

ADDRESSING THE CONCERNS OF VICTIMS OF TYPOSQUATTING

| Authored By : Sneha Singh & Shruti Shikha |

People in general are well aware of how cybercrime is perpetrated, the profits of the attackers, but the harms suffered by such victims is less known. Still less, are we aware of trifling cybercrimes like typosquatting. This paper presents a comprehensive study of the losses suffered by the internet users, that is the consumers, which has been less dealt by both the state and public, across the globe. While there are provisions regarding providing remedies to the site owners, people in general affected through typosquatting goes unaddressed. Ignorance regarding this is very widespread in public who become easy targets of such crime and due to veniality of the crime states hardly bother. While the efficiency of cyberattackers is increasing at a constant pace, legislations lag hugely behind particularly in India.

I. INTRODUCTION

Internet is growing as one of the most important aspects of individual's life, today. It serves the needs of communication, data processing, controlling machines, typing, editing, sale and purchase; almost all aspects of life. The growth of cyberspace has set into motion a totally different set of crimes whose causes and consequences is yet to be understood. It is no secret that legislators, jurists, and organizations – despite many years of effort – continue to search for solutions to the complex legal issues spawned by the World Wide Web, a technological forum that allows billions of people to communicate almost instantaneously.¹

It is required, that we understand the technicalities behind the issue discussed in the paper; each website on the internet has an ip address behind its name. Each web server requires a domain name system to convert the domain name to ip address which is a string of particular numbers.² A domain name is unique to a website. It is an identification to that website. Creating websites with unique domain names is a common practice nowadays, through which the companies are easily identified by their trademarks. A single company has large number of consumers which is not possible on part of either the company or the consumer to connect with each other physically. Domain names provide the company with such a base where they are easily able to connect with their consumers, both the parties being citizens of cyberspace. The holder of domain names make money through pay-per-click advertising on a website. Every time any user clicks on the advertisements popping or presented on the website, money rolls in for the domain holder.

The very first domain name, symbolics.com was registered almost 31 years ago, in March 1985. With modernisation in World Wide Web, domain names registration exploded. Today, there are millions of domain names functioning. Domain names enable the companies to connect with their consumers. However, unlike trademarks, domain names are mostly registered on first come- first served basis. This approach has enabled tech-savvy outlaws to

¹ Carl C. Butzer And Jason P. Reinsch ,Cybersquatting, Typosquatting, And Domaining: Ten Years Under The Anti-Cybersquatting Consumer Protection Act .

²<http://www.ijser.org/researchpaper%5CCybersquatting-and-its-Effectual-Position-in-India.pdf>(Aug.25,2016,10:00PM).

profit from others' marks and goodwill through "cybersquatting" i.e., the "registration as domain names of well-known trademarks by non-trademark holders who then try to sell the names back to the trademark owners."³

II. WHAT IS TYPOSQUATTING?

Typosquatting is a type of cybersquatting. While, definitions to cybersquatting has been provided under various legislations and judgments, typosquatting is yet to be provided with a legal definition. Still, some authors have attempted to define typosquatting as follows:

Typosquatting is the registration of internet domain names which are similar to those of established sites, in the hopes that the user typing the site's name makes a mistake and visits the typo domain rather than their intended target.⁴

Typosquatters are aware of the fact that the user intended to visit another site, instead of theirs which is a misspelled version of the intended site presents the users with many ads, or sometimes, even malware to its visitors. Typosquatting has not been shown as particularly harmful from a malware infection standpoint, as the number of typo sites visited still remains lower than that of legitimate ones.⁵ Even though the harm caused by typosquatting is modest in nature, it forces the users to invest in defensive registration.

Though typosquatting is not a major cybercrime, we can still pinpoint certain properties of it:

It can be observed at the network level itself;

Typosquatting sites serve no other purpose than targetting unsuspecting consumers of the similarly spelled site;

Typosquatters rely on the fact that internet users will make typographical errors while entering domain names into their web browsers. Some common examples of typosquatting include⁶:

The omission of the "dot" in the domain name: wwwexample.com;

A common misspelling of the intended site: exmple.com

A differently phrased domain name: examples.com

A different top-level domain: example.org

³Spoty's Farm L.L.C. v. Sportsman's Market, H.R. Rep. No. 106-412, at 5-7 (1999).

⁴Mohammed Taha Khan, Xiang Huo, Zhou Li & Chris Kanich, Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting.

⁵ J. Szurdi, B. Kocso, G. Cseh, M. Felegyhazi, and C. Kanich, "The Long "Taile" of Typosquatting Domain Names," in Proceedings of the 23rd USENIX Security Symposium, 2014.

⁶ Sanchit Mehta, *Cyber Squatting And Its Legal Positions*, Manupatrafast.Com(AUG.30,2016,10.00AM), www.manupatrafast.com/articles/PopOpenArticle.

III. CONCERNS OF VICTIMS OF TYPOSQUATTING

The confusion caused by such misspelling of website names, not only causes loss of potential visitors to the website owners but frustrates the consumers as well who incur not only monetary loss but loss of effort and time on their part altogether. Every time a consumer visits a typo site, it signifies the amount of time, money and effort wasted on part of him. While, these are the direct losses suffered by the consumers by typosquatting, he suffers indirect losses as well, which have been discussed below:

Monetary loss: this is the most common and well known loss suffered by any citizen of cyberspace, due to any form of cybercrime. Cybercrimes are growing day to day and the primary objective of all such forms of cybercrime offenders is financial gain in the process, whether it be finances gained by stealing of credit cards, or by accidental visitors clicking on the ads provided on the sites. In the case of typosquatting, where internet users unintentionally visit lexically similar sites, which are armed with various malwares and adwares, instances of financial to users are pretty common.

Loss of effort: while we are generally aware of the loss of money on part of users, frustration of time and effort of visitors by their coming across such typosquatted sites is usually neither known nor talked about. Typosquatted sites are often full of adwares and malwares. A user may lose his credit card, but this is just an immediate damage. The user as a consequence has to go for issue of new card, block the old one; not to mention he will have to update his security, remove all the flaws from the system which the malware must have caused. The loss of money is nonetheless substantial, but one cannot ignore the effort wasted, which could have been deviated to more productive works rather than dealing with the harm caused by visiting such unintended lexically similar site.

Loss of time: negative externalities involving cybercrime have hardly been dealt with. Not to mention, that our country is far than lacking in it. Time lost for visitors and visitors lost for the site operators still remains untouched. Time that a user has to spend subsequent to an attack from some malware installed in the typosquatting site. Renewal of card, cleanup of the system after attack. Even if the malware fails to register any harm in the system, the consumer has to eventually go for updating of security to prevent any such harms that may be caused due to unchecked malware in future.

Apart from, direct harm to the users, indirect harms that have seldom been accounted with, should also be taken into consideration. The fact that cybercrimes like typosquatting psychologically affects the users cannot be denied. As of the latest statistical studies and reports, there might be a risk of lowering of online transactions, and usage of other such internet facilities due to lack of faith in security guarding cyberspace.⁷

IV.LEGISLATIONS: INDIA VIS- A- VIS WORLD SCENARIO

Some countries have special laws against cyber squatting beyond the normal rules of trademark law but India does not have special legislation on Domain Name Protection Law and cyber squatting cases are decided under Trade Mark Act, 1999 ⁸.

⁷ Ross Anderson, Chris Barton , Rainer B" Ohme , Richard Clayton , Michel J.G. Van Eeten , Michael Levi , Tyler Moore & Stefan Savage, *Measuring The Cost Of Cybercrime* .

⁸ Trademark Act,1999.

Position in U.S.A.

The United States has the U.S. Anti-cyber-squatting Consumer Protection Act (ACPA) of 1999⁹. This provides protection against cybersquatting for individuals as well as owners of distinctive trademarked names. A victim in United States has two options:

Sue under the provisions of the Anti-cyber-squatting Consumer Protection Act (ACPA), or

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

However, due to jurisdictional problem arising in the court WIPO (world intellectual property organization) Arbitration and Mediation center has come up with an online Internet based system for administering commercial disputes involving intellectual property. It provides solution within 45 days¹⁰.

Position in India

In India a cybersquatting victim has three options¹¹

(I).Court Of Law: Victim can file a suit in court of law under Trademark Act,1999 for various injunctions restraining cyber squatter from misusing domain. Like in other cases under Trademarks Act, 1999 two kind of reliefs are available:

1. Remedy of infringement
2. Remedy of passing off

Remedy of Infringement: Trade mark Act permits owner of the trade mark to avail the remedy of infringement only when the trade mark is registered.

Remedy of Passing off: No registration of the trade mark is required in case the owner intends to avail the relief under passing off.

In the case of Rediff¹², the Bombay High Court granted an injunction restraining the defendant from using the domain name “RADIFF” or any other similar name, as it was held that when both domain names are considered, there is every possibility of internet users being confused and deceived into believing that both domain names belong to one common source and connection.

(II).Uniform Domain Name Dispute Resolution Policy (UDRP): Dispute involving bad faith registrations are typically resolved using the Uniform Domain Name Dispute Resolution Policy (UDRP) process developed by the ICANN. Under UDRP, WIPO is the leading ICANN accredited domain name dispute resolution service provider and was established as a vehicle for promoting the protection, dissemination, and the use of intellectual property throughout the world. India is one of the 171 states of the world which are members of WIPO.

⁹Anti Cyber Squatting Consumer Protection Act,1999.

¹⁰ Anti-cyber squatting Consumer Protection Act (ACPA) , 1999.

¹¹ Singh & Associates,India: Cyber Squatting Laws In India, (Aug.20,2016,10:05),mondaq, www.mondaq.com/india/x/208840/.../CYBER+SQUATTI+NG+LAWS+IN+INDIA.

¹² 1999 (4) BomCR278.

A person may complain before the administration dispute resolution service providers listed by ICANN under Rule 4 (a) that:

- (i) A domain name is "identical or confusingly similar to a trade mark or service mark" in which the complainant has rights; and
- (ii) The domain name owner/registrant has no right or legitimate interest in respect of the domain name; and
- (iii) A domain name has been registered and is being used in bad faith.

(III). IN Dispute Resolution Policy (INDRP): The .in top level domain is operated under the authority of National Internet Exchange of India or NIXI. Hence, domain name or cybersquatting disputes pertaining to .in domains are handled by the .IN Dispute Resolution Policy and the INDRP Rules of Procedure. It provides resolution of the dispute within 30 days. As like URDP three ingredients provided under rule 4(a) of ICANN needs to be fulfilled for proving the crime.

The only difference between the legislation in India and U.S.A. is that there is a specific legislation for cybersquatters in U.S.A while in India it is dealt under The Trademark Act, 1999. But, no where users are protected by the law.

V. SOME IMPORTANT JUDGMENTS RELATING TO TYPOSQUATTING IN INDIA

Yahoo! Inc. V. Akash Arora and Another's¹³

In this case respondent had registered the domain "yahooindia" which is very much similar to the complainant domain name "yahoo". The Court observed that usually the degree of the similarity of the marks is vitally important and significant in an action for passing off for in such a case there is every possibility and likelihood of confusion and deception being caused. When both the domain names are considered, it is crystal clear that the two names being almost identical or similar in nature, there is every possibility of an Internet user being confused and deceived in believing that both the domain names belong to one common source and connection, although the two belongs to two different concerns.

Tata Sons Limited and Anr Vs fashion ID Limited¹⁴

The Hon'ble High Court of Delhi Court held that "The use of the same or similar domain name may lead to a diversion of users which could result from such user's mistakenly accessing one domain name instead of another. This may occur in e-commerce with its rapid progress and instant (and the erotically limitless) accessibility to users and potential customers and particularly so in areas of specific overlap. Ordinary consumers/users seeking to locate the functions available under one domain name may be confused if they accidentally arrived at a different but similar web site which offers no such services. Such users could well conclude that the first domain name owner had miss-represented its goods or services through its promotional activities and the first domain owner would thereby lose their customer. It is apparent therefore that a domain name may have all the characteristics of a trademark and could found an action for passing off".

¹³ 1999 II AD (Delhi)229.

¹⁴ 117 (2005) DLT 748.

Dr Reddy's Laboratories Limited Vs Manu Kosuri and Anr¹⁵

Respondent domain name 'DR. REDDY'S' and complainant domain name 'drreddyslab.com' were very similar and confusing in this case. The court observed that the domain name serve same function as the trademark and is not a mere address or like finding number of the Internet and, Therefore, plaintiff is entitled to equal protection as trade mark. The domain name is more than a mere Internet address for it also identifies the Internet site to those who reach it. In an Internet service, a particular Internet site could be reached by anyone anywhere in the world who proposes to visit the said Internet site .The court held that, it is clear that two names being almost identical or similar in nature, there is every possibility of an Internet user being confused and deceived in believing that both the domain names belong to plaintiff although the two domain names belong to two different concerns.

Aqua Minerals Limited Vs Mr Pramod Borse & Anr¹⁶

He Hon'ble High Court of Dehi Court has held that Unless and until a person has a credible Explanation as to why did he choose a particular name for registration as a domain name or for that purpose as a trade name which was already in long and prior existence and had established its goodwill and reputation there is no other inference to be drawn than that the said person wanted to trade in the name of the trade name he had picked up for registration or as a domain name because of its being an established name with widespread reputation and goodwill achieved at huge cost and expenses involved in the advertisement.

Nestle India Limited Vs Mood Hospitality Pvt. Limited¹⁷

The Hon'ble High Court of Delhi Court has held that in case of interim relief/injunction test of prima facie case as traditionally understood has been replaced, at least in trade mark matters, by the test of comparative strengths of the rival cases.

VI.CONCLUSION AND SUGGESTIONS

This paper's ultimate goal is assessing and categorizing the loss suffered by the users due to typosquatting. Being a venial offence in the arena of cybercrime, typosquatting largely goes unnoticed. The paper has sought to present, the lack of awareness among people with regard to this offence, as well as lack of effort on part of governments of states to address the issue. As has been said by edmund burke, "we must all obey the law of change"; change is constant in nature. Law is the reflection of society, so must it adjust to the changes that arise in it. As the citizens of cyberspace are growing, so is the number of cybercrimes. While, internet has brought people closer, it has also brought into scenario multiple offences that majority of people are affected with, but are unaware of its causes, consequences and of course remedies. Government and other authorities have yet take notice of these offences, and step forward to make legislations in this regard.

As shown in this paper there are some legislations in few countries regarding typosquatting, but yet in others it has been just passed off as a venial offence, and largely goes unnoticed. It cannot be ignored that the whole arena of internet has grown at a very explosive speed, and the crimes involved are so diverse, that a lot of them still need recognition. Yet, there are some

¹⁵ 2001 (58) DRJ241.

¹⁶ AIR2001Delhi 467.

¹⁷ 2010(42)PTC514 (Del).

globally recognised rules for all such offences including typosquatting which lacks recognition all around mostly. The highest rate of cybercrimes have been reported in U.S.A, and it also has the most legislations addressing them. Not to mention, India is hugely lagging behind.

There is no separate existing law in India to deal with the offence of typosquatting, It is dealt by Trademark Act,1999. Also, remedy is only available to the legitimate domain owner whose rights get violated due the offender who creates a confusingly similar domain as that of legitimate owner. But the tragedy is that users whose many rights get violated due to the fraudulent act of the offender do not have any remedy in existing legal system. Users suffering from monetary loss, effort loss and time loss are ultimately left with nothing but a psychological pain as there is no remedy in court of law for readdressed of their grievances. In other developed countries like U.S.A, legal system provides remedy only to the legitimate domain owner under Anti cybersquatting Consumer Protection Act, 1999. Also, ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) allows a trademark owner to challenge domain name registrations in expedited administrative proceedings. UNDR is a uniform solution available to all the website owner worldwide against cybersquatting.

Suggestions

The arena of cyberspace is widely unexplored and unguarded. The exponential increase in cybercrimes largely goes unregistered. Governments, non-governmental organisations and people, all should take collective effort to see to the spreading of awareness of these cybercrimes that are largely plaguing the societies at this date.

Cybercrimes whether major or minor, cause a huge amount of direct and indirect harm to people and state. It is regrettable that not only these offences goes unnoticed due to lack of proper legislation, the consequences per se of such offences have also not been accounted till date.

The rate with which cyber-attackers are increasing their efficiency is much beyond which people and state are able to match with. The causes, consequences and remedies are unknown, this is why there is no proper legislation guarding these offences. We can only say so less about major cybercrimes like hacking, frauding much less is to be expected of venial offences like typosquatting that causes relatively modest level of harm.

Typosquatting is majorly concerned with using the goodwill of the consumers of a trademark company to its own advantage. While, there are still enough laws to guard the intellectual property rights of companies, no steps have as far been taken to assess and remedy the harm done to users who become victims of such. As stated in the paper, a user suffers many indirect and direct losses, whereby he may lose trust in internet services; authorities have yet to look upon their issues, and remedy it through legislations. Efforts must be taken to take into account and understand various cybercrimes that are sprouting day to day, and spread awareness about the same. Awareness will set into motion the process of legislation.

Full understanding can only bring effective legislations into force and victims will be remedied; otherwise, cyberattckers which include the typosquatters will go on making illegal profits at the cost of innocent visitors, and this crime as well as other such cybercrimes will go unwarranted, increasing as they are.