Page 740 - 757 **DOI:** *https://doij.org/10.10000/IJLMH.111980*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 5

2021

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This Article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact **Gyan@vidhiaagaz.com.**

To submit your Manuscript for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at **submission@ijlmh.com.**

Cybersquatting India: Genesis & Legal Scenario

MANTHAN AGARWALA[1] AND SIMRAN KANG[2]

ABSTRACT

Trademarks serve as identifiers and representatives of a company's goodwill. In recent years, there has been a lot of fuss about trademark infringement through various techniques, one of which being cybersquatting. Cybersquatting is the registration of a domain name that contains a reference to a well-known trademark in order to create the false impression that the domain name belongs to the trademark owner. Such misrepresentation can jeopardize a company's future potential. However, there is no regulation in India that governs cybersquatting, and efforts to achieve this goal have been primarily piecemeal. Despite the existence of an international framework to combat cybersquatting, it is insufficient to address the growing threat of cybersquatting. This document provides the groundwork for enacting anti-cybersquatting laws in India.

The authors have adopted black letter method of research and has used secondary materials such as books, online journals, databases, newspaper reports, statistical data etc. to arrive at conclusions.

Keywords: *Domain Name, IP Address, Arbitration, Owner, Trademark, Cyber squatter.*

I. INTRODUCTION

The recent internet trend has ushered in a transformation in the commercial world. Many company groups have moved to the online world of marketing and commerce, giving their companies more visibility. This has sparked an unhealthy competition in which people try to profit from other people's existing trade names in order to cash in on the goodwill connected with a trade name that was meticulously crafted by the proprietor. All reputable trade mark owners may not have or do not have their own domain, which could be used by a competitor. When it comes to registering a domain name, it's a first come, first served basis. Cybersquatting is when someone obtains a name that is similar to a trademark and attempts to sell or lease it. The legal problem in recent years has been to find a way to promote the development of intellectual property on the internet while limiting its unlawful exploitation. With the

[1] Author is a Student at O.P Jindal Global University, India.
[2] Author is a Student at Symbiosis International University, India.

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

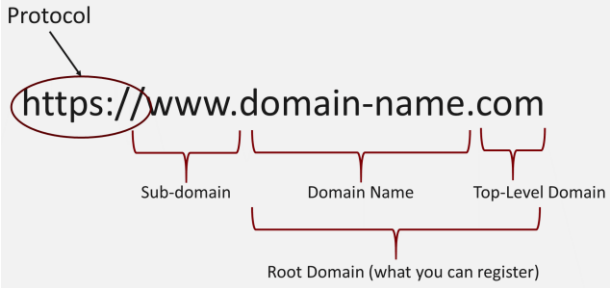
introduction of domain names, the practice of cybersquatting was born. Because not all merchants are internet or technology knowledgeable, their trade name may be utilized by another trader, who may then try to sell it to the true owner of the trademark, such as a domain name.

In this paper, the author's area of research is limited to trademark infringement through the phenomenon of cybersquatting. The researcher's in this work employed the black letter approach to collect data in order to find out about various studies and findings on Cybersquatting. The effectiveness of the available remedial treatments is also investigated. Cybersquatters are usually free to register any domain names, even if a domain name with a similar name already exists. Cybersquatters frequently utilize a combination of illegal and legitimate work to get money. As a result, the legitimate owner suffers a significant loss.

(A) Emergence of Cybersquatting

The threat of cybersquatting, also known as brand-jacking, initially surfaced in the 1990s, when the internet was a global craze[3]. The act of obtaining fraudulent registration of a domain name with the goal of selling it to the lawful owner of the name at a premium, as defined by Indian law, is known as cybersquatting[4]. This domain name is confusingly similar to or dilutive of an offline trademark or personal name that has already been registered[5].

A domain name is a combination of names on multiple levels[6]. For better understanding of domain name, we can look into the picture below-



To finish off this definition of a domain name, here is a quick explanation of its structure. Let's take the domain name of the domain-name website as an example: www. Domain-name.com

- www: this refers to the third-level domain (*World Wide Web*).

[3] Jonathan Anschell & John J Lucas, What's in a Name: Dealing with Cybersquatting, 21 Ent. & Sports Law 3 (2003).
[4] Manish Vij v Indra Chugh, AIR 2002 Del 243
[5] Mastercard v Trehan, 629 F. Supp. 2d 824, 830 (N.D. III 2009)
[6] Stefan Kuipers, The relationship between Domain names and Trademarks/Trade Names, Lund University (2015).

- Domain-name: refers to the second-level domain; this is the name of the site.
- .com: this is the *top-level domain* (TLD), also known as a domain name extension.

Country code TLDs (ccTLDs) and generic Top Level Domain (hence 'gTLD') names are the two categories of Top Level Domain (hereinafter 'TLD') names[7]. ccTLDs are country-specific domain names[8], such as '.in' in India and '.au' in Australia (which may or may not be available for foreign national registration). gTLDs are generic top-level domains that have no geographical restrictions[9]. Second-Level Domain (SLD) names are usually the target of cybersquatting[10]. Cybersquatting has expanded dramatically as more firms move online and enter the ecommerce market.[11]

Cybersquatters are focused on money. The cost of registering a domain name is low; however, after it is registered, revenue can be generated by placing advertisements on the website, such as pay-per-click ads[12]. Cybersquatting is also used to deflect attention away from the original trademark owner, making the latter to lose money[13]. Furthermore, a registered domain name is sold to the owner of a trademark whose identity is represented in the domain name for a large premium. Such a trademark owner is willing to pay a hefty fee to acquire the domain name because any ill will or nuisance caused by the latter can be traced back to the original brand owner due to their resemblance[14].

Cybersquatting is of various types[15], which are as under-

- Domain Name Squatting- The practice of registering an existing registered trademark as a domain name in order to extract money from the brand's original owner is known as domain name squatting.

[7] Michael L. Katz et al., Economic Considerations in the Expansion of Generic Top-Level Domain Names, Phase II Report: Case Studies, ICANN (Dec. 2010)
[8] Internet Assigned Numbers Authority, Delegating or transferring a country-code top-level domain (ccTLD), https://www.iana.org/help/cctld-delegation
[9] Daniel Fisher, Cybersquatters Rush To Claim Brands In The New GTLD Territories, Forbes (Feb, 2014), https://www.forbes.com/sites/danielfisher/2014/02/27/cybersquatters-rush-to-claim-brands-in-the-new-gtldterritories
[10] Stefan Kuipers, The relationship between Domain names and Trademarks/Trade Names, Lund University (2015)
[11] WIPO, Cybersquatting Cases Reach New Record in 2017, Geneva, (Mar. 14,2018), PR/2018/815, at http://www.wipo.int/pressroom/en/articles/2018/article_0001.html.
[12] Jordan A. Arnot, Navigating Cybersquatting Enforcement in the Expanding Internet, 13 J. Marshall Rev. Intell. Prop. L. 321 (2014)
[13] Dara B. Gilwit, The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How to Prevent Public Deception and Trademark Infringement, 11 Wash. U. J. L. & Pol'y 267 (2003)
[14] Rastogi Anirudh, Cyber Law, Law Of Information Technology And Internet, Lexis Nexis, P. 322
[15] Sankalp Jain, Cyber Squatting: Concept, Types and Legal Regimes in India & USA (Nov. 2015), SSRN: https://ssrn.com/abstract=2786474 or http://dx.doi.org/10.2139/ssrn.2786474

- Identity Theft- Identity theft is performed by using web apps to track the expiration dates of well-known domain names and then registering them in the monitors' names as soon as the prior registration expires. This is done in order to deceive prior website visitors who believe the site still belongs to the previous owner.[16]
- Typo Squatting- Typosquatting is the deliberate misspelling of a well-known brand in order to register a domain name that is similar to it. These cybersquatters bet on users misspelling the original trademark and being sent to their website as a result[17].
- Name-Jacking-Name-jacking is the act of registering a domain name that has its own goodwill or that reflects sponsorship by the person whose name appears in the domain name. The diverting of traffic from the target individual (whose name is used) to themselves is exploited by these cybersquatters

(B) How Cybersquatting can be an issue for one's business

If suppose one decides to develop a website and invests time, money into it, on search engine optimization, google adwords for building and driving traffic to the site and it becomes popular and important for the business as then the website acts as an address for the business on the internet. Suppose after all this, one finds out that tons of similar domain names have been registered by the Cybersquatters, be it every humanly imaginable typo of that domain name, or imaginable misspellings all have been registered as all of them are going to get substantial amount of traffic as a result of the popularity of that website and it is quite common for people to make mistakes while typing the domain name and end up at these misspelled domain names and ultimately the customers are being diverted. Although it may not be a large amount of customers or probable leads, but it is quite possible that these customers might end up with the Cybersquatters website and one cannot have control over the content of squatter's website.

Cybersquatters tend to redirect people to other sites which probably could be a gambling website, pornographic website, phishing website or most commonly to competitor's website or throw up automatically generated page covered in links, sponsored pay-per-click links.

The main issue is that the sites are relatable to the domain name, and as mentioned earlier the links are most likely to be that of the competitor and it is also possible that the links may even redirect to one's own website, if it is tied with google adwords as what they do is they automatically place ads on relevant sites which can include the Cybersquatters sites and

[16] Neil L. Martin, Cybersquatting: Identity Theft in Disguise , 35 Suffolk U. L. Rev. 277 (2001)
[17] Jude A. Thomas, Fifteen Years Of Fame: The Declining Relevance Of Domain Names In The Enduring Conflict Between Trademark And Free Speech Rights, 11 J. Marshall Rev. Intell. Prop. L. 1 (2011)

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

ultimately one will have to pay to have his/her own customers sent back to the website.

It is also possible that the customers will get distracted to a competitor's website and go there instead which will lead to loss of a valuable customer.

Thus we can say that, bigger the web presence, the more business one generates online, the bigger problem of Cybersquatting persists.

(C) Thin line between Cybersquatting and Domain Investment

It is important, however, to differentiate between domain investing and cybersquatting, as some people fail to identify the fine line between the two. Domain investors purchase domains that contain random dictionary terms or popular names in the hopes of reselling them at a greater price in the future. They make predictions about the kinds of domain names that people will require in the future and keep an eye on the latest industry news and trends in order to forecast future business trends and purchase domains accordingly.[18]

For instance, if we observe cryptocurrency, they are gaining more popularity and tend to register their names with phrases related to them. This is not cybersquatting. One falls into the realm of cybersquatting when:

- They buy a domain that resembles an already well-established business/brand.
- They already have a trademark on their name.
- They have an aim of defrauding people.
- They have an aim of generating income in the future by coercing the original business to buy it at a higher price.

For instance, buying a domain name like biiitcoin.com, btcoin.org etc to deceive people who wish to visit bitcoin.org.

Some of the latest cybersquatting incidents are:

- **Amul**

  It is one of India's largest dairy companies with a fiscal year 2019-2020 sales turnover of about 38,550 crore Indian rupees. It became a victim of cybersquatting when someone bought domains like Amuldistributor.com, Amulboard.com, Amufran.com etc.

  The con men created fraudulent bank accounts in Amul's name and sent false forms through email. They even demanded money as a subscription to become a Amul

[18] Elliot Silver, Domain Investing Guide, Domaininvesting.com

distributor and franchise and ran recruiting frauds and asked people to pay fees to submit job applications.

The con was active from 2018 until 2020, when Amul issued a public warning[19] about the fraud and initiated legal action to address the issue.[20]

- **Fox News**

  The owner of the domain names xofnews.com and foxnews-entertainment.com was sued by Fox News for using the same logo and design as the original Fox News site.[21] Moreover, when a person visited these websites, they were greeted with an article touting a miraculous weight loss supplement. A link to a payment page for purchasing the supplement was included towards the end of the article. The problem here is that people would trust the claims as they are published on what appears to be a credible media channel's website.[22]

- **TikTok**

  FotiosTsiouklas and Alan Gokugolu, two American friends, predicted that the app TikTok would become a big brand and acquired tiktoks.com for $2,000 shortly after it launched. Bytedance, TikTok's parent company, offered them $145,000 in exchange for the domain.[23] The couple, however, opted to keep the domain and launch a 'follower growth' business, offering a "follow-for-follow" service. They also charged a fee to help people grow their following.

  Bytedance launched a cybersquatting action against the two friends in August 2020 after a failed negotiating effort for the tiktoks.com domain.[24] According to the WIPO administrative panel decision report, the company filed an updated complaint in September to include three more domain names: tktokcharts.com, tiktokplant.com and Tiktokexposure.com.[25]

  As of Jan 2021, the Panel ordered the pair to transfer all the domains in dispute to the plaintiff.

- **Mistubishi**

  Another vogue for creating complaint sites has been on the rise, wherein cybersquatters

[19]https://amul.com/m/amul-parlours-fake-websites
[20]Prachi Gupta, August, 2021, No More Fake Amul Websites: Gujrat Coop wins legal battle against fraudsters, Financial Express.
[21]https://storage.courtlistener.com/recap/gov.uscourts.vaed.467676/gov.uscourts.vaed.467676.1.0_2.pdf
[22] Andrew Allmenn, February 2020, Fox News sues to take down Fake News sites, Domain Name Wire.
[23] Alexis Carey, June 2020, Melbourne Teens' Digital Agency Sparks $5 Million Business, Herald Sun.
[24]WIPO Case Summary: https://www.wipo.int/amc/en/domains/search/case.jsp?case_id=49963
[25]WIPO Arbitration and Mediation Centre, Administrative Panel decision, 2021: https://www.wipo.int/amc/en/domains/search/text.jsp?case=D2020-2439

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

purchase domain names they despise and then add the phrase "sucks" at the end. One of the most well-known gripe sites is Mitsubishisucks.com. This website was created by a Mitsubishi hater wherein he offered charts and graphs depicting Mitsubishi's sales decrease, customer complaints, workman discrimination issues, safety concerns, etc.[26]

II. PREVENTION OF CYBERSQUATTING AROUND THE WORLD

The United States was the source of the most disputes in 2018, with 920[27] in total. Some nations, such as the Philippines[28] and the United States[29], have strict regulations against cybersquatting that go beyond trademark law, whereas others, such as China[30], have lax laws for safeguarding intellectual property online, allowing cybersquatting to flourish. Squatters from China are notorious for registering domain names that sound like American brands. Pinterest, a photo-sharing service, has filed a lawsuit against a Chinese man, alleging that he had registered the domain name "pintersts.com" in bad faith[31]. The man was also accused of utilising Pinterest's unique "red-colored" logo on his website, which was only intended for dumping adverts, according to the firm. The cybersquatter from China was fined USD 7.2 million in damages, plus legal fees[32].

Following is a discussion of municipal legislation against cybersquatting in several jurisdictions, particularly Australia and the United States, followed by the international dispute settlement process at the international level, in keeping with the aims of this research work.

III. UNITED STATES OF AMERICA

The United States holds the distinction of implementing the first comprehensive cybersquatting legislation. The Anti cybersquatting Consumer Protection Act[33] (ACPA), which was passed by Congress in 1999, allows trademark owners to initiate a civil suit against cybersquatters who register domain names containing trademarks in order to profit from the marks. The ACPA allows two types of actions: one under the "Trademark" clause and the other under the "in rem"

[26] WIPO Arbitration and Mediation Centre, Administrative Panel decision, 2012: https://www.wipo.int/amc/en/domains/decisions/text/2012/d2012-1431.html
[27] Id
[28] Philippines: Analysis of the Cybercrime Prevention Act of 2012, Centre for Law and Democracy, (Nov. 2012), p. 14.
[29] Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d)
[30] Wu R, New Rules for Resolving Chinese Domain Name Disputes - A Comparative Analysis, 2001 (1) JILT, http://elj.warwick.ac.uk/jilt/01-1/wu.html
[31] Ilana Bergstrom, Pinterest Files Suit Against Chinese Cybersquatter, (Sep. 2012), https://lawblog.justia.com/2012/09/11/pinterest-files-suit-against-chinese-cybersquatter/.
[32] Dara Kerr, Pinterest wins $7.2M in legal battle with cybersquatter,, (Sep. 2013), https://www.cnet.com/news/pinterest-wins-7-2m-in-legal-battle-with-cybersquatter/.
[33] Supra 25, 15 U.S.C. § 1125

provision.[34] When cybersquatters can be found and the matter falls under the authority of US courts, the trademark provision[35] of the ACPA can be used. In order to prevail under this rule, the plaintiff must show that:

- the impugned mark is distinctive or famous;
- the domain name is identical or confusingly similar to a distinctive or famous mark or is dilutive of a famous mark; and
- the registrant registered, used, or trafficked in the domain name with a bad faith intent to profit from plaintiff's mark[36].

To protect innocent registrants from harassment, the ACPA provides them with a good faith defence as well as other protections available to defendants under the Federal Trademarks Act of 1946 (commonly known as the "Lanham Act")[37]. Apart from the attorney fees to the victorious plaintiff, the courts have the authority to impose injunctions, revocation and transfer, or damages[38] against the cybersquatter. The in rem provision[39] was inserted into the Act in order to bring to justice defendants who are unable to be located or who are outside of the Court's personal jurisdiction. The plaintiff has the burden of proof under this section to establish that:

- the trademark is registered with the United States Patent and Trademark Office ("USPTO") or is protected under Section 43(a) or (c) of the Lanham Act, and
- the plaintiff was unable to establish personal jurisdiction over the registrant or was unable to locate the registrant after the exercise of due diligence.[40]

The in rem provision limits the Court's authority to order the domain name to be forfeited, cancelled, or transferred to the mark owner[41]. One of the major flaws of the ACPA is that there is no mechanism for awarding damages. Furthermore, in the United States, the Department of Commerce manages the.us ccTLD in conjunction with NeuStar, a commercial company. There

[34] Domain Names and Trademarks, March 2000, Berkmen Klein Centre, Harvard.edu: https://cyber.harvard.edu/property00/domain/main.html
[35] Supra 25, § 1125 (d)(1)
[36] Supra 25, § 1125(d)(1)(A)
[37] J. Thomas McCarthy, On Trademarks And Unfair Competition, 25-268 (4th Ed. 2000)
[38] Supra 25, § 1117(d)
[39] Supra 25, § 1125(d)(2). "In rem" is a "technical term used to designate proceedings or actions instituted against the thing, unlike personal actions, which are said to be in personam.", Black's Law Dictionary 797 (7th ed. 1999)
[40]Pope, Michael Brian; Warkentin, Merrill; Mutchler, Leigh A.; and Luo, Xin (Robert) (2012) "The Domain Name System—Past,Present, and Future,"Communications of the Association for Information Systems: Vol. 30, Article 21.Available at: http://aisel.aisnet.org/cais/vol30/iss1/21.
[41] Supra 25, § 43, (d)(1)(C)

is no common Dispute Resolution Policy for.us domain names because there is no single entity[42] managing the domain name space. The usDRP[43] is used to request cancellation or transfer of.us domain names that infringe the complainant's trademarks, whilst the usNDP[44] assures that all.us domain name registrations have a close connection to the United States. There is no independent authority, like there is in Australia, that provides a fast-track method for resolving issues other than through litigation.

IV. AUSTRALIA

There is no specific legislation in Australia that provides a cause of action for cybersquatting.

However, a civil complaint for trademark infringement under the Trade Marks Act 1995[45], a passing off action under common law, or a suit for defamation can be brought against the cybersquatter. Consumer law, specifically the Competition and Consumer Act of 2010[46], prohibits misappropriation.

Apart from the civil law remedies listed above, the parties are free to arbitrate the matter under the.au Domain Administration Ltd's Dispute Resolution Policy (auDRP)[47] (auDA). The Australian Domain Authority (auDA) is a policy-making body tasked with developing and enforcing laws governing the registration of.au domain names as well as the functioning of the Australian domain industry[48]. It was founded in 1999 as a limited-by-guarantee not-for-profit organisation. It works under an industry self-regulatory paradigm, with members from both the supply and demand classes[49] on its Board of Directors. Its mandate is defined by the Ministry of Communications in Australia Development's Letters of Endorsement.

The (auDRP) establishes a process for impartial arbitration of conflicts between the objecting party (in some cases, a trademark holder) and the registrant. auDA does not actively arbitrate auDRP complaints; instead, it refers them to an auDRP that has been approved by auDA.The provider, in turn, appoints an arbitrator to investigate the complaint[50].WIPO is one among them

[42] Working Party on Telecommunication and Information Services Policies, Evolution In The Management Of Country Code Top-Level Domain Names (ccTLDs), Organisation for Economic Co-operation and Development, DSTI/ICCP/TISP(2006)6/FINAL (Nov. 2006)
[43] .us Dispute Resolution Policy, at http://www.neustar.us/policies/docs/usdrp.pdf
[44] Nexus Dispute Policy, at http://www.neustar.us/policies/docs/nexus_dispute_policy.pdf
[45] Trade Marks Act 1995, No. 119, 1995, Compilation No. 36.
[46] Competition and Consumer Act 2010, No. 51, 1974, Compilation No. 111.
[47] .au Dispute Resolution Policy (auDRP), Policy No: 2016-01 (Apr. 15, 2016), https://www.auda.org.au/assets/pdf/auda-2016-01.pdf
[48] About auDA, The .au Domain Administration Ltd., https://www.auda.org.au/about-auda/
[49] Review of the .au Domain Administration, Australian Government, Department of Communication and the Arts (April 2018)
[50] Domain Registration Services Australia, Domain Name Registrar, Information Centre, at https://www.domainregistration.com.au/infocentre/info-domain-cybersquatting.php

Provider of auDRP[51]. In the meanwhile, auDA may apply a registry server lock on the domain name. Suomotu or at the request of the parties, the matter will be resolved. After the conflict has been resolved, After a successful arbitration, a Deed of Settlement is prepared to document the final conclusion of the dispute disagreement.

One of auDA's biggest flaws is that it lacks a dispute resolution mechanism for conflicts involving Second Level Domain names based on gTLDs. It also exclusively handles disputes involving a breach or potential breach of an auDA Published Policy. To make matters worse, AuDRP establishes a concept for 'Domain Complaints.' Although this definition is broad, it only covers some sorts of cybersquatting, such as domain name squatting or typosquatting, due to the concept of ejusdem generis, but name-jacking and identity theft are not covered.

(A) International Framework on Cybersquatting

So far, we've looked at the local regulations that govern domain name disputes. However, because domain names are international in nature, disputes over them may be best resolved at the international level. The Internet Corporation for Assigned Names and Numbers (ICANN) is a major player in this area. The Internet Corporation for Assigned Names and Numbers (ICANN) was founded by the United States government in 1998. It presently serves as the administrator of the Domain Name System around the world, coordinating domain names, IP addresses, and autonomous system numbers[52].

Most notably, on October 24, 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) introduced a Uniform Dispute Handling Policy (UDRP)[53], which has proven to be a model law in the resolution of e-commerce issues. The UDRP is intended to provide a framework for resolving disputes between domain name holders or registrants and third parties claiming a prior interest in the domain name[54]. This policy has shown to be an effective and low-cost method of combating cyber squatters, among other things. Since its inception, it has dealt with over 7000 cases. To bind the registrant to the UDRP, all Registrars are required to include a dispute resolution clause in the registration agreement, compelling the registrant to submit to the UDRP in the event of any registration problems[55]. The UDRP is implemented by

[51]Id.

[52] M. Froomkin, ICANN'S Uniform Dispute Resolution Policy – Causes and (Partial) Curses, 67(3) Brooklyn Law Review 605 (2002)

[53] Uniform Domain Name Dispute Resolution Policy, ICANN, at http://www.icann.org/ udrp/udrp-policy24oct99.htm

[54] Second WIPO Internet Domain Name Process, World Intellectual Property Organization, at http://wipo2.wipo.int/process2 (on file with the Duke Law Journal)

[55] Vaibhavi Pandey, ICANN's UDRP As A Domain Name Dispute Redressal Mechanism (11 December 2013), http://www.mondaq.com/india/x/279078/IT+internet/ICANNs+UDRP+As+A+Domain+Name+Dispute+Redressal+ Mechanism.

ICANN-approved bodies. WIPO is the largest provider of UDRP services, handling UDRP for 76 ccTDLs in addition to gTLDs[56]

The UDRP has failed to achieve its goals in a number of areas. Before attempting to establish a skeleton of Indian legislation against cybersquatting, it would be necessary to spell out the UDRP's flaws. As a result, they've been enumerated.

1. The decisions of the arbitral tribunals under the UDRP are not final, in the sense that they do not constitute res judicata, and the parties are free to pursue their claims in any competent court. As a result, the fundamental goal of the UDRP, which was to provide time-bound dispute resolution, has been defeated.
2. The UDRP's limited applicability is a second fundamental impediment to the creation of a standard international dispute resolution system. UDRP does not apply to disputes involving ccTLDs or those originating under newly emerging alternative providers such as New.net.[57]
3. The UDRP is extremely vague and open to different interpretations. One example is the case of Wal-Mart Stores v Walsucks[58], in which the use of the word "sucks" in the domain name "walmartcanadasucks.com" was deemed confusing to the trademark "Walmart," while another case, Wal-Mart Stores v Wallmartcanadasucks.com[59], held that the use of the word "sucks" in the tradename "walmartcanadasucks.com.
4. The complainant must prove the registrant's bad faith in registering the domain name, while the registrant must demonstrate a "legitimate interest" in the domain name[60]. While the policy mentions the criteria that make up the constitution, such as "bad faith" and "legitimate interest," these lists aren't exhaustive. This gives a panel much too much leeway to interpret the phrases in their own way. However, common sense does not always win out, and as a result, there are significantly divergent UDRP conclusions on the same topic.
5. Furthermore, because the UDRP is not adopted as law in many countries, its dispute resolution system only has advisory value. As a result, the stare decisis doctrine does not bind arbitrators to past rulings, leading to even more uncertainty in decision-making.

[56] World Intellectual Property Organisation, Domain Name Dispute Resolution Service for Generic Top-Level Domains, http://www.wipo.int/amc/en/domains/gtld/.
[57] Lisa M. Sharrock, The Future Of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions From Within The UDRP Framework, 51 Duke Law Journal 817 (2001)
[58] D2000-0477 (WIPO July 20, 2000)
[59] D2000-1104(WIPO Nov 23, 2000)
[60] SK Lubricants Americas v. Andrea Sabatini, Webservice Limited, WIPO Case No. D2015-1566

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

6. Finally, the UDRP contains no deterrent provisions, such as awarding exemplary damages to the person whose trademark has been violated by the cyber squatter. The aggrieved party's two options are to have the cyber squatter's domain name registration cancelled or to have the domain name transferred to the complainant[61].

V. WHY ICANN & ACCPA FAILS TO CURB ANTICIPATORY CYBERSQUATTING

Many businesses' efforts to establish a claim on the Internet are being thwarted by online privateers who register and hold domain names in the hopes of subsequently ransoming them to enterprises that want to use them for lawful and beneficial reasons. As a result of this behaviour, individuals who are unable or unwilling to pay the fees requested by these domain-name marauders lose out on business opportunities.

While anticipatory cybersquatting may appear to be similar to other lawful speculative actions at first glance, it is distinct in that it actively obstructs corporate opportunity and hinders rights holders from fully utilising such rights. If a company's desired domain name has already been used, it will have to settle for a less attractive domain name that may be less successful in drawing consumers. As a result, anticipatory cybersquatting resembles ticket scalping in many ways, the practice of acquiring huge quantities of tickets to popular events and then reselling those tickets at inflated rates.[62]

Despite the fact that both the Anti-Cybersquatting Consumer Protection Act and ICANN's Uniform Domain Name Dispute Resolution Policy were created to prevent domain-name extortion, neither is especially effective in combating anticipatory cybersquatting. Both technologies were created to combat the types of cybersquatting that were widespread in the late 1990s, that is, the registration of domain names similar to well-known names and well-established brands. The Internet was not yet recognised as a tool for commercial success at the time, and few firms had an online presence, let alone a domain name. Cybersquatterscapitalised on the corporate world's sluggish embrace of the Internet by registering domain names that were identical or similar to the names of well-known companies' goods.[63]

Panavision lnt'l, L.P. v. Toeppen,[64]

The defendant registered over 200 Internet domain names in 1995, including those that were

[61] PSA, India: Tackling Domain Name Disputes - A Simpler Way (Aug. 2013), http://www.mondaq.com/india/x/257384/Trademark/Tackling+Domain+Name+Disputes+A+Simpler+Way
[62]EranKehana, Trademarks in Cyberspace: 2013 in Review, The Business Lawyer; Vol. 70, Winter 2014/2015.
[63] Linda A. Freidman, February 2016, Online use of Third Party Trademarks: Can your Trademark be used without your permission?, American Bar Association
[64]141 F.3d 1316 (9th Cir. 1998), aff'g 945 F. Supp. 1296, was a case of first impression involving domain-name registration (C.D. Cal. 1996): https://law.justia.com/cases/federal/district-courts/FSupp/945/1296/1457774/

similar to well-known corporations and brands. "Panavision.com," the name of a well-known motion picture equipment firm, was one of these domain names. Panavision filed action under the Federal Trademark Dilution Act after the defendant sought to sell the domain name to Panavision for $13,000. The defendant was in the business of registering trademarks as domain names and then selling them back to the genuine trademark owner, and this constituted commercial use of the domain name, according to the court. Furthermore, the court determined that the defendant had diluted Panavision's mark on the basis that a domain name serves as both an address marker and an identifier for the business that controls the website.

In the years after Panavision, cybersquatting has evolved into a variety of new forms, including anticipatory cybersquatting. Given that the bulk of cybersquatting laws and legislation were adopted almost two decades ago, substantial gaps in cybersquatting blocking presently exist. Victims of anticipatory cybersquatting do not have to suffer in silence any more, although most existing remedies are, regrettably, quite indirect in their approach.

For instance, while the ACPA allows for the acquisition of domain names for resale to existing trademark owners, it does not provide for the modern practice of registering domain names with low current value in the hopes that they will become more desired and hence more valuable in the future.

Despite the fact that the ACPA was established as part of trademark law, it fails to apply one of the legislation's major concepts to domain names, rendering the law mostly ineffective in combating anticipatory cybersquatting. In the United States, trademark rights are closely linked to commercial use. The first-to-use, not the first-to-file, is the owner of a trademark. When a trademark owner ceases using a mark and does not plan to use it again, the mark is considered abandoned.

Notably, the absence of use of a trademark for three years generates a rebuttable presumption of abandonment. As a result, trademark law includes the idea that someone who is not utilising a trademark should not be able to prevent another person from using it productively. Anticipatory cybersquatters, meanwhile, fail to put the domain name at issue to useful use while also preventing others from doing so. As a result, anticipatory cybersquatting runs counter to the public policy that underpins trademark law. Despite this, the ACPA leaves cyberquatting essentially unregulated.

In spite of the fact that the UDRP does not explicitly prohibit anticipatory cybersquatting, ICANN has frequently tried to mitigate the impact of this activity by establishing new top-level domains. However, anticipatory cybersquatting has not been eliminated by this regulation.

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

ICANN's strategy of expanding top-level domains has minimal impact on cybersquatting since ".com" domains remain the most popular and profitable. The bulk of potential website visitors are familiar with ".com" names. In fact, Internet-based firms are commonly referred to as "dot-coms." As a result, people searching for a company's website are likely to believe it is a ".com."

UDRP panels have been progressively extending their interpretation of the bad-faith UDRP factor to find against anticipatory cybersquatters. To be more specific, administrative panels are more inclined to decide that actions taken to take advantage of a complainant's goodwill in its mark are sufficient to constitute bad faith under the UDRP. A respondent's passive ownership of a domain name is proof of bad faith usage and registration since it implies registration to sell the domain name for profit.

UDRP panels' interpretations and decisions are not directly reflected in the UDRP's wording. The UDRP should include a "not-for-resale" clause or a non-use restriction that gives registrants a limited length of time from the date of registration to make bona fide use of the domain name. A domain proprietor might be restricted from reselling the domain for more than the registration price. A non-use provision allows third parties to request a domain transfer if a registrant fails to use the domain for a certain period of time.

The UDRP already uses the criteria of bona fide usage to evaluate lawful use. Therefore, this change is obviously in the spirit of the policy. No extra infrastructure is required since non-use domain-name challenges follow the same procedures and result in the same remedies as present arbitration. In 2015, ICANN revised the UDRP to simplify the dispute resolution process. However, no specific wording or provision has been included to address anticipatory cybersquatting.

VI. INDIA'S STAND ON CYBERSQUATTING

Cybersquatting is a global threat that resembles terrorism in its scope[65]. Despite being aware of the consequences of cybersquatting, India has yet to pass legislation specifically outlawing the practice.

In and of itself, cybersquatting presents two fundamental questions:

- Is it possible to register domain names as trademarks?
- Which law should govern cybersquatting if domain names cannot be registered as trademarks?

[65] Ashwin Madhavan, Domain Names and Cybersquatting, Indian Law Journal, http://www.indialawjournal.org/archives/volume1/issue_2/article_by_ashwin.html

(A) Is it possible to register domain names as trademarks?

A domain name is, by definition, an address comparable to any residential address, such as '9 Akbar Road, New Delhi.' A domain name, on the other hand, is unique, and no two people may hold the same domain name. Furthermore, a domain name may include a person's name or any descriptive term as the SLD, which is in violation of trademark law's essential premises[66]. As a result, it appears that domain names and trademarks are not interchangeable. Domain names, on the other hand, serve as identifiers for a certain brand of goods or a given level of service in the world of ecommerce[67]. This may have spurred the Indian judiciary to apply trademark law concepts to domain name disputes, ensuring that cybersquatting does not infringe on offline trademark rights.

Yahoo Inc. v Aakash Arora &Anr[68]. was the first case in India to bring cybersquatting to the notice of the judiciary. The defendant in this case created a website with the domain name YahooIndia.com that offered services identical to those offered by the Plaintiff. The court decided in favour of Yahoo. Inc (the Plaintiff) in a lawsuit filed by the Plaintiff, stating, "It was an attempt to profit from the fame of Yahoo's trademark." A domain name registrant does not acquire any legal right to use that domain name just by registering it; he could still be held accountable for trademark infringement.

The Supreme Court of India, in Satyam Infoway Ltd. v Sifynet Solutions[69], brought this High Court judgement to a conclusion and potentially a step forward. The Respondent in this action registered two domain names, www.siffynet.com and www.siffynet.net, that are confusingly similar to the Plaintiff's domain name, www.sifynet.com. The plaintiff originally utilised the term "Sify" as an acronym for its business name, Satyam Infoway. This brand had a lot of clout in the marketplace. "Domain names are commercial identifiers, serving to identify and distinguish the firm itself or its goods and services, and to define its associated online location," the Supreme Court said in an oft-quoted statement in response to the Plaintiff's plea. This case is significant because the court acknowledged that the domain contains all of the characteristics of a trademark and upheld the Plaintiff's claim based on the principle of passing off.

(B) Which law should govern cybersquatting if domain names cannot be registered as trademarks?

[66] Surgicenters of America, Inc. v Medical Dental Surgeries Co., 601 F.2d 1011, 1014 (9th Cir. 1979) citing Abercrombie & Fitch Co. v Hunting World, Inc., 537 F.2d 4, 9-10 (2d Cir. 1976)
[67] Anish Dayal, Law and Liability on the Internet, in Kamlesh N. Agarwala & Murali D. Tiwari (eds.), IT and Indian Legal System, (New Delhi: MacMillan, 2002), p. 56.
[68] 78 (1999) DLT 285.
[69] 2004 (6) SCC 145

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

According to India's current legal framework, cybersquatting can be challenged in court, through arbitration before ICANN-approved panels, or by physically issuing cease-and-desist warnings to the putative cybersquatter[70]. Furthermore, a disagreement can be registered with the.in registry, which is managed by the National Internet Exchange of India (NIXI). The.in registry provides a quick dispute resolution procedure, with issues being transferred to arbitration within 30 days of the complaint being lodged[71]. However, as stated in the previous section, these strategies are insufficient in a number of ways.

The principal legislation punishing cybercrime, the Information Technology Act of 2000[72], is mute on the issue of cybersquatting. In India, there is no law prohibiting cybersquatting. The legislature appears to have thrown the ball in the court of the judiciary, as it is the judiciary that has stepped forward to prevent cybersquatting in the lack of effective laws. As a result, in the realm of domain names, courts adopt the principle of passing off. For example, in Dr. Reddy's Laboratories Ltd. v Manu Kosuri[73], the defendants were barred from using the domain name drreddyslab.com, which was identical to the plaintiff's trade name, because it gave the impression to customers that the defendant's products were linked to the plaintiff's, allowing the defendant to profit by passing off its products as the plaintiff's.

The plaintiff was awarded a permanent injunction, and the defendant was prohibited from utilising the trademark.

VII. RECOMMENDATION & SUGGESTION

Effective cybersquatting redress necessitates efforts in two directions: first, the acknowledgment of domain names as trademark subject matter, and second, the prohibition and penalization of cybersquatting. One can argue that simply registering a domain name with the relevant Registry is adequate security for a domain name because no one else can register it (due to the uniqueness of the IP address associated with a domain name). So, why should domain names be protected as trademarks? The explanation is simple: as e-commerce grows in popularity, a company may only have an online presence; this online presence will undoubtedly necessitate the purchase of a domain name, which will serve as the company's identity. What is the remedy available to the owner of the earlier domain name if another entity

[70] Divya Srinivasan, India: DNS The Menace: Cybersquatting (Sep. 2015), http://www.mondaq.com/india/x/425096/Trademark/DNS+the+Menace+Cybersquatting.
[71] Charms, And Dangers Of Harry Potter's World, (Text of speech delivered by Justice Yatindra Singh, Judge Allahabad High Court, Allahabad] (May 2008), http://www.allahabadhighcourt.in/event/IPR_on_the_Internet_4-5- 2008.pdf
[72] No. 21 OF 2000
[73] [2001 PTC 859 (Del)]

tries to falsify and benefit from its goods under this domain name, for example, by inserting a comma or an underscore in the SLD and registering it (in other words, typosquatting)? If the domain name is identified as a trademark, the domain name owner will have legal grounds to have the deceptively similar or confusing domain name removed. In light of this, it is strongly recommended that cybersquatting legislation be adopted as quickly as possible, preferably by revising the Information Technology Act of 2000 and the Trade Marks Act of 1999.

(A) Domain Name as Trademark

Proposed amendments to Trademarks Act 1999-

- Existence of an identical or confusingly similar trademark in the same class of products or services in the offline market should be made a relative ground for a domain name's refusal to be registered as a trademark.
- The definition of mark in Section 2(m) should be changed to explicitly include domain names in its ambit.
- When a trademark application is pending or the trademark's title is questioned in court, the law must prohibit the registration of a domain name that is identical to or confusingly similar to the one in issue. This is because cybersquatters frequently take advantage of trademark registration ambiguity to steal lucrative domain names.
- The issue of establishing jurisdiction is one of the most difficult aspects of domain name disputes. When the cybersquatter is located in another country, the courts are frequently unable to exercise jurisdiction under national laws. Furthermore, locating the cybersquatter in person is not always practicable. In such circumstances, India should consider adopting the American Anti-Cybersquatting Consumer Protection Act's "in rem" provision.
- The Trademarks Act of 1999 could be amended to include a new chapter prohibiting cybersquatting that results in trademark infringements. For this purpose, cybersquatting should be widely defined to include domain name registrations based solely on conjecture, registration of a deceptively similar domain name to capitalize on the goodwill of a certain business, and so on.
- Section 103's reach should be broadened to include anybody who "provides online access to products or services or publishes any information about such goods or services on a webpage with a domain name that is confusingly similar to an already existing trade mark.

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]

- One way to counter abuse of domain name is to award it to those who can identify the proposed name with their business. Likewise, filing of Incorporation Certificate of the company are some such documents that can be made a pre-requisite for registration of a domain name.
- Concerning anticipatory cybersquatting, a rigorous industry specific market cap can be introduced that will regulate the selling of the domain names by the investors. This will dissuade unnecessary filings of domain names and will avoid extortion of money at the hands of businesses and the rightful owners of the domain name.

VIII. CONCLUSION

Businesses have been robbed of their fortunes by cyber squatters. In light of the current global situation, it is safe to say that cybersquatting is a threat that has no boundaries, because of the issues raised, many jurisdictions investigated them. The most effective countermeasure is not found in soft law instruments such as policies or regulations; rather, existing relevant laws must be amended to give statutory effect to the crime of cybersquatting. It is also recommended that frequent international meetings be organized to monitor and review the functioning of ICANN. As the authors pointed out in their proposals, India can cherry-pick useful provisions from other jurisdictions. Once an efficient cybersquatting mechanism is in place, India will join the select group of countries that have enacted such legislation.

*****

© 2021. International Journal of Law Management & Humanities [ISSN 2581-5369]