court has held that the Registrar himself cannot review his own decision as the Act does not authorize him to do that.

III. CONCEPT OF DOMAIN NAME

At the time when the DNS was inexistent, the alternative left with an individual was to literally download the Host file that had details of the hostnames and their respective IP addresses. With the proliferation in a number of hosts of the internet, the capacity of the host file also significantly increased. As a result of which, there was increased traffic on downloading this file. To solve this problem the DNS system was initially introduced. It is imperative to understand that the Domain Name System helps to resolve the hostname to an address. It uses a hierarchical naming tactic and distributed database of the IP addresses and its associated names.

IP Address: IP address can be understood as a combination of 32-bit number whereas the domain names are easy to remember names. For instance, while we attempt to enter an email address, we essentially enter a symbolic string redirecting to the desired location.

Uniform Resource Locator: Uniform Resource Locator (URL) redirects a user to a web address that can be uniquely identified as a document over the internet. These documents can be anything from a web page, image, audio, video to any random information that is present on the internet. There are two types of URL:

Absolute URL: An Absolute URL can be understood as a complete address of a particular resource located on the web. The address mainly constitutes the protocol used, the server's name, path's name, and file name.

Relative URL: Relative URL can be understood as a partial address of a particular webpage. The protocol and server part are omitted from the relative URL, unlike the Absolute URL. Relative URLs are mainly used for the internal links to create the links to a file that is part of the same website as the Webpages, on which, you are placing the link.

Domain Name: TLD – Top Level Domains

These can be understood as the highest level in the entire DNS structure of the internet. There are varied types of TLD's:

1. CCTLD: Country Code Top Level Domains
   - Two-letter domain well-known for geographical location; eg; .in means INDIA
   - When genuinely selected, normally only people of a country could register their corresponding ccTLD; but from last few years quite a rare countries have owed parties their shores to register website name.
   - In the case of the .in domain name, firm rules are still in place. Eg; .com.in registrants must still be INDIAN or have registered business interests in India. The registration admissibility criteria for the .in name has meant .in is still sturdily connected with India and has fostered a great deal of trust and assurance in local and even foreign online shoppers.
2. GTLD: Generic Top Level Domain
   - The best known generic TLD's contain .com, .net, .biz, .org and .info-these can be registered by anyone, anywhere in the world. However, some of the new gTLD's are more recently released have various limitations/boundaries.
3. IDN CCTLD: Internationalized Country Code Top Level Domain
   - A top-level name with an specially encrypted format that permits it to be showed in a non-Latin character set. (i.e special character).
4. Subdomain
   - Part of a higher-ordered domain name is DNS hierarchy; eg- domainregistration.com.in
   - Subdomain offers some services 'registration' but this naturally isn't perfect for business and should possibly be stooped for generating a commercial website as the registrant for the upper order name has control on the address. Having your name can also benefit with integrity.

THE PROCESS OF REGISTERING A DOMAIN NAME

- To reserve a domain name in a gTLD, the registrant must be registered with an ICANN-accredited registrar. The registrar will determine the availability of the domain name and create a WHOIS record with the information of the registrant. It is also plausible to register the domain names through a registrar's resellers.
- A registrant can be understood as the person or organization who has booked or registered the domain name. To do so, the domain name registrant may apply online to a domain registrar or to one of their resellers. The registrant is usually restricted by the terms and conditions of the respective registrar, with which, it gets to register the domain name, for instance, agreeing to a certain code of conduct or indemnifying the registrar and registry against any potential legal or civil action taken as a result of the use of the domain name. Domain name registrants essentially have certain responsibilities that are incorporated into the terms and conditions like payment for the registration fees and its submission and the timely update of accurate data.
- In addition to the registration of the domain name, the domain name registrants should also have their domain names listed on the name servers to ensure for that domain name to be reachable over the Internet. A domain name registrant is primarily responsible for procuring or hosting his or her own name server and if the registrar doesn't offer the service or he/ she has opted out of the registrar's service.
- In some cases, a person or organization who is not willing to have their information listed in the WHOIS may contract with a proxy service provider to register the domain names in their name. In such a case, the service provider is a domain name registrant and not the end customer.
- Registrars can be understood as the organizations accredited by the ICANN and certified by the registries to sell their domain names. Registrars are significantly bounded by the (RAA) Registrar Accreditation Agreement along with ICANN and by their mutual agreements with the registries. The RAA mentions out the responsibilities for all the registrars which also includes the maintenance of the WHOIS data, submission of the data to the registries, facilitating public WHOIS queries, and ensuring domain name registrants details are escrowed, and complying with RAA conditions are in relation to the conclusion of the domain name registration period.
- Some domain name registrants may consider registering through a reseller and these organizations are mainly affiliated or under the contract with registrars, and usually offer other services such as hosting, email mailboxes, etc. Resellers are restricted by their agreements with the registrars whose services they deal in; they are not accredited by ICANN, however, the registrar for whom they are reselling will still be the main sponsor for domain name registration and responsible for the domain names which are sold by the reseller.
- While the registrars are contracted to conduct the day-to-day operations of selling the domain name registrations, the registries are primarily responsible for the maintenance of the registry for each TLD. The responsibilities of the registries include the acceptance of the registration requests (which can be from registrars or directly from domain name registrants), maintenance of the database of the mandatory domain name registration data and providing the name servers to publish the zone file data throughout the Internet.
- The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that supervises the assignment of both IP addresses and domain names. It is responsible for managing the root server and TLD name system management. It has contractual agreements with both registries and registrars that provide the foundation for the WHOIS system.

RESPONSIBILITIES OF THE ICANN

To reach out to other individuals on the Internet, one has to feed the address into your computer. The address should be unique to enable the computers to figure out where to find one another. ICANN coordinates with these unique identifiers across the world. Without such coordination, we would not have one global Internet.

To get into the technical understanding, the Internet Corporation for Assigned Names and Numbers (ICANN) assists in the coordination of the Internet Assigned Numbers Authority (IANA) functions which are the key technical services pertinent to the continued operations of the Internet's address book, the Domain Name System (DNS). The IANA functions mainly include:

1. The coordination of the assignment of the technical protocol parameters that includes the management of the address and essential routing parameter area (ARPA) top-level domain.
2. The administration of certain responsibilities associated with the Internet DNS root zone management like the generic (gTLD), and country-code (ccTLD) Top-Level Domains.
3. The distribution of Internet numbering resources.
4. Other miscellaneous services.

WORKING OF THE ICANN

Apart from providing the technical operations of DNS resources, ICANN also essentially defines the policies for determining the ways in which, the "names and numbers" of the Internet should execute. The task is promoted in a style, in which, we describe as the "bottom-up, consensus-driven, multi-stakeholder model"

1. **Bottom-up:** At ICANN, rather than the Board of Directors solely declaring what all topics ICANN addresses, members of the sub-groups in the ICANN can raise issues at the grassroots level. If the issue is worth addressing within the ICANN's sphere, it can increase through various Advisory Committees and Supporting Organizations until eventually the policy recommendations are passed to the Board for a vote.
2. **Consensus-driven**: Through its processes, bylaws, and international meetings, ICANN provides an arena where all the advocates can decide the Internet policy issues. Anyone can join a majority of the ICANN's volunteer Working Groups that assures the broad representation of the world's perspectives. Taking a keen cognizance all the viewpoints, searching for the mutual interests, and working towards ensuring comprehensive consensus takes significant time but the procedure resists capturing any single point of interest– an important consideration whilst managing a resource as vital as compared to the global Internet.
3. **Multistakeholder model**: ICANN's all-inclusive approach treats the public sector, the private sector, and technical experts as a team. This shall enable you to find the registries, the registrars, the Service Providers of the Internet facilities (ISPs), intellectual property advocates, commercial and business interests, noncommercial and the non-profit interests, the representations from over 100 governments, and also a global array of individual Internet users in the ICANN community. All the points of view receive consideration on their own merits. ICANN's fundamental belief is understanding that all the users of the Internet deserve a say in how it is run.

IV. LEGAL SCENARIO IN CASE OF CYBERSQUATTING:

Due to the advent of online transactions, e-business, e-comers, and e-communication, our day-to-day life has become easier. This practice leads some critical issues in a cyber arena like- Identity, territorial, jurisdiction, and unavailability of laws. In cyberspace, the first and for the most challenge is to execute or to activate the justice system.

U.S. Anti-cyber-squatting Consumer Protection Act (ACPA) 1999:

The introduction of this act was done with the intent of providing the assurance of protecting the trademark owners of distinct names of the trademark against the potential cyber squatters. The person who went through the theft have the following two options:

1. To essentially sue the cyber squatter under the recommended provisions of the Anti-cybersquatting Consumer Protection Act (ACPA)
2. Making use of the International System of arbitration by the Internet Corporation of Assigned Names and Numbers (ICANN).

- One of the biggest problems in the case of courts in the jurisdiction and according to the courts, the seat of the trial should either be the place of the plaintiff, the defendant, or it can be the place of the service providers, through which, the name is initially registered.
- The World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre has taken essential steps to offer an Internet system for the comprehensive administration of the commercial disputes that involve the matters pertaining to intellectual property. This stands as a unique form of a mechanism intended to provide solutions and this system is introduced to be used for both filling of evidence and for document exchange purposes. It is an efficient and inexpensive service where the arbitration can take place online.
- On the international forum, the United Nations copyright agency WIPO (World Intellectual Property Organization) has essentially provided a system of arbitration wherein the holder of a trademark can make attempts to claim a squatted site. In the year 2006, there were a whopping 1823 complaints filed with the WIPO and this was a rise 25% rise over the 2005 rate. In the year 2007, it was essentially suggested that 84 % of the claims filed since the year 1999 went to the favor of the complaining party. This agency specializes to maintain a balanced system that is easily accessible.

POSITION IN INDIA

In India, the victims of cybersquatting have a number of ways to deal with the unpleasant consequence and these include the following:

- Sending the cease-and-desist letters to the cybersquatter.
- Opting for the arbitration under the ICANN's rules,
- Attempting for a trial in a state or federal court.

To bring the case on a fast track form of resolution and expedite the procedure, the case could be filed with the registry which is handled by the National Internet Exchange of India (NiXI).

In India, there is a lack of specific provisions to punish the cyber-squatters. Also, the IT Act does not significantly proffer for any legal compensation but, the registry has now taken steps to provide compensation to the victim companies.

What is Cyber Squatting

In situations, where an individual or a company book a domain name that is similar to a trademark of any other party and tries to sell the same for a profit. This concept is known as "Cybersquatting."

Understanding the Roles of Cybersquatters.

Cybersquatters may attempt to attract people from the competitor websites by including the names of the rival organizations in the metatags.

Categories of Cyber Squatting

Cybersquatting can be executed in several ways, however, typosquatting can be considered as the most popular form of cybersquatting.

It is premised on the fact that people using the internet are bound to make typographical errors while entering domain names into individual browsers. Some of the common examples are as follows:

- If a person removes the "dot" while typing the domain name: www.example.com;
- The potential misspelled name of the intended site: exemple.com
- The differently phrased name: examples.com
- Any other potential top-level domain: example.org

The other reality that a cybersquatter usually relies on is that in situations when the trademark holders own the domain name often forgets to re-register his domain names after the expiry. The registration of the domain name may not be for a fixed period and in case the domain name is not re-registered before its expiration, the domain name can be purchased by any individual. In situations where cybersquatters register a domain name that aligns with the initial registered name. The process is commonly called as "renewal snatching."

History of Cybersquatting

The common practice is commonly known as the cybersquatting actually originated at a time when most of the businesses were not technically used to and aware of the financial opportunities available on the Internet. Several firms register the names of commonly-known companies as their domain names, with the intent of selling these domains back to the companies when they finally realize. Panasonic, Fry's Electronics, Hertz and Avon were among the most popular "victims" of the cybersquatters. We have to understand that the opportunities for the cybersquatters are rapidly reducing because most businesses now know that domain names are of a high priority.

Recognizing the Cybersquatting

- How do you figure out that the domain name you wish to have is actually being used by a cybersquatter? To understand that, one may follow these steps to find out.
- Crosscheck whether the domain names take you to the ideal website. If it does not take you to the functional and operational website and instead, it takes you to a website that may essentially state "this domain name for sale," or "under construction," or "can't find server," the similarity exponentially increases and indicates that you may be essentially dealing with a cybersquatter. The absence of any real website may essentially indicate that the owner of the domain name intends to buy the domain name and to sell it back to the owner at a comparatively higher price.
- It is for sure that the absence of a website may not always essentially mean that the presence of a cybersquatter. There can be circumstances where the domain name owner may have perfectly legit plans to have a website in the future with the same domain name.
- If the domain redirects you to an operational website that is illegally comprised primarily of advertisements any project related to your trademark, you may also face a case of cybersquatting. For example, if a company is eminent and known for providing the audio-visual services and the website you are redirected to is full of advertisements for a different company's audio-visual services, there are chances that the site is maintained by a cybersquatter who is making profits out of your company's eminence to sell Google ads to your competitors.
- If the domain name takes you to a web portal that appears to be operational and is also having a reasonable relation to the domain name, but it does not compete with your range of services, you probably are not involved in a case of cybersquatting. For example, if your trademark is "ABC XYZ" for fine art dealing with whaling and the website you come across (www.abcxyz.com) is for street maintenance, you do not have a case of cybersquatting. However, you may, under certain circumstances, have a situation of infringing of the trademark.

Various options available to fight against the concept of Cybersquatting

Victims of cybersquatting may have the following two options:

- Sue under the provisions of the Anti-cybersquatting Consumer Protection Act (ACPA), or
- Using an international arbitration system that is created by the Internet Corporation of Assigned Names and Numbers (ICANN).

The experts of the trademarks effectively consider the ICANN arbitration system to be quick and frugal than suing, also, the procedure essentially does not require an attorney.

Making the use of the ICANN Procedure

In the year 1999, the ICANN adopted and started implementing the Uniform Domain Name Dispute Resolution Policy (UDNDRP) as an essential policy for the resolution of the disputes of the domain name. The international policy results in the arbitration of dispute and not litigation. Actions can be essentially brought by any person who is complaining:

- Domain names are identical and similar to the trademark or the service mark, in which, the complainant has rights.
- Domain names owner have absolutely no rights or legit interests in the domain names
- Domains names have been registered and are being used with negative intent.

All of the aforementioned factors must be established for the complainant to sustain. If the complainant prevails, the respective domain name will be canceled or transferred to the complainant, however, financial remedies may not be available under the UNDP. Information.

Suing Under the ACPA

Anti cybersquatting Consumer Protection Act (ACPA) allows a trademark owner to sue a supposed cybersquatter in the court and obtain a court order that orders for transferring the domain name back to the trademark owner. In some situations, the cybersquatter needs to pay money damages.

To stop a cybersquatter, the trademark owner must prove all of the aforementioned points:

1. The registrant potentially had a malicious intent to generate profit from the trademark
2. The trademark was distinct at the time of first registration
3. The domain name is confusingly similar to the initial trademark
4. The trademark qualifies for legal and legit protection under applicable laws -- that is, the trademark is distinct and the initial owner was responsible for the inception of the trademark in commerce.

- Defences to lawsuits. If an accused cybersquatter suggests that he is potentially having a reason for registering the domain name instead of selling it back to the trademark owner for generating profit, then a court may probably allow him to keep the domain name.
- One may consider asking Google Assistant, Cortana or Alexa to search for your business online and instead of your domain, you're essentially redirected to a page with a domain name confusingly identical. That is an ideal situation of domain squatting.
- One should resist the desire to yap a few harsh words. The culprit may not be an ideal and favorite form of artificial intelligence.
- Also referred to as cybersquatting, the concept of domain squatting is shifted from being completely legal to falling in a grey area and is permissible in some cases and illegal in others.

The concept of domain squatting

How can we ideally determine the concept of domain squatting? It's imperative to understand the disparity between the legit use of purchasing and selling the domain names. In short, it all comes down to the real intent. Domain name squatting can be understood as an act of purchasing a generic and top-level domain (gTLD) to block someone else from re-registering it for conducting any sort of financial activity.

Domain squatting significantly differs from the concept of domaining. In domaining, we emphasize buying domain names which may have potential value to a number of buyers on the basis of their habits, interests, and trends. The domain can be auctioned on the domain aftermarket to the highest bidder and is sold to them through a domain broker.

Why be a part of the domain squatting?

1. It may essentially seem to be baffling as to why someone would even register the domain name of small business, especially if you have just started the business process. Ideally, they should go after the big names that would potentially be of more value. But why would someone even want with thesmallnewbusinessname.com? And also, how did they manage to register them in the first place?
2. Domain name squatters are the ones who purchase the names of famous people or brand names and often, they reach out to the related people or the businesses aspiring to charge more than they paid. Often, they use these domain names to post explicit content, this actually happened in the case of Madonna, whose name was unfortunately used for a porn site. They may even post positive content which was possible in the case of Julia Roberts fan who registered her name, however, both the celebrities fought back and won the case.
3. Generating Profits from the ads can be another motive for domain squatting. Misspelling a brand name intentionally and then posting ads to those who visit there unintentionally can essentially be lucrative.

- When it comes to new and barely-known names, the domain name squatters do not need to look further than the official public notices for the newly registered limited liability companies and business license records or other registries for their small businesses and organizations. When they understand that the name has not been registered yet and the fictitious name is referred to as doing business as (DBA) name, they get these names often for pennies on the dollar.

1. The risk is worth it primarily because there are chances one would rather pay the domain squatter the demanded price instead of refiling the paperwork, reorder business signs, etc., just at the inception of a new business.
2. The same is effectively applied to a professional domain investor who may regularly scour the database to comprehend the recently expired domains and use the same to divert the traffic to their site or sell to a new or previous owner. If the site is not yours, chances are, it is of a cyber squatter.
3. The General top-level domains are based on the copyrighted works and the phrases are protected under the Applicable Policy. This also essentially means that the owner of a copyright or trademark may have the claim on domains registered with negative intent.
4. Buying the domains with an intent to damage a competitor and profit from an assumed connection between the one that is copyrighted and owner of the domain, or an attempt to intentionally block the rightful owner from registering the name themselves would be considered as acts of negative intent.

Procedure for re-claiming the squatted domain

If you suspect that a particular domain name potentially infringes your copyright or trademark, you can surely contact the owner of the domain or proceed with filing a UDRP claim or court proceeding.

You may be required to file a complaint, whilst considering the need to communicate it in as all possible ways. Select an Internet Corporation for the (ICANN) approved provider to comprehensively monitor the administrative proceedings and stay ready to display the evidence of the trademark or copyright ownership at your end and the intent of generating profits on the part of the accused domain squatter.

Preventing domain squatting

It's convenient to avoid being a victim of domain squatter than following the aftermath steps. Following are five tips that can significantly help to prevent losing a domain in the future:

1. Register the domain you require before you ay potentially put that to use
2. Proactive methods are required. Merely adding a domain to your cart does not essentially prevent others from purchasing it. Domain squatters often purchase the recently searched domain names in aspirations to sell it to the original person who searched for it.
3. One may effectively register similar names
4. One may consider buying domains with multiple extensions including .com, .co, .biz, etc., and this will considerably prevent the squatters from purchasing them. One may also make a research on the common misspellings of their domain name and registering them as well.
5. Domain ownership protection can be purchased too.
6. GoDaddy proffers Protected Registration to ensure that you retain registration of your domain name, irrespective of the expiration dates or attempts to transfer.
7. One may effectually register a trademark
8. Attempt to establish your legal right to the domain by registering it with the concerned authorities.
9. On the record

You can also prevent someone else from holding on your domain hosting. If an employee or third-party registers a domain name on your name, make sure it is done in your name.

V. SOME CASES OF CYBER SQUATTERS IN TABLE FORM:

There are many cases of cybersquatters were registered in India, the following table contains the cases of cyber squatters with the company's original Domain Name and name used by the Cyber Squatters to harm the goodwill of the owner and to get profit by misusing the name/fame of the company.

Sr. No.	Name of the company	company's original domain name	Company's fake domain name
1.	**Amazon**	www.amazon.in	www.amazone.in
			www.amazoñ.in
			www. ãmazon.in
			www.àmàzon.in
			www.amązon.in
2.	**Sony**	www.sony.co.in	www.soni.in
3.	**Apple**	www.apple.com	www.apÞle.com
			www.applę.com
			www.ąpple.com
			www.apple.cf
			www. ąpple.cf
4.	**Adobe**	www.adobe.com	www.adobe.com
			ns1. adobe.com
			ns2. adobe.com
			adobe.com
5.	**Google**	Google.in	Googlee.in
6.	**Starbucks**	www.starbucks.co.in	www.starbucks.in
7.	**Morgan Stanley**	www.morganstanleybank.co.in	www.morganstanley.in
8.	**Yahoo Inc. v. Akash Arora & Anr.**	www.yahoo.com	www.yahooindia.com
9.	**Rediff communication Ltd. v. Cyberbooth**	www.rediff.com	www.radiff.com
10.	**Titan Industries Ltd v. Prashanth Koorapati & others**	www.tanishq.co.in	www.tanishq.com
11.	**Dr. Reddy's Laboratories Ltd v. Manu Kosuri**	www.drreddys.com	www.drreddyslab.com

12.	**SBI Cards and payment Services Private Ltd v. Domain Active Private Ltd**	www.sbicard.com	www.sbicards.com

VI. CONCLUSION:

- It is evident that strict laws are immediately required in this field to penalize the squatters and make attempts to avoid these crimes in the future. Legal remedies should be provided to the service mark and Domain Name owners to protect themselves against the Defendants who aspire to obtain the domain names with malicious intent. The plaintiffs should have an option to obtain statutory damages and this will significantly act as a significant tool that can potentially help the Domain Name holders to protect their intellectual property in the digital establishments.

VII. REFERENCES:

[1]. J. P. Mishra "INTELLECTUAL PROPERTY RIGHTS", Central Law Publications, India, pp. 265-274, 2012.

[2]. Steven Wright, "Cybersquatting at the Intersection of Internet Domain names and Trade mark Law", IEEE Communications Surveys & Tutorials, Vol.14, No.1, First Quarter 2012.

