THE MENACE OF CYBERSQUATTING AND THE AVAILABLE LEGAL MEASURES TO MITIGATE ABUSE OF DOMAIN NAMES

Sangeetha Lakshmi V, Tamil Nadu Dr Ambedkar Law University, Chennai

ABSTRACT

Internet has become a very powerful tool, having the ability to create jobs, curtailed international communications barriers and shortened political and social boundaries. The challenge we are facing in recent years is, how to strengthen and authenticate the intellectual property rights on the Internet and prevent its unauthorized use. Cybersquatting is one of the riskiest menace which has no boundaries of compound ability and is similar to the passing off of Trademarks. The Cyber security and defense mechanisms fight against newly emerging problems and find legal solutions for the the cybersquatting. In this web of the internet called "Cyberspace" the most common way for consumers to find out what they are looking for, is to type the Domain name of the brand or company they look for. The natural connection between trademarks and domain names has been explored by some who have the trademarks of others as domain names and then tried to sell those domain names back to the trademark owners or third parties at a high price, this is cybersquatting. These are the various types of cyber squatting. .What emerges from these factors is that the Internet domain names are of importance and can be a valuable corporate asset. Some countries have specific laws against cybersquatting beyond the normal rules of trademark law. The introduction of a strong Digital Global platform for all traders to interact and interface in an authenticated manner would be the solution to curb cybersquatting.

Keywords: Cybersquatting, Domain-name abuse, Passing-off, Trademark Laws, Cyberspace Laws

INTRODUCTION

The World Wide Web has revolutionised big industrial movements of the 19th century. Internet is now predominantly used for business transactions, governmental policies, social interaction etc. It has comprehensively covered technology and acquisition of data. It has provided opportunities to millions and also brought liabilities to many especially in the field of intellectual property, data privacy etc. As we all know Internet has become a very powerful tool, having the ability to create jobs, curtailed international communications barriers and shortened political and social boundaries. The challenge we are facing in recent years is, how to strengthen and authenticate the intellectual property rights on the Internet and prevent its unauthorized use.

Cybersquatting is one of the riskiest menace which has no boundaries of compound ability and is similar to the passing off of Trademarks. The Cyber security and defense mechanisms fight against newly emerging problems and find legal solutions for the the cybersquatting. This paper has attempted at explaining about the offence of cybersquatting, the methods in which the squatters misrepresent and the legal solutions to combat the problems. Usually, we have addresses for our homes and offices. The same way domain names are nothing but simple forms of addresses on the internet. These addresses enable users to locate websites on the net in an easy manner. Domain names correspond to various IP (Internet Protocol) numbers which connect various computers and enable direct network routing system to direct data to the correct addressee. In other words a domain name is a “uniform source locator”. The misuse and abuse of such domain name leads to the crime of cybersquatting.

DEFINITION OF CYBER SQUATTING

Cybersquatting is referred to as "the abusive registration of trademarks as domain names".[1]US law defines cybersquatting as “registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else.” [2] In this web of the internet called “Cyberspace” the most common way for consumers to find out what they are looking for, is to type the Domain name of the brand or company they look for. The natural connection between trademarks and domain names has been explored by some who have the trademarks of others as domain names and then tried to sell those domain names back

[1] http://news.domainmonster.com/cybersquatting_domain_problems/)
[2] http://www.lexero.com/practices/domain-name-attorney/types-of-domain-name-disputes

to the trademark owners or third parties at a high price, this is cybersquatting. Cybersquatting is the most crucial type of domain dispute prevalent around the world. This definition is well established in**, Manish Vij v. Indra Chugh,**[3] the court held that "an act of obtaining fraudulent registration with intent to sell the domain name to the lawful owner of the name at a premium". This is an abusive practice which is a form of trafficking domain names. Cybersquatting is the practice of registering a trademark as a domain name with the intent of profiting from it by selling it, usually to the trademark owner. As long as the cybersquatter owns the domain name, the trademark owner cannot register his own trademark as a domain name. In this way, the squatter breaches the fundamental rights of the trademark owner to use its trademark. Cyber squatters typically have no use for these domain names, except to resell them and turn a profit. Many multinational companies like Tata, Bennett & Coleman, Mc Donald's etc were among the first victims of cybersquatting. Many cases are also decided by the WIPO (World Intellectual Property Organization) and ICANN.

HISTORY OF CYBERSQUATTING

Before 1999, the business world was still in need of Internet as a tool for success. They didn't know the need to register their trademarks as domain names. Gradually, cyber squatters started to see the increasing importance of the Internet, and felt the mistake of ignoring it. This is how cyber squatting was born and began causing problems. Cyber squatters took advantage of those companies by registering domain names identical or similar to the business' trademarks. Domain name registrars accept all applications for domain names by applicants unless that exact identical name is in use. After the cyber squatter has the domain name registered, the company can no longer have their trademark as their domain name. This causes a problem since customers and clients frequently try to find businesses online.

One of the first cyber squatters were Dennis Toppan in the early 90's who registered some very famous marks before companies did. He then demanded a ransom of $13,000 for each domain name[4]. This type of cyber squatting causes firms to lose money not only by paying cyber squatters to get their domain names, but as a loss of profit for what they could be making with an effective website. This could take away the reputation of a company and business they had at one point. Cyber squatting cause's monetary losses and damaged reputations. Businesses were not happy when these issues become apparent to them. They

[3] All India reporter 2002 Del 243
[4] http://faculty.ist.psu.edu/bagby/Fall05/346F05T8/history.html

have learned of the important benefits of owning their trademark domain names. Congress decided to take action in 1999 to help out businesses and stop cyber squatting. The laws and acts passed helped businesses battle, the decrease in cyber squatting.

TYPES OF CYBERSQUATTING

"Cybersquatting is the practice of registering a trademark as a domain name with the intent of profiting from it by selling it, usually to the trademark owner". So we need to know what a trade mark is. Trade mark means a "mark capable of being represented graphically and which is capable of distinguishing goods and services from one person of others and may include shape of goods, their packing and combination of colours."[5]

Cyber squatting can be of various types:

1. Typo squatting

The most common type is typo squatting, when a cyber squatter registers domain names containing variant of popular trademarks. Typo squatters mainly rely on a fact that Internet users will make 'typographical errors' when entering domain names into their web browsers.

Some common examples of typo squatting includes:

i) the omission of the "dot" in the domain name: wwwindia.com .ii) a common misspelling of the intended site: india.com.iii) a differently phrased domain name: indias.com. iv) A different top-level domain: india.org.

2. Reverse-Cybersquatting

Reverse cybersquatting occurs when a trademark holder attempts to wrestle a domain name from someone that lawfully registered the name at an earlier point in time. For example, if a corporation named "Morgan Lewis Bockius" registered the name "mlb.com" for use as a website address for a law firm, and Major League Baseball attempted to sue the law firm for trademark infringement and the use of the name, this would be an example of reverse cybersquatting.

[5] Trade marks act,1999

3. Domain Name Warehousing

This is the practice of "holding" expired domains instead of releasing them back into the public domain. By preventing certain domains from being released, the registrar hopes to resell the domains to the previous registrant or a new registrant at a higher rate than the market price.

4. Grace Period Violations

Known as domain name "kiting" or "tasting," this practice occurs when a registrant registers a domain name for a temporary purpose, but then takes advantage of the domain purchase grace period to reject more permanent ownership.

5. Deceptive similarity

Deceptive similarity[6] generally means one person using any Trade mark which is identical or deceptively similar to the Trade mark which is already in use, whether registered or unregistered, it can also be called as Passing off when one tries to pass off his goods with the Trade mark or name of another and it is an offence punishable under relevant law, but this is in regular format when it comes to cyber space.

6. Innocent squatting

A trademark is not infringed by a domain name unless the trademark existed at the time of domain name registration. This kind of cybersquatting is speculative and legitimate. John D. Mercer also identifies "innocent" cybersquatting,[7] whereby the registrant does infringe a trademark "based on some unrelated interest in the word itself, without intending harm to a trademark owner" and "concurrent" cybersquatting, whereby the registrant uses the same trademark as another commercial entity, but not within a competing industry.

7. Intentional squatting

The harmful kind of cybersquatting involves intentional bad faith trafficking in domain names that are the same as, or a dilution of, existing trademarks. Mercer offers a fitting definition: "an illegal cyber squatter should be one who acquires a domain name for the sole purpose of

[6] Trademarks act, 1999
[7] John D. Mercer, "Cybersquatting: Blackmail on the Information Superhighway" (2000) 6 Boston University Journal of Science and Technology Law, 11.

obtaining money or other advantage from the trademark owner, with no intent or desire to use the domain name, except as an instrument toward this purpose".

8. Creating Likelihood of Confusion

The main function of a trademark is to prevent consumer confusion. For example, a consumer knows that he or she can get the same quality food in a McDonald's in Chennai as he or she can from a McDonald's in Bangalore. The law of trademarks is designed to prevent competitors from confusing customers into thinking that they are buying products and services from a trusted, known source when in reality, this is not the case. A competitor who uses a trademark that is confusingly similar to an existing trademark can be prevented from doing so by the application of trademark law. This usually occurs when the holder of the trademark raises a claim or sues the alleged infringer.

In order to prove trademark infringement, the owner of the trademark must show that there is a "likelihood of confusion"[8] between his or her trademark and the allegedly infringing mark. Over many years and many cases, the courts have set forth a list of eight to 13 elements that are relevant to this determination. The most important element of the likelihood of confusion analysis is;

i) Comparison of the appearance

ii) Pronunciation,

ii) Meaning

iv) Commercial impression

Of the respective marks. If the marks are the same in spelling and how they are pronounced, there is a greater chance of likelihood of confusion between the marks. It is important to note that slight misspellings or changes in an established mark will not enable a competitor to use his proposed mark.

For example, a beverage manufacturer could not adopt the mark "Koka Kola," because although this mark is spelled differently from the famous Coca-Cola mark, it is still pronounced

[8] http://www.tms.org/pubs/journals/JOM/matters/matters-0212.html

the same.

Factors for Likelihood Confusion:

1. the similarity in the overall impression created by the two marks (including the marks' look, phonetic similarities, and underlying meanings);
2. the similarities of the goods and services involved (including an examination of the marketing channels for the goods);
3. the strength of the plaintiff's mark;
4. any evidence of actual confusion by consumers;
5. the intent of the defendant in adopting its mark;
6. the physical proximity of the goods in the retail marketplace;
7. the degree of care likely to be exercised by the consumer; and
8. the likelihood of expansion of the product lines

These are the various types of cyber squatting. What emerges from these factors is that the Internet domain names are of importance and can be a valuable corporate asset. A domain name is more than an Internet address and is entitled to the equal protection as trade mark. A best example which could be coated is the series of Microsoft cases. Microsoft Corporation v. Peppler, Microsoft Corporation v. Kovyrin, Microsoft Corporation v. Cody.[9] All these three cases were related to cybersquatting, which confronted that domain names are the valuable assets of the owner.

Cybersquatting has been a serious issue in the United States over the years. The US has the highest number of cybersquatting suits so far and every year the numbers are rising. Only time will tell as to when this monster on the internet would be rout out completely. With the advancement and progress in the technology, the services rendered in the Internet site have also come to be recognised and accepted and are being given protection so as to protect such provider of service from passing off the services rendered by others as his services. In yahoo Inc. (supra) it was observed that in a matter where services rendered through the domain name

[9] http://go.microsoft.com/fwlink/?linkid=140813

in the Internet, a very alert vigil is necessary and a strict view is to be taken for its easy access and reach by anyone from any corner of the globe.

LEGAL SCENARIO

As stated in the above headings the Cybersquatting cannot be brought within a purview of a single Law. It can be brought under Trademark infringement in some cases, Deceptive similarity in some cases, passing off in some cases, but regarding my concern the Deceptive similarity and passing off, suits it more even it is a Trademark infringement, though there are no proper provisions to punish Cyber squatters across world, but developed countries like U.S, Canada, U.K are having provisions in their respective laws for this. The important organisations which works on protecting the domain owners against the cyber squatters are:1**.**

WIPO[10]

World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre has developed an online Internet based system for administering commercial disputes involving intellectual property.

2**. ICANN [11]**

The Internet Corporation for Assigned Names and Numbers (ICANN) is the official body charged with monitoring the allocation of domain names. In December 1999 ICANN unveiled a standard procedure for settling name disputes, the Uniform Domain Name Dispute Resolution Policy (UDRP).

To reach another person on the Internet you have to type an address into your computer a name or a number. That address must be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination, we wouldn't have one global Internet.

In more technical terms, the Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These

[10] World intellectual property organizations
[11] Internet Cooperation for Assigned Names and Numbers

services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.[12]

ICANN's procedure determines the plausibility of the cyber-squatting claims using three tests;

> First, it verifies that the domain name is identical or confusingly similar to the trademark.
>
> Second, it determines whether the domain name owner maintains a legitimate interest in the name.
>
> Finally, ICANN judges whether or not the domain owner acted in bad faith.[13]

3. **UDRP[14]**

Is the Proven Way of Dispute Resolution**.** The complainant shall assert that the;

(i) contested domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;

(ii) The registrant (the respondent) has no rights or legitimate interests in respect of the Domain name;

(iii) The domain name has been registered and is being used in bad faith by the Respondent.

There are four organizations that are entitled to provide dispute resolution under UDRP:

1. The Asian Domain Name Dispute Resolution Centre (ADNDRC),
2. The International Institute for Conflict Prevention and Resolution (CPR),
3. The National Arbitration Forum (NAF) and
4. The World Intellectual Property Organization (WIPO)[15]

[12] http://www.icann.org/en/about
[13] http://ecommerce.hostip.info/pages/287/Cybersquatting.html
[14] Uniform Domain Name Resolution Policy
[15] 11 WASH. U. J.L. & POL'Y 267, 282
(2003).

The benefits of UDRP are quick resolution since the dispute providers usually decide on the merits within 45-50 days. Furthermore, the cost of the UDRP is considered low.

LEGAL RESOLUTION IN DIFFERENT COUNTRIES

Some countries have specific laws against cybersquatting beyond the normal rules of trademark law.

POSITION IN UNITED STATES:

The United States, has the U.S. Anti-cybersquatting Consumer Protection Act[16] (ACPA) of 1999. This expansion of the Lanham (Trademark) Act (15 U.S.C.) is intended to provide protection against cybersquatting for individuals as well as owners of distinctive trademarked names.

A victim of cybersquatting in the United States has two options:

A. To sue under the provisions of the Anti-cybersquatting Consumer Protection Act (ACPA).

B. To use an international arbitration system created by the Internet Corporation of Assigned Names and Numbers (ICANN).

In court system, jurisdiction is often a problem, as different courts have ruled that the proper location for a trial is that of the plaintiff, the defendant, or the location of the server through which the name is registered.

Recognizing the problems raised by clash between domain name system and trademarks, the World Intellectual Property Organization (WIPO) Arbitration and Mediation Centre has developed an online Internet based system for administering commercial disputes involving intellectual property. This Dispute Resolution Mechanism is unique in that it is designed to be used online both for document exchange and for filling of evidence. However, the original documentary evidence will still be needed to be filled in a physical form. The dispute resolution is simply signed and thus, providing an inexpensive and efficient service and does not in any way seek to take the place of national jurisdiction.

[16] ACPA, 1999

A successful complainant's remedy is limited to requiring the cancellation of the registrant's domain name or the transfer of domain name registration to the complainant.

The procedure will be handled in large part online and is designed to take less than 45 days with a provision for the parties to go to courts to resolve their disputes or contest the outcome of the procedure.

Internationally, the United Nations copyright agency WIPO (World Intellectual Property Organization) has, since 1999, provided an arbitration system wherein a trademark holder can attempt to claim a squatted site.

1. In 2006, there were 1823 complaints filed with WIPO, which was a 25% increase over the 2005 rate.

2. In 2007 it was stated that 84% of claims made since 1999 were decided in the complaining party's favour.

WIPO is the UN's specialized agency for developing a balanced and accessible international system in the field of intellectual property rights

POSITION IN INDIA

In India victims of cyber squatting have several options to combat cyber squatting. These options include: sending cease-and-desist letters to the cyber squatter, bringing an arbitration proceeding under ICANN's rules, or bringing a lawsuit in state or federal court.

A case could be filed with the .in registry handled by National Internet Exchange of India (NiXI) who brings the matter to fast-track dispute resolution process whereby decisions are transferred within 30 days of filling a complaint.

Our legal system is silent on this matter, there is no provision in the current or proposed Information Technology Act in India to punish cyber-squatters, at best, the domain can be taken back. Though there is no legal compensation under the IT Act, .in registry has taken proactive steps to grant compensation to victim companies to deter squatters from further stealing domains. Most squatters however operate under guise of obscure names.

CYBER-SQUATTING CASES

Even though much legislation has not been enacted, almost all cyber squatting court-case decisions are against cyber squatters. These case laws are the some of the best examples of relief for the aggrieved of cyber-squatting.

U.S CASE STUDY:

Intermatic Inc. v. Toeppen,[17]

Defendant Dennis Toeppen registered over 240 domain names incorporating famous trademarks including intermatic.com. Intermatic, a manufacturer of electrical and electronic products sued alleging trademark infringement and dilution. The court granted summary judgment that there was no likelihood of confusion caused by Toeppen's intermatic.com web page. The court granted the motion for summary judgment for Intermatic as to dilution after finding that the Intermatic mark was famous and that Toeppen's intent to arbitrage the name constitutes commercial use. While this appears to be a grant of a per se dilution rule, the court distinguishes cases where there are legitimate competing uses of the same name.

Archdiocese of St.Louis and Papal v. Internet entertainment group[18]

Defendant registered papalvisit.com domain name and used the name to provide limited information on the Pope's upcoming visit. The site was primarily used, however to advertise defendant's adult entertainment site and list off-colour jokes about the church. Plaintiff, owner of the Papal Visit trademark, brought suit alleging trademark infringement, dilution and unfair competition. The court granted a preliminary injunction, finding that plaintiffs were likely to prevail on their dilution claim. The court found that the Papal Visit marks were famous and that their association with adult entertainment sites would likely cause a repair of reputation to the Trademark owner.

Teletech Customer Care Mgmt., Inc. v. Tele-Tech Co.[19]

Defendant Tele-Tech registered and used the domain name teletech.com for its company web site. The court determined that the plaintiff was likely to succeed on the merits of its dilution claim since the TeleTech trademark is probably famous. Relying on the Toeppen cases, the

[17] 947 F. Supp. 1227 (N.D. Ill. 1996).
[18] No. 4:99CV27SNL.
[19] 977 F.Supp. 1407 (C.D. Cal. 1997).

court determined that dilution probably exists if the trademark owner is prevented from using its federally registered mark as its domain name. Although this seems to be a case where the defendant had legitimately registered the name for business purposes and not simply as a cybersquatter, the court indicated that such a distinction is irrelevant in granting preliminary injunction. Because the defendant can use its exact name "tele-tech" (with a hyphen) as a domain name, the case is unlike many other cases where a conflict arises between two companies with similar names. In its likelihood of confusion analysis, the court indicates that the plaintiff will have to show more than "brief confusion" on the part of the Internet browser who accesses defendant's web site to prove likelihood of confusion. Thus the court decided that it was unlikely that TeleTech would succeed on its likelihood of confusion claim. The court granted a preliminary injunction preventing continued use of the domain name.

INDIAN CASE STUDY

Yahoo! Inc. v. Akash Arora [20]

This case is considered to be the landmark case in Indian history of cyber squatting. There are very few reported judgments in our country, newspaper reports and information from reliable sources indicate that there are at least twenty-five disputes pertaining to domain names pending before the Delhi High Court itself. Probably the first reported Indian case in cyber squatting.

The plaintiff, who is the registered owner of the domain name “yahoo.com” succeeded in obtaining an interim order restraining the defendants and agents from dealing in service or goods on the Internet or otherwise under the domain name “yahooindia.com” or any other trademark/ domain name which is deceptively similar to the plaintiff’s trademark “Yahoo .com”. [21] The court ordered interim injunction restraining defendants from using the domain name of the plaintiff.

Tata Sons Ltd vs. Ramadasoft [22]

Tata Sons, the holding company of India’s biggest industrial conglomerate, the Tata Group, won a case to evict a cyber-squatter from 10 contested internet domain names. Tata Sons had

[20] Arb. L. R. 620 (Delhi High Court).
[21] Brain league journal
[22] 2004 (29) PTC 522 Del

filed a complaint at the World Intellectual Property Organisation.

The Respondent was proceeded ex-parte. The Panel concluded that the Respondent owns the domain names .These facts entitle the Complainant to an order transferring the domain names from the Respondent. It was held that these domain names are confusingly similar to the Complainant's trademark TATA, and the Respondent has no rights or legitimate interests in respect of the domain names, and he has registered and used the domain names in bad faith

SBICards.com vs. Domain Active Property Ltd. [23]

Sbicards.com was ordered by the World Intellectual Property Organisation to be transferred to the Indian Company from an Australian entity, which hijacked the domain name hoping to later sell it for a hefty sum to the State Bank of India subsidiary. The court accepted SBI Card counsel's argument that the Australian company was in the business of buying and selling domain name through its website.

Bennett Coleman & Co Ltd vs. Steven S Lalwani [24]

Since 1996, the complainant has held the domain names, www.economictimes.com, using them for the electronic publication of their respective newspapers. The complainant had registered in India this mark for literary purposes. However in1998, Steven S.Lavani, USA registered the same domain name.

The WIPO judgement made it clear that the complainant have a very substantial reputation in their newspaper titles arising from their daily use in hard copy and electronic publication. It was also categorically held that the registration and use of the domain names by the respondents is in bad faith in the sense that their use amounted to an attempt intentionally to attract, for commercial gain, Internet users to their web sites by creating a likelihood of confusion with the complainant's marks as to the source, sponsorships, affiliation or endorsement of those web sites and the services on them.

Rediff Communication Limited vs. Cyber booth & another [25]

The plaintiffs have filed the present suit for a permanent injunction restraining the defendants

[23] WIPO August 23, 2002
[24] http://articles.timesofindia.indiatimes.com/keyword/lavani
[25] 1999 (4) BomCR 278

from using the mark/domain name "RADIFF" or any other similar name so as to pass off or enable others to pass off their business or goods or services as for the business or goods or services of the plaintiffs. The plaintiffs are also seeking a permanent injunction restraining the defendants from using the mark "RADIFF" or any other word on mark either as part of their trade name or trading style which is deceptively similar to plaintiffs' trading style and/or "REDIFF" or using the get up, concept and lay out, etc., so as to pass off the defendants' product and/or services as those of the plaintiffs or in some way connected with the plaintiffs. The plaintiffs are further seeking an injunction against the defendants from using the literary or artistic work found on the plaintiffs' web page or infringing the defendants copyright thereon without the plaintiffs' licence. Along with the suit, the plaintiffs have taken out this Notice of Motion for interlocutory injunctions. The Court held that there is a clear intention of passing off. Hence permanent injunction was granted. Similarly in,

Satyam Info way Ltd. v Sifynet Solutions[26]

The Respondent had registered domain names www.siffynet.com and www.siffynet.net which were similar to the Plaintiff's domain name www.sifynet.com. Satyam (Plaintiff) had an image in the market and had registered the name Sifynet and various other names with ICANN and WIPO. The word Sify was first coined by the plaintiff using elements from its corporate name Satyam Info way and had a very wide reputation and goodwill in the market. The Supreme Court held that "domain names are business identifiers, serving to identify and distinguish the business itself or its goods and services and to specify its corresponding online location." The court also observed that domain name has all the characteristics of a trademark and an action of Passing off can be found where domain names are involved. The decision was in favour of the plaintiff.

Thus, from the above judgements, action against Passing off is when the defendant is restrained from using the name of the complainant to pass off the goods or services to the public as that of the complainant. It is an action to preserve the goodwill of the complainant and also to safeguard the public. In India cybersquatting cases are decided through the principle of Passing off. India does not have a law for prohibition of cybersquatting. Therefore, courts interpret the principle of Passing off with regard to domain names. The court looks into certain criteria while dealing with the cybersquatting cases and the relevant case laws. Not only these Other Global

[26] 2004 (6) SCC 145

brands like Monster Jobs, PepsiCo, Sony Ericsson, Siemens, McAfee, Kingston and search giant Google have of late been at the receiving end of the squatters.

Apart from global brands, celebrity's domains are also targeted by the squatters like Amitabh Bachhan, Sonia Gandhi, Sushmita Sen and Gul Panag. [27] In order to put an end to the continued acts of the domain squatters there is a urgent need for the strict laws in this field, so that these squatters could be punished and these crimes could be avoided in future. The new domain name dispute law should be intended to give trademark and service mark owner's legal remedies against defendants who obtain domain names "in bad faith" that are identical or confusingly similar to a trademark. And the plaintiff may elect statutory damages and has discretion to award in damages for bad faith registration. It should act as an important weapon for trademark holders in protecting their intellectual property in the online world.

CONCLUSION AND SUGGESTIONS

Many business owners fail to realize that cybersquatting is a civil matter and not a criminal matter. You can protect yourself and your good name. But safeguarding your presence on the Internet requires ongoing vigilance. Here are some steps to take toward ensuring that your domain is not easily undermined or stolen by unscrupulous characters:

1. Have a registered trade mark

That is the first protective strategy which is to register your trademark with the Patent and Trademark Office Name. There are two ways you can have a trademark it can be registered or unregistered. Having it listed in the government registry is the right way to go. There are hundreds of millions of domain names that are being registered and renewed every year. The number of legitimate trademark claims that comes out of those registrations is a tiny percentage.

2. Record the proper domain ownership:

The domain information that is registered is the ownership information. So, if a person is properly registered it might make easier for him to administrate it. But, failing of which makes it harder for him to claim ownership, because it is technically under the name and control of

[27] http://www.mightylaws.in/201/cyber-squatting-legal-position

someone else

3. Buy up variations of your domain name:

The easiest and cheapest way to protect your company is to register common variations of your domain before someone else does so and before any damage is done. The only reason a third-party would go out and register those domain names was if they thought that there was valuable traffic out there," he says. "That means if a mistype of your name is valuable to someone else you need to get it first".[28]

If your domain is made of more than one word, consider registering it with hyphens; for example, race-horsing.com and racehorsing.com. Consider also registering the singular and plural versions of your domain, for example, product.com and products.com.Typo squatting is a form of cybersquatting; so, be sure to register any known common mistypes or misspellings of your domain name; for example, lawcounsel.com and lawcouncil.com.

4. Get More Than One extension:

In addition to registering common mistypes, consider registering all of the common versions of your domain, such as .com, .net, and .biz. You might also consider registering .org and .info. If you are doing business outside of the country you will definitely want country extensions, such as .uk. But don't get too distracted by all of these extensions. If you are not a nonprofits organization you shouldn't get an .org, for instance.

5. Head of the haters:

A common practice is to take a domain or company name and add "sucks" to it, such as Nikesucks.com. Angry former employees, dissatisfied customers, or anyone with a personal grudge may use a "sucks" site to bad mouth your company and your products or services. Legal cases have stated that this is not trademark infringement. It is considered free speech. Consider buying your company name sucks.com site. You don't have to use it, better just keep someone else from having it.

6. Fight back through arbitration:

[28] http://dl.acm.org/citation.cfm?id=2339599

Arbitration is available if cybersquatter go too far and infringe on your trademark or libel your company. In order to stop a cybersquatter, you must prove the domain name registrant had bad-faith intent to profit from your distinctive name or trademark and that the domain name is identical or confusingly similar to your name or trademark.

Arbitration is very cost-effective. Also, arbitrations take only six months to 1 year to resolve to get the domain name transferred back, whereas with a lawsuit the court may get an injunction within six weeks to stop the other party from using the domain name.

7. Think like a consumer:

Consumer is the most important base for the traders online. Thus, it is the responsibility of every owner to think like a consumer and give them a cyber free environment and make all measure to protect them.

Thus, With advancement in Technologies and transparency in the Global digital market, cybersquatting has gradually been put on check. But still small enterprises and start-ups are suffering from squatters who abuse names and brands in the digital world, thereby tarnishing the reputations and goodwill of genuine owners and also cheating the digi-consumers by passing of duplicate goods, services, etc., The introduction of a strong Digital Global platform for all traders to interact and interface in an authenticated manner would be the solution to curb cybersquatting.