International Journal of Law and Social Sciences (IJLS)
Volume 6, Issue 1, 2020 | P-ISSN No: 2454-8553

DOMAIN NAME DISPUTES AND THE RISING THREAT OF CYBERSQUATTERS

Jalaj Agarwal[1]

Gracy Bindra[2]

INTRODUCTION

In recent decades, the world has been taken over by the internet, giving rise to digital age menaces. The Internet is now being used for commercial purposes in recent years; this has led to the transformation in the businesses. With the changing trends of marketing and a paradigm shift of physical marketplace to e-commerce, many companies have been successful in their business and commerce positioning services online.[3]

As cyberspace takes over the businesses, the importance of domain names and trademark law increases. A domain name refers to a computer address by which a company or an individual can be located by any other internet users.[4] The main aim to pose domain names is to distinguish and locate the different computers, users, files, and resources accessible over the Internet.[5] In usual practice, the companies are inclined to choose domain names which are easy to memorize, everyday words and well- known trademarks by their consumers. The problem arises when two or more people claim the same name, which is forbidden under trademark law. Trademark law has often been referred to as it restricts the use of already registered trademarks because it tends to confuse a potential customer about the profile and true seller of the product or service involved. The same has been invoked to resolve disputes between computer users that obtain Internet domain names and the owners of the registered trademarks.[6] There are various negative consequences of the transition to cyberspace in the form of trademark issues such as cyber-squatting, typo- squatting, mega tagging, renewal snatching etc.

---

[1] BA LLB (Hons.) 5th Year, Symbiosis Law School, Pune
[2] BA LLB (Hons.) 5th Year, Symbiosis Law School, Pune
[3] Michael D. Scott, *Advertising in Cyberspace: Business and Legal Considerations,* COMPUTER LAW., 1 (1995).
[4] Sally M. Abel, *Trademark Issues in Cyberspace: The Brave New Frontier*, MICH. TELECOMM. & TECH. L. REV., (1999).
[5] Bonifaz, Monica. *Domain names, Internet and Trademarks, infringements in cyberspace*, PAPER REVIEW, (2015).
[6] Froomkin, A., *The collision of trademarks, domain names, and due process in cyberspace*, COMMUN. ACM. , (2001).

DOMAIN NAME SYSTEM AND TRADEMARK

Every web page has a unique address which not only represents the branding of the company but also distinguishes it from the other companies in the market. The domain names aid internet users to remember, locate and access the sites instead of writing the long IP address in binary computer language.

A domain name refers to a unique name which recognizes the website[7] and contains three parts to it. The first part known as third level domain which contains- "www". which represents that the website is connected to the world wide web and discoverable on the internet search engines. The second part is the most essential part which includes the unique name of the company, for eg. - "Facebook", and better known as second level domain name. The last part is known as top level domain name and could be of various types -generic code, country code, special top- level domain names or restricted use domain names. If it is a country code, such as- ".in" for India or ".jp" for Japan; it represents a particular country. In case, a company chooses generic codes, such as- ".com", ".org", ".edu"; it represents deployment to no particular class of organization and is regulated by the Internet Corporation for Assigned Names and Numbers popularly known as ICANN. Some of the special top-level domain names are- ". legal", ". app" etc. Restricted top- level domain names are not allowed to be used by everyone as the name suggests, such as ". arpa", ".biz" etc.

The process of allotment of such domain names differs on case to case basis. It could either be a first come first serve basis or if a company with legitimate business claims a domain name of that company name, would be given preference over others.

In this changing world of e-commerce, the domain name systems have a great significance and disputes arising out of it have no bounds. This calls for a need for a specific regulating authority. Since recognising the source of product is an important role played by the domain name, there is a need to treat them as equivalently important to trademark as far as the legal protection and recognition is concerned, as this could lead to trademark infringement.[8]

---

[7] Pope, Michael & Warkentin, Merrill & Mutchler, Leigh & Luo, Robert, *The Domain Name System: Past, Present, and Future*, COMMUNICATIONS OF THE ASSOCIATION FOR INFORMATION SYSTEMS, (2012).

[8]Richard L. Baum and Robert C. Combow, *First Use Test in Internet Domain Name Disputes*, NATL. LJ 30, (1996).

Trademarks not only give unique identification to the product but have also become a way of digital branding for various companies. Businesses use fancy, unique and distinct domain names by often combining two languages, different font and color schemes in order to attract more users to their websites, thus it is an important tool for communication in business transactions.

In the real world, two people belonging from different countries can have one trademark for goods and services unlike the domain name which belongs to only one person in the virtual world and need not be for one good/service but could be for the whole company dealing in a range of different goods and services.

UNDERSTANDING CYBERSQUATTING

Domain name abuse and misuse in the form of cyber-squatting has increased in great numbers with the growth in commercial activities and use of cyberspace. In the 1990s, the internet had become a growing sensation and grew the menace of cyber-squatting, also known as brand-jacking.[9] The Delhi High Court interpreted the term Cyber-squatting as "an act of obtaining fraudulent registration of a domain name with the intent to sell it to the lawful owner of the name at a premium."[10]

The ultimate motive of maximum profit maximization drives the menace of cyber-squatting. Another reason for indulging in cyber-squatting could be to defame and bring bad name to the company by using fake identities. Registration of a domain name is a cheap and economical process; however, once a domain name is registered, it allows the party to earn profit through various means such as by publishing advertisements on the web page or by pay-per-click advertisements.[11] It can also be used to divert user's traffic from the original trademark holder's business by creating confusion in the minds of the consumers, and thereby causing losses to them.[12] Moreover, such individuals often sell a registered domain name at significantly high prices to the legitimate owner of a trademark whose identity is reflected in

[9] Jonathan Anschell & John J Lucas, *What's in a Name: Dealing with Cybersquatting*, ENT. & SPORTS LAW 3rd edn., (2003).
[10] Manish Vij v Indra Chugh, [2002] AIR Del 243.
[11] Jordan A. Arnot, *Navigating Cybersquatting Enforcement in the Expanding Internet*, J. MARSHALL REV. INTELL. PROP. L., 13th edn., (2014).
[12] Dara B. Gilwit, *The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement*, WASH. U. J. L. & POL'Y 11th edn., (2003).

the domain name by creating a similar one, creating confusion and deception and using unfair trade practices such as blackmailing and harassing the original owners to gain revenue.[13]

There are various types of cyber-squatting like[14]-

1. Typo squatting- This type includes 'URL hijacking', 'a sting site', and 'a fake URL' wherein typo squatters take advantage of the mistakes internet users make while searching the browser and typing web addresses. Due to the similarities in the visuals, fonts and hardware, the users are often confused. Typo squatters might go to the extent of creating fake websites using similar logos and colors to divert and confuse the traffic and create malware.

2. Identity Theft – In case an owner forgets or fails to renew their domain, the cyber squatter takes undue advantage of the situation by misleading the internet users by posing to be the legitimate owners. They do so by monitoring and targeting such domain names and purchase them as soon as renewal gets delayed or fails.

3. Name Jacking- Cyber squatters use celebrities or famous personalities posing to be related to them and illicitly attracting traffic to their website.

4. Reverse Cyber-squatting- Reverse cyber-squatting refers to a scenario wherein the cyber squatters attempt to secure legitimate domain names to indicate authenticity and create confusion and undue benefits.

There is a need to curtail such practices and therefore countermeasures have been devised by various organizations', which will be discussed in the next segment of the paper.

COUNTERMEASURES TO CYBERSQUATTING

In order to prevent the growing threat of Cyber-squatting it is important to have proper regulation, policies and authorities to counter and seize any such malicious acts. Globally, Internet Corporation for Assigned Names and Numbers (ICANN) is the organization that administers the domain name system. It was established in 1998[15] as an American not for

[13] RASTOGI ANIRUDH, CYBER LAW, LAW OF INFORMATION TECHNOLOGY AND INTERNET (Lexis Nexis 2014).
[14] Sankalp Jain, *Cyber Squatting: Concept, Types and Legal Regimes in India & USA*, SSRN ELECTRONIC JOURNAL, (2015).
[15] THE HISTORY OF ICANN,

profit private organization which undertakes the task of overseeing and supervising the distribution of IP addresses and domain names thereby managing and coordinating the domain name system. However, it is pertinent to note that the actual domain name registration is done by particular domain name registries located in different countries across the globe.

In order to resolve and facilitate the disputes arising in relation to domain names, the Uniform Domain Name Dispute Resolution Policy (UDRP) was established in the year 1999 by the ICANN.[16] Since its establishment UDRP has been successfully implemented in resolving a large number of domain name disputes over the years.[17] Currently there are six approved dispute resolution providers to which complaints can be filed as per procedure laid down under the UDRP; they are: World Intellectual Property Organization (WIPO), Asian Domain Name Dispute Resolution Centre (ADNCRC), National Arbitration Forum (NAF), Canadian International Internet Dispute Resolution Centre (CIIDRC), Arab Center for Dispute Resolution (ACDR) and Czech Arbitration Court (CAC).[18] Among them WIPO has been the most popular domain name dispute resolution platform.

Paragraph 4(a) of the UDRP provides the necessary elements when a trademark holder can apply to any ICANN dispute resolution service provider. According to this, the UDRP is capable of resolving disputes which arise when:[19]

- The domain name is alike or confusingly similar to the trademark to which the complainant has rights.
- The opposite party has no legitimate right or interest in the domain name.
- The opposite party has registered the domain name with mala fide intentions.

---

https://www.icann.org/history#:~:text=ICANN%20was%20founded%20in%201998,the%20U.S.%20with%20global%20participation (last visited on 14 September 2020).

[16] UNIFORM DOMAIN-NAME DISPUTE-RESOLUTION POLICY, https://www.icann.org/resources/pages/help/dndr/udrp-en (last visited on 14 September 2020).

[17] Zohaib Hasan Khan, *Cybersquatting and its Effectual Position in India*, Vol. 6 Issue 2, IJ SCIENTIFIC & ENGINEERING RESEARCH, (2015).

[18] ICANN, LIST OF APPROVED DISPUTE RESOLUTION SERVICE PROVIDERS, https://www.icann.org/resources/pages/providers-6d-2012-02-25-en (last visited on 14 September 2020).

[19] UNIFORM DOMAIN DISPUTE RESOLUTION POLICY, https://www.icann.org/resources/pages/policy-2012-02-25-en (last visited on 14 September 2020).

Furthermore, Paragraph 4(b) enumerates the factors for determining if there's a case of registering or using the domain name in bad faith by the concerned party. Various factors which are taken into consideration for this purpose are:

- The domain name was registered with the main objective of selling it at a higher price afterwards
- The domain name was registered with the primary purpose of causing loss to the business and brand value of the competitor
- The domain name was registered so as to prevent the rightful owner of the trademark from acquiring the domain name for its mark
- The domain name was registered in order to take undue advantage of the brand value of the complainant's trademark and attract users to its website by creating confusion between the two parties.

Once the domain name dispute is resolved, the concerned authorities can either transfer the domain name to the complainant or cancel the domain name altogether. On the other hand, if the complaint is found without merit it can be rejected by the service providers. UDRP does not provide for any remedy in the form of monetary damages or any kind of injunctive relief. In case the losing party is not satisfied with the decision of the authority it can file a lawsuit against the opposite party in a court of competent jurisdiction within 10 days of the said decision.[20]

World Wrestling Federation Entertainment, Inc. v Michael Bosman[21] was the first case decided by WIPO through the UDRP. In this case the respondent had first registered the domain name "worldwrestlingfederation.com" and thereafter offered to sell the domain name to WWF at a higher price. WWF filed a complaint alleging that the domain name was registered with mala fide intention by the respondent and was in violation of WWF's trademark. The WIPO panel ascertained that the domain name was identical or confusingly similar to the WWF's trademark. It further held that the respondent had no bona fide interest or right in the said domain name and ordered the transfer of the registration of the said domain name to the complainant.

[20] THE UNIFORM DOMAIN DISPUTE RESOLUTION POLICY, https://www.icann.org/resources/pages/policy-2012-02-25-en (last visited on 14 September 2020).
[21] World Wrestling Federation Entertainment, Inc. v Michael Bosman, [2000] WIPO, Case no. D99-0001.

Similarly in Philip Morris Incorporated v r9.net[22], the complainant was the owner of the well-known brand and trademark 'Marlboro'. However, the respondents registered the domain name "Marlboro.com" against which a complaint was registered alleging that the said domain name was confusingly similar to the complainant's trademark and was registered in bad faith. The allegations were held to be valid by the WIPO panel and the registered name was transferred to the complainants.

Overall, the UDRP as operated by the approved service providers under ICANN is very efficient and popular in resolving domain name disputes. The UDRP process is much quicker and cheaper than the court litigation, it has an international jurisdiction and the cases are resolved by individuals who are experts in trademark law which is not always possible in normal litigation.

Over the years some countries such as Canada (Canada's Domain Name Dispute Resolution Policy) and the United Kingdom (UK's Domain Dispute Resolution Service) have even adopted their own dispute resolution mechanism being unrelated to the UDRP.[23] Although India has formulated its own dispute resolution policy, INDRP 2005, which is in line with the UDRP and the provisions of the Indian Information Technology Act, 2000 it has not been put to use much on account of it being a mere guiding policy.[24]

SITUATION IN INDIA

Over the years there have been numerous cases of cyber-squatting in India, but with the unprecedented growth in digital media and internet, there has been a surge in such cases in recent years. However, currently, there is no specific legislation in India for resolving domain name disputes such as cyber-squatting. The Indian Trademarks Act, 1999 does not provide for any specific provision protecting domain names in pursuance of trademark infringement. Furthermore, the jurisdiction of the act is not extra-territorial; therefore, it does not provide for adequate protection in case of infringement happening outside the Indian territory. Similarly, the provisions of the Information Technology Act, 2000 are not sufficient to

[22] Philip Morris Incorporated v. r9.net, [2003] WIPO Case no. D2003-0004.
[23] Doug Isenberg, *These Countries have adopted the UDRP*, GIGALAW, (2017) https://giga.law/blog/2017/5/23/these-countries-have-adopted-the-udrp (last visited on 13 September 2020).
[24] Jayakar, Krishna & Patricia, *India's Domain Name Dispute Resolution Process: An Empirical Investigation*, SSRN E-J, (2012).

resolve the domain name disputes in relation to trademark infringement and to curtail the acts of cyber-squatting.

However, the Indian courts have been active in resolving cases relating to cyber-squatting under the laws relating to passing off. Passing off is a common law tort and has been further developed by the Hon'ble courts to be applied in such cases of domain name disputes. This can be inferred from the judgment in *Satyam Info way Ltd. v Sifynet Solutions (P) Ltd.*,[25] wherein the Supreme Court stated that although there is no specific legislation in India with respect to resolving disputes pertaining to domain names and the Trademarks Act, 1999 also do not provide adequate protection as its operation is not extraterritorial, however domain names in India were protected under the laws relating to passing off to the maximum extent possible.

A passing off action inter alia restrains the defendant from using the name or trademark of the complainant so as to cease the respondent from passing off the goods or services to the general public as that of the complainant. It is used to safeguard the goodwill of the complainant and protect the general public from such deceitful activities. The applicability of this principle can be further understood through various landmark cases adjudicated by the Indian courts in this matter:

The first case in India pertaining to Cyber-squatting was *Yahoo! Inc. v Akash Arora & Anr.*[26] in the year 1999. The plaintiff was the owner of the well-known mark "Yahoo!" and also of the domain name "Yahoo.com." The defendants however registered a confusingly similar or identical domain name "YahooIndia.com" that too with similar format and colour scheme and provided similar services like that of the plaintiff. The Delhi High Court applying the law of passing restrained the defendant from using the said domain name. Ruling in favour of the plaintiff the court reasoned that the defendant's domain name was deceptively similar to confuse the general public and more of an effort to take undue advantage of the reputation of Yahoo Inc.

[25] Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd., [2004] (3) AWC 2366 SC
[26] Yahoo! Inc. v. Akash Arora & Anr., [1999] IIAD Delhi 229

Rediff Communication v Cyberbooth & Anr.[27] was another early case relating to cyber-squatting decided by the Bombay High Court. The respondents had registered a domain name "radiff.com" being similar to the plaintiff's domain name "rediff.com". The court decided in favour of the plaintiff as the defendant's domain name could create confusion between the distinctiveness of the two parties. In this case the court further held that domain names are an important and highly valued asset of the company and need to be adequately protected.

Similarly, in the case of *Acqua Minerals Ltd. v Mr. Pramod Borse & Anr.*,[28] the plaintiff was the owner of the trademark "Bisleri" in India. The defendant subsequently registered the domain name "bisleri.com" which was found to be an infringement of the trademark of the plaintiff as it was deceptively similar to the plaintiff's brand. The Court ordered the defendant to transfer the domain name to the plaintiff.

Satyam Infoway Ltd. v Sifynet Solutions[29] was the first case relating to cyber-squatting decided by the Supreme Court. The plaintiff was the registered owner of the word "Sifynet" which was developed using the initials of its corporate name Satyam Infoway and had goodwill and reputation in the public. The respondent had registered domain names "Siffynet.com" and "Siffynet.net" which were deceptively similar with plaintiff's domain name "Sifynet.com". The Apex Court set aside the judgment of the High Court and gave its decision in favour of Satyam Infoway. It stated that the respondent had adopted the said domain name with a dishonest intention as the marks were found to be deceptively similar. The Supreme Court in this case held that domain names were regulated under the Trademarks Act, 1999 as they inculcated all the features of a trademark.

Even though the Indian Courts have been fairly active in dispensing cases relating to cyber-squatting and providing adequate reliefs, it has been observed that with the increasing number of domain name disputes parties have started using alternate dispute resolution mechanisms such as arbitration and mediation for resolving cases relating to cyber-squatting. Parties generally prefer resorting to the UDRP process offered by WIPO and other ICANN approved

[27] Rediff Communication v Cyberbooth & Anr., [2000] AIR Bombay 27
[28] Acqua Minerals Ltd. v Mr. Pramod Borse & Anr., [2001] AIR Delhi 463
[29] Trademark Act, 1999, §103.

service providers rather than formal litigation mechanism offered by the Indian courts for various reasons.

RECENT DEVELOPMENTS

The world has recently been struck by a pandemic and as businesses are facing huge losses, the only sector that has boomed is e-commerce. Every company is shifting to the virtual world and claiming domain names and devising new ways to approach their clientele and attract more consumers. This has however increased cybersquatting disputes by manifold numbers.

In recent times, in countries like China, various cyber-squatting suits have been filed wherein giant companies such as "Pinterest" have been targeted and revenues were made using the advertisements.[30] The main reason attributed to such a large number of suits have been recognized to be the absence of stringent laws against cyber-squatting, unlike in countries like Philippines[31] and United States[32] which have specific laws for cyber-squatting. The United States passed a legislation to govern such a serious and recurring offence, back in 1999, called the Anti-cybersquatting Consumer Protection Act (ACPA)[33]. The law allows the perpetrators to be booked for a civil suit and thereby damages.

Statistics from the World Intellectual Property Organization (WIPO) demonstrate that in 2017, the number of domain name disputes have shown a growth of 1.3 percent since the preceding year.[34] In 2018, the maximum disputes were from the United States amounting to a total of 920.[35]

In India, the Hon'ble Bombay High Court gave an important decision recently in June 2020, in the case of Hindustan Unilever v Endurance Domain and Ors[36] regarding the

[30] Dana Kerr, *Pinterest wins $7.2M in legal battle with cybersquatter*, (CNET, 30 Sept 2013) https://www.cnet.com/news/pinterest-wins-7-2m-in-legal-battle-with-cybersquatter/ (last visited on 05 September 2020)
[31] *Philippines: Analysis of the Cybercrime Prevention Act of 2012*, CENTRE FOR LAW AND DEMOCRACY, (Nov. 2012).
[32] Anti-cybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d).
[33] Anti-cybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d) (1)
[34] WIPO, *Cybersquatting Cases Reach New Record in 2017*, Geneva, (Mar. 14, 2018), http://www.wipo.int/pressroom/en/articles/2018/article_0001.html (last visited on11 September 2020).
[35] *Id.*
[36] Commercial IP Suit [2019] (L) NO.577.

responsibilities of domain name registrars (Intermediaries) and their technical capabilities in such cases of Cyber-squatting. The plaintiff was the registered owner of websites www.hul.co.in and www.unilever.com. However, the plaintiff observed that some parties had registered domain names such as "info@hulcare.co.in", "unilevercare.co.in", "unilevercare.org.in" and "unlevercare.co.in" which were deceptively similar to its own website. The Court ruled in favour of the plaintiff ordering an immediate injunction on the use of these domain names by the infringing parties.

HUL in this case has also impeded National Internet Exchange of India (NIXI), Endurance Domains, GoDaddy and other domain name registrars praying the court for blocking of these websites and continued suspension of registration of such domain names by these registries. Justice Gautam Patel discussed at length the role of these intermediaries and relief that can be granted against them. The court held that such intermediaries cannot be asked to permanently block domain names and suspend the registration of domain names until they are found to be infringing the rights of another party and are fraudulent in nature. The court observed that any such decision of blocking or suspending a domain name cannot be taken by the parties alone without any judicial finding. It is a significant decision for the future of cyber-squatting cases in India as it clarified the role and liabilities of the intermediaries in such cases. The said judgment also puts an end on the growing trend of injunction orders being passed by the courts against these domain name registrars without considering the technical and legal liabilities of the intermediaries in providing such relief. The world faced a huge number of cyber -criminal activities during the unprecedented times of COVID-19 pandemic wherein the global marketplace shifted online. About 48,000 new cases were seen around the globe by one service provider, WIPO during the lockdown.[37] Attackers targeted some very famous and major brands such as Facebook, Apple, Netflix and Amazon wherein the customers were scammed with the help of cyber-squatting techniques and deceived with reward and re bill scams.[38]

With the growing intersection between trademark and domain name systems in this digital age, negative consequences have increased drastically and need to be curtailed. In this

[37] WIPO, *Cybersquatting Case Filing Surges During COVID-19 Crisis*, [June 2020], https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html (last visited on 10 September 2020).
[38] Janos Szurdi, *Cybersquatting*, [September, 2020] https://unit42.paloaltonetworks.com/cybersquatting/

segment, authors have attempted to list down some grey areas as well as issues that must be addressed at the earliest.

- In India, currently there is no specific legislation for resolving disputes pertaining to cyber-squatting. The Trademark Act, 1999 does not include a chapter about "cyber-squatting" with stringent damages in case of contravention of the law.
- One of the main issues that cyberspace faces is domain name grabbing wherein people buy domain names with the intention to later monetize and sell it at high prices instead for personal usage. This results in the unauthentic and fraudulent use of the domain names.
- Due to the increasing online presence of various establishments, mere registration of domain names with the Registry is not enough for safeguarding the legitimate rights of parties, there is a dire need for specific statutory provisions regulating and penalizing acts like cyber-squatting. A proper procedure of registration would help in safeguarding as well as tracking the ownership of the domain names which are already registered as trademarks by another party. These records would also be beneficial in cases where any domain name is used to commit any cyber-crime such as phishing or identity theft etc. which is punishable under IT Act, 2000.
- The main issue that arises is about the jurisdiction since the internet has no boundaries and the trademark laws of every country are territorial in nature. Cyber-squatting can be committed from distant places which are outside the purview of the national courts and it poses the questions as to whether to file the case or where the complainant resides or the defendant. Secondly, the binding value of the decision of the registration authority is questionable. This often leads to non-reporting of cases of defaulters getting away after the crime due to the lack of proper regime of punishing.
- ICANN is a private organization and the involvement of all the countries is voluntary making it difficult to regulate such a growing and serious issue. In spite of WIPO being the service provider agency, there is a need to have a treaty/convention establishing a holistic international organization making it mandatory to all the UN members to ratify the same.

CONCLUSION AND SUGGESTIONS

In today's digital environment, domain names are seen as vital business assets. They play an important part in building brand value, consumer loyalty and popularity. With the growing business and commerce activities online, the threat of cyber-attacks has also grown exponentially. Cyber squatters target and attack the identity of well-known businesses so as to garner undue rewards by use or sell of these fraudulent websites. Considering the rise in Cyber-squatting cases in the recent years it is pertinent that strong measures are taken to counter this global menace as this misrepresentation not only infringes the rights of the legitimate trademark holders but also creates confusion in the general public.

In a country like India, where there is a lack of digital literacy there is an urgent need to have strong and specific Cyber and Intellectual Property laws as the current Trademark Act, 1999 and the Information Technology Act, 2000 are not adequate to prevent the cyber squatters from causing fraud to the general public and targeted businesses. There are certain recommendations that the authors would like to suggest in order to curb the situation, which are as follows:

- In India, Trademark Act, 1999 must include a chapter about "cyber-squatting" with stringent damages in case of contravention of the law. This would require amendment in the explanation of Section 2(m) to expressly include "domain name" in the definition of "mark".
- Under Trademark Act, 1999, ambit of penalty in case of infringement of copyright/trademark law must be widened to include online access to goods and services as well as public information through a website.[39]
- It is recommended for India to impose a strict liability with severe penalties in case of cyber-squatting. This is a great learning from the USA which has established legislations such as Anti-squatting Consumer Protection Act.[40]
- It is advised to resolve jurisdictional issues for better execution of laws and the binding nature of the decision.
- To avoid frivolous and wrong claims of domain names, registration must be cancelled, and such acts done in bad faith must be dealt with utmost strictness.

[39] Trademark Act, 1999, §103.
[40] Anti-cyber squatting Consumer Protection Act (ACPA), 1999

- Online mediation and expedited arbitration are a great way to resolve conflicts over the domain name disputes. This would be governed by rules of the WIPO Arbitration and Mediation Centre which will have a binding nature on the decision. The same would be reiterated as part of the application process when the companies/individuals buy their second level domain name.
- Administrative panels should be set up to regulate the domain name challenges and administer the allotment of second level domain names which tend to be identical or closely similar to names which could violate the existing intellectual property rights and put the legitimate owners at huge losses.[41]
- All the second level domain names must be published on its registration, much like a trademark application process. This would ensure transparency and avoid deceit and disputes.
- In case of instances of "identity theft" wherein misuse of famous celebrities and personalities is done, it is advisable to amend Section 66 of the Information Technology Act, 2000 and Section 469 of the Indian Penal Code, to execute the criminal liability created by the act of cyber-squatting. This would facilitate the filing of FIR against the perpetrators and penalize them for hacking of computer systems or for unauthorized extraction of data from computer systems as they had forged the electronic records to harm the reputation of others with a mala fide intent.

Thus, eliminating the menace of cyber-squatting is the need of the hour not only for preventing fraudulent acts, but also to promote and protect businesses in this growing age of digitisation and globalisation.

[41] WIPO, *Cybersquatting Case Filing Surges During COVID-19 Crisis*, [June 2020], https://www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html (last visited on 10 September 2020).