



A CRITICAL STUDY ON CYBER SQUATTING INVOLVING IN TRADEMARKS UNDER IPR IN INDIA

**AUTHOR : LOKESHWARAN MURUGESANREGISTER
NUMBER 131902028DEPARTMENT :BA LLB(HONS)**

YEAR :5TH YEAR

SAVEETHA SCHOOL OF LAW

**I'M SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES(SIMATS) SAVEETHA
UNIVERSITY
CHENNAI - 77**

ABSTRACT:

Cybersquatting takes place while someone registers, sells, or makes use of a site call that contains the trademark or carrier mark of an current company, normally proceeding to promote the area call to the mark`s proprietor at a profit. It consists of any time someone registers, sells, or makes use of a site call with the intention to take advantage of a trademark`s goodwill. There are methods to achieve a prison treatment towards a cybersquatter: suing beneath the Anticybersquatting Consumer Protection Act (the “Act”) or the use of the Internet Corporation of Assigned Names and Numbers` (ICANN) global arbitration system. However, you'll be capable of achieve statutory cash damages from \$1,000 to \$100,000 in keeping with area call. In a few cases, you could document an movement towards the area call itself, as opposed to suing an character or business.In a lawsuit, you'll want to show that the area call registrant possessed a bad-religion motive to take advantage of the trademark, that the trademark became specific while the alleged cybersquatter registered the area call, that the area call is similar to or confusingly much like your trademark, and that federal trademark regulation protects your trademark.

KEYWORDS:

Cybersquatting,Trademarks, consumer, business, anticybersquatting.

INTRODUCTION:

Cybersquatting means unauthorised enrollment and use of internet sphere names that are identical or analogous to that of trademarks, service marks, company names, or particular names. For illustration, using a brand name to increase hunt results for another product is a traditional violation, pretending to be or represent a brand still is cyber-squatting. Cyber-squatting in India has increased drastically in the last many decades and has put adverse goods on the rights of Intellectual Property holders. Cyber-squatters can oppressively damage the brand and trademark proprietor simply by using the sphere name of their brand. In India in the absence of needful cyber laws it's delicate to help cyber-squatting. The cases of cybersquatting are decided under the applicable position of trademark laws. Daniel J. Boorstin said that “ An image isn't just a trademark, a design, a watchword, or an fluently remembered picture. ” It's a cleverly drafted personality profile of a person, organisation, business, product, or service. Sphere names on the internet have a huge request of their own. The world is passing a new revolution in the area of dispatches, which has handed a plethora of new openings for cyberspace. The internet's adding significance has converted it into an important platform for companies to promote, announce, and vend goods and services. Unfortunately, cybersquatting, which is the result of deceptive and illegal conduct, has risen as well. In this composition, we will understand the meaning of cybersquatting and how it interferes with a brand identity. The composition will also reflect on how social media platforms have given rise to new forms of cybersquatting. In light of this, we will bandy the cases involving cybersquatting and the remedies available. The word “ squinching ” comes from the act of enwrapping an abandoned or unoccupied space or structure that the squatter doesn't enjoy, rent, or have authorization to use. Cybersquatting, on the other hand, is distinct in that the sphere names that are being “ scrunched ” are (occasionally but not always) paid for by the cyber squatters during the enrollment process. Cyber squatters typically demand much advanced rates than the bones they paid for it. Some cyber squatters make disparaging reflections about the individual or business the sphere is supposed to serve in order to convert the subject to buy the sphere from them. Others monetise their squinching by posting paid links to the factual point that the stoner likely wanted through announcement networks. There are a variety of realistic forms of cybersquatting that attract attention, which come under the broader order of cybersquatting. Typosquatting, classic cybersquatting, cyberpiracy, and mock cybersquatting are exemplifications of these variations. The “ classical cybersquatting ” is the simple enrollment of a sphere name grounded on a trademark with the intention of dealing it to the trademark's licit proprietor for a profit. The aim of the paper is to study about the cybersquatting and their involvement in trademark.

OBJECTIVES:

- To study cyber squatting and their involment with trademark.
- To analyse the legal aspects relating to trademark and Cybersquatting
- To find out general public view on Cyber squatting
- To examine the effectiveness of the same.

REVIEW OF LITERATURE:

(Alok 2010)The growth of commercial activities on the internet have propelled domain names to emerge as significant business identifiers. At the same time, domain name disputes have also increased. Also, there has been instances of domain name abuse and misuse in the form of cyber-squatting. Despite having no specific law to handle domain name disputes, Indian courts have played a prominent role in resolving the generic top level domain disputes (gTLDs) under the Trademarks Act, 1999.

Alok 2010; Dasgupta 2009)Indian courts have repeatedly held the domain names as online trademarks and business identifiers. They have applied the grounds of trademark infringement and passing off someone else's goods as one's own to domain names to protect the interest of genuine parties. They have granted injunctions against the cyber-squatters and ordered the transfer of domains to genuine parties. In some cases, they have also imposed monetary penalties against the cyber-squatters and ordered them to pay legal fees to the plaintiffs.

Neupane 2019)Corporations and TradeMark holders are required to use their preferred domain name by buying it from cybersquatters for a huge amount of money because there is no way to use two domain names that are pronounced exactly the same. Apart from that, they frequently have to pound on the doors of courts in order to bring cybersquatters before the judiciary and to get justice against their unethical and illegal act.

Mambi 2010)A Trade Mark is an exclusive identity of the goods or services of the its owner.

A Trade Mark is defined as "a mark capable of being represented graphically and which is

capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours.A registered Trade Mark distinguishes the goods and services of its owner from the goods and services of his competitors in the business course by empowering the owner with the right to exclusively use the mark for only his goods and services.

Dewani et al. 2022)Domain names can be registered and protected as a Trade Mark provided that it fulfils all the conditions which are required in order to be registered as a Trade Mark. So, a domain name which is unique, distinctive and distinguishes the goods and services offered by its owner from others, can be registered and protected as a Trade Mark. It must fulfil criteria like it should not be misleading, confusing or deceiving to consumers of other corporations engaged in similar business courses.

Dewani et al. 2022; Ryder and Madhavan 2014)The number of cybersquatting disputes filed with the World Intellectual Property Organization (WIPO) in 2006 increased by 25% as compared to 2005. In a related development, the evolution of the domain name registration system is causing growing concern for trademark owners, in particular some of the effects of the use of computer software to automatically register expired domain names and their 'parking' on pay-per-click portal sites, the option to register names free-of-charge for a five-day 'tasting' period, the proliferation of new registrars, and the establishment of new generic Top Level Domains (gTLDs).

Sharma 2011)While electronic commerce has flourished with the expansion of the Internet, recent developments in the domain name registration system have fostered practices which

threaten the interests of trademark owners and cause consumer confusion. Practices such as 'domain name tasting' risk turning the domain name system into a mostly speculative market. Domain names used to be primarily specific identifiers of businesses and other Internet users, but many names nowadays are mere commodities for speculative gain," noted Mr. Francis Gurry, WIPO Deputy Director General, who oversees WIPO's dispute resolution work.

United States. Congress. House. Committee on the Judiciary 1999) In 2006, a total of 1,823 (gTLDs and country code Top Level Domains (ccTLDs)) complaints alleging cybersquatting - the abusive registration as domain names of trademarks - were filed with WIPO's Arbitration and Mediation Center (Center), representing the highest number of cybersquatting cases handled by WIPO since the year 2000.

United States. Congress. House. Committee on the Judiciary 1999; Rockman 2004) The WIPO dispute resolution procedure served a wide range of users, ranging from well-known brands, to smaller enterprises and organizations, as well as individuals. They covered categories including luxury items, famous persons, entertainment, hospitality, sports, gambling, and pharmaceuticals. In addition, charitable organizations and educational institutions were involved.

Thomas McCarthy 1996) Domain name tasting is a practice in which a person or entity (who may be affiliated with a registrar) registers a domain name for a five-day grace period without payment of the registration fee, and parks it on a pay-per-click website monitored for revenue, whereupon the name is dropped or re-registered by a new registrant, thereby starting a new grace period. Only those domain names generating significant traffic are permanently registered.

Thomas McCarthy 1996; Sharma 2011) WIPO panel decisions are beginning to explore the practical implications for the UDRP of these developments, for example in terms of whether or not the privacy service discloses the identity of its client once the service has been alerted to concerns of trademark infringement. The fundamental assumption of the UDRP is that the formal respondent for case purposes is to be found in the applicable Whois database.

World Intellectual Property Organization 2004) WIPO panels have generally held that for a domain name to be transferred under the UDRP, there needs to be some indication that the registration was made with the intention of taking advantage of the complainant-trademark owner's rights in that name. The rate at which domain names change hands and the difficulty to track such mass automated registrations challenge trademark owners in their pursuit of cybersquatters.

World Intellectual Property Organization 2004, 2002) Cybersquatting is a process of registration of a trademark as a domain name and trading it with the intent of gaining profits. A trademark cannot be registered as a domain name by the owner itself until it is owned by the cybersquatter. This results in a breach of fundamental rights for the owner to use the trademark.

Levine 2015; Davidson 2009) Intentional bad faith usage in domain names that are similar to the existing trademarks is the negativity of cybersquatting. These registrants are considered "modern day extortion". A fitting definition: "an illegal cybersquatter should be one who

acquires a domain name for the sole purpose of obtaining money or other advantage from the trademark owner, with no intent or desire to use the domain name, except as an instrument toward this purpose.”

Levine 2015; Rockman 2004)Cyber-squatting is a practice of registering the domain name that is likely to be wanted by another person, business, or organisation in the hope that it can be sold to them for a profit in the Internet. It involves the registration of trademarks and trade names as domain names by the third parties, who do not possess any rights over such domain names. Cyber-squatters or bad faith imitators register such trademarks belonging to third parties with the common motive of trading the reputation and goodwill of such third parties by either confusing potential customers and later selling the domain name to the rightful owner at higher profit.

Lindsay 2007; United States. Congress. House. Committee on the Judiciary 1999)The use of trademarks in domain names with the goal of attracting more traffic to a list of similar web pages identified by a common name is referred to as “cyberpiracy.” While “pseudo cybersquatting” is described as the registration of a domain name without actually using it or connecting it to any online web pages or active website. These are also known as “blocking registrations,” and they aim to prevent legitimate right holders from using domain names. All of the above actions are classified as different types of cybersquatting.

Lindsay 2007; Trade-Mark Practice in Canada 2011)The practice of cyber-squatting originated from the time when most businesses were not savvy about the commercial opportunities over the Internet. Some enterprises registered the names of well known companies as domain names with an intention of selling the names back to the companies when they finally woke up. Panasonic, fry’s electronics, Hertz and Avon were amongst the victims of cyber-squatting. Opportunities for cyber-squatters are rapidly diminishing as most of the companies now know that nailing down domain names is their higher priority in order to survive in the global market.

Lindsay 2007; Trade-Mark Practice in Canada 2011; Fishman 2022)Cybersquatters deliberately exploit the first-come-first-served nature of the domain name registration system and then the squatters either offer to sell the domain to the person or company who owns a trade mark contained within the name at an inflated price. In India, there is no statute law which explicitly refers to dispute resolution in connection with cyber squatting or other

domain name disputes.Clemson 2019; Wolfe and Chasser 2012)Cyber squatters usually demand much higher rates than the ones they paid for it. Some cyber squatters make insulting remarks about the business or individual the domain is supposed to serve to convince the subject to purchase the domain name from them. Others monetise their squatting process by posting paid links to the original site that the user likely wanted via advertisement networks.(Elias and Gima 2001)The Trademarks use in domain names with the goal of attracting more traffic to the list of similar web pages recognised by a name is referred to as “Cyberpiracy”. At the same time, Pseudo Cybersquatting is explained as the Domain Name Registration without actually using it or associating it to any online websites/web pages. There are also known as “Blocking Registrations”, and they intend to avoid legitimate correctholders from using domain names.

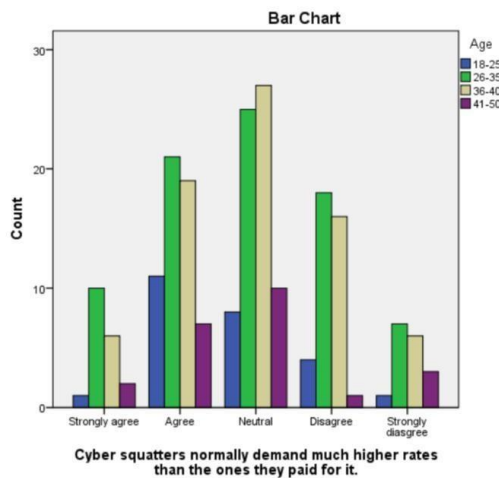
METHODOLOGY:

This research has adopted empirical study. Key characteristics for empirical research are Cyber Crimes, Economic Impact, Cyber Threats, Internet, Manipulation. Specific research questions to be answered And Description of the process used to study this population or phenomena, including selection criteria, controls, and testing instruments (such as surveys).the statistical tools used for this research work is chi square, correlation. SPSS graphics and diagrams are attached in this research work.cross table has been used for this research work. The essence of the survey method can be explained as “questioning individuals on a topic or topics and then describing their responses”. Convenient sampling method was used for the purpose of this study. There are a total of 200 samples collected for this study. Independent variables were Name, Age, Gender, Education qualification, Occupation and monthly income. Dependent variables were cyber squatters normally demand much higher rates than the ones they paid for it and social media is a new target for cyber squatters. The tool uses for analysis was chi square method.

DATA AND ANALYSIS:

Figure 1:

Figure 1:



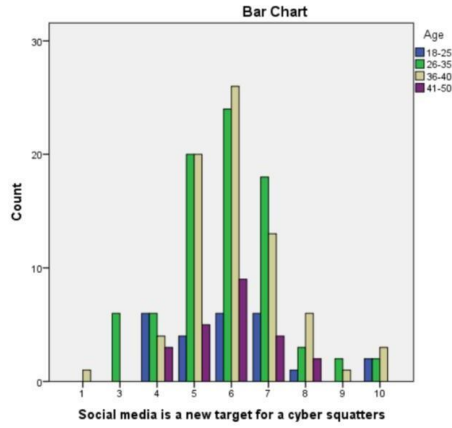
Legend:

Age of the respondent and higher rates of demand by cyber squatters than the ones they paid for it.

Age of the respondent and higher rates of demand by cyber squatters than the ones they paidfor it.

FIGURE 2

FIGURE 2



Legend:

Age of the respondent and social media is the best target for cyber squatters .

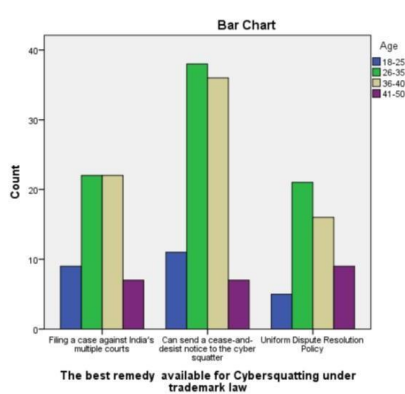
Legend:

Age of the respondent and social media is the best target for cyber squatters .

Figure

3

Figure 3



Legend:

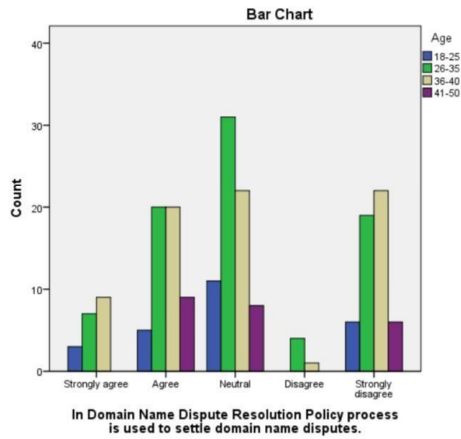
Age of the respondent and best remedy available for cyber squatting under trademark law.

Legend:

Age of the respondent and best remedy available for cyber squatting under trademark law.

Figure 4

Figure 4



Legend:

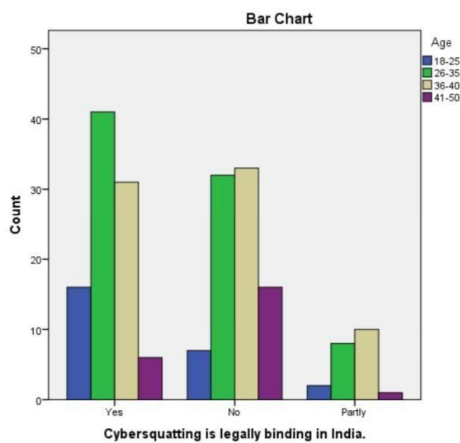
Age of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Legend:

Age of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Figure 5

Figure 5



Legend:

Age of the respondent and cyber squatting is legally binding in India.



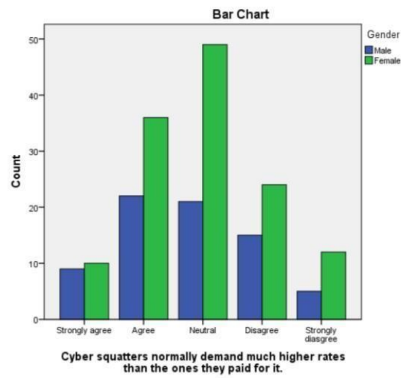
Legend:

Age of the respondent and cyber squatting is legally binding in India.

Figure

6

Figure 6



Legend:

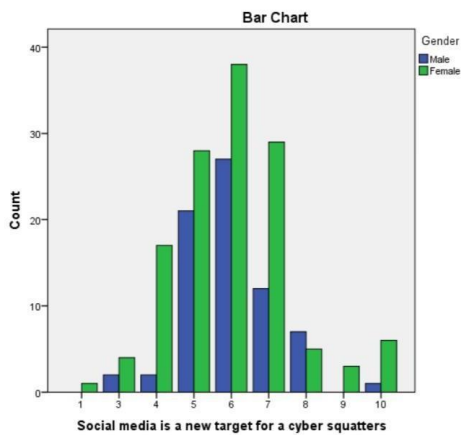
Gender of the respondent and higher rates of demand by cyber squatters than the ones they paid for it.

Legend:

Gender of the respondent and higher rates of demand by cyber squatters than the ones they paid for it.

Figure 7:

Figure 7:



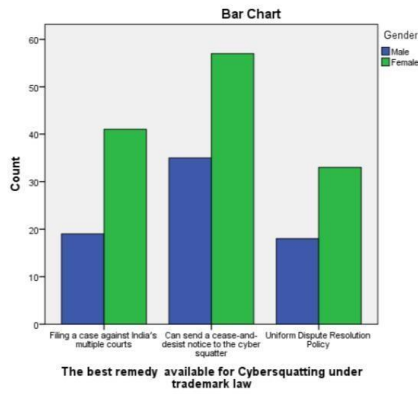
Legend:

Gender of the respondent and social media is the best target for cyber squatters.

Legend:

Gender of the respondent and social media is the best target for cyber squatters. Figure 8

Figure 8



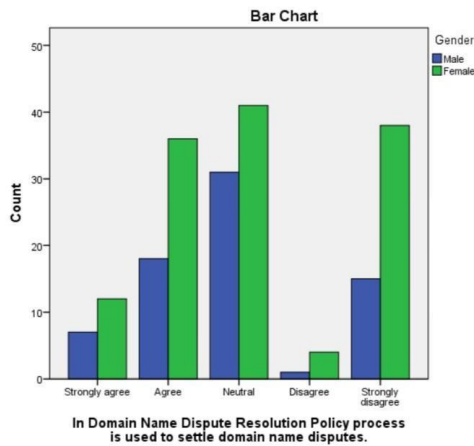
Legend:

Gender of the respondent and best remedy available for cyber squatting under trademark law.

Legend:

Gender of the respondent and best remedy available for cyber squatting under trademark law. Figure 9;

Figure 9;



Legend:

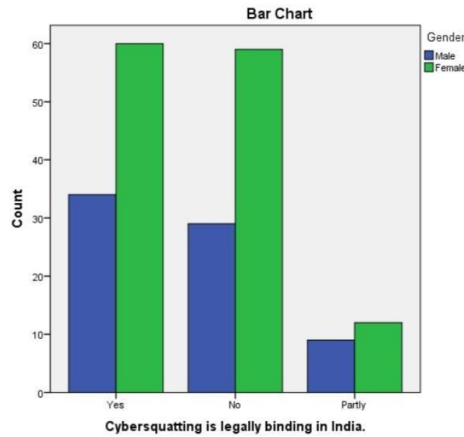
Gender of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Legend:

Gender of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Figure 10

Figure 10



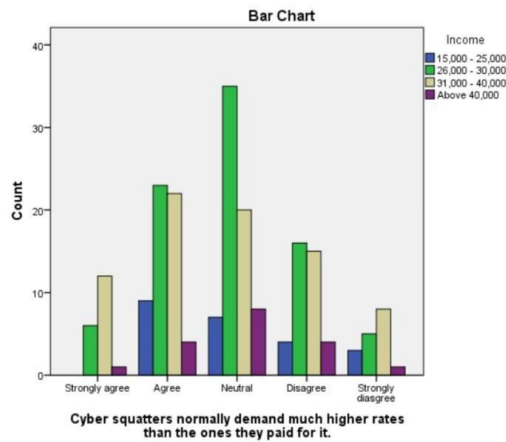
Legend:

Gender of the respondent and cyber squatting is legally binding in India.

Legend:

Gender of the respondent and cyber squatting is legally binding in India. Figure 11:

Figure 11:



Legend:

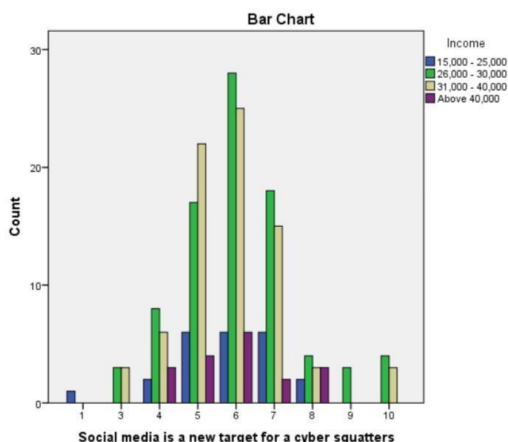
Income of the respondent and higher rates of demand by cyber squatters than the ones they paid for it.

Legend:

Income of the respondent and higher rates of demand by cyber squatters than the ones they paid for it.

Figure 12

Figure 12



Legend:

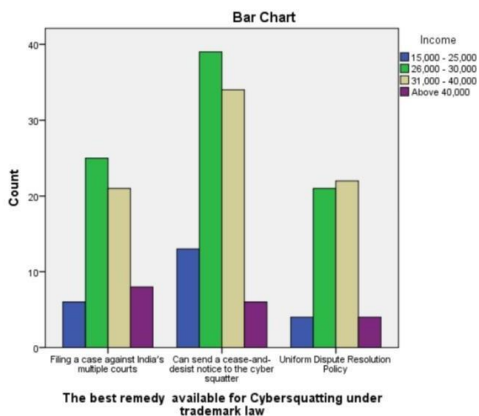
Income of the respondent and social media is the best target for cyber squatters

Legend:

Income of the respondent and social media is the best target for cyber squatters

Figure 13

Figure 13



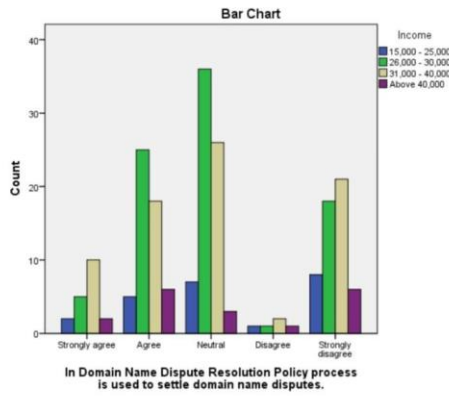
Legend:

Income of the respondent and best remedy available for cyber squatting under trademark law.

Legend:

Income of the respondent and best remedy available for cyber squatting under trademark law. Figure 14:

Figure 14:



Legend:

Income of the respondent and domain name dispute resolution policy process is used to settle domain name disputes

Legend:

Income of the respondent and domain name dispute resolution policy process is used to settle domain name disputes

Figure 15:

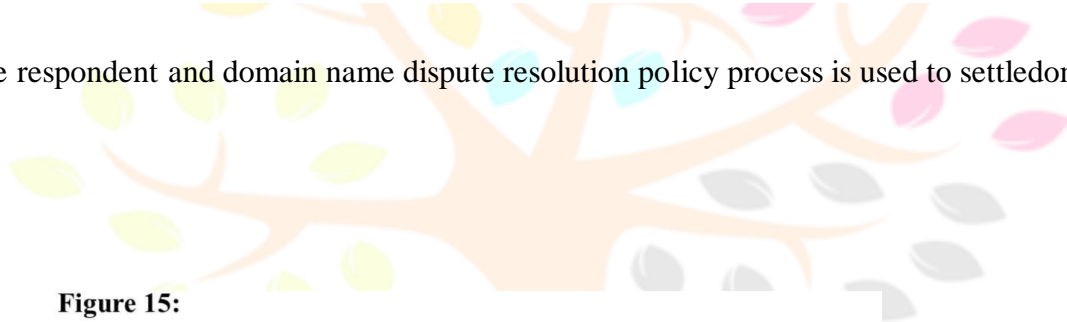
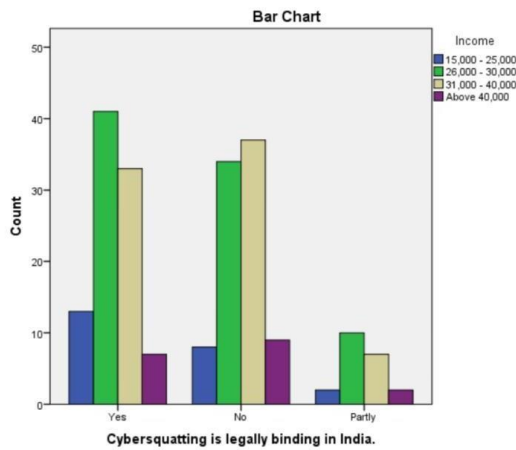


Figure 15:



Legend:

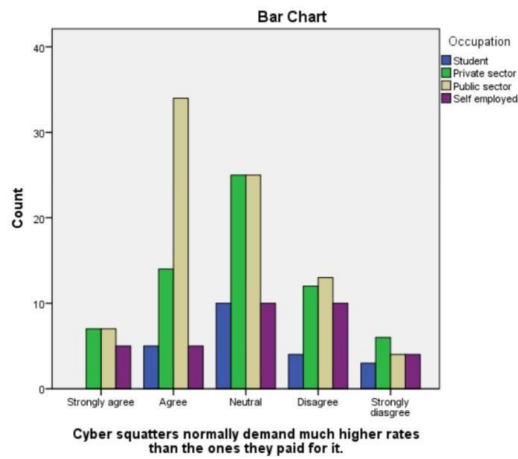
Income of the respondent and cyber squatting is legally binding in India.

Legend:

Income of the respondent and cyber squatting is legally binding in India. Figure 16:



Figure 16:



Legend:

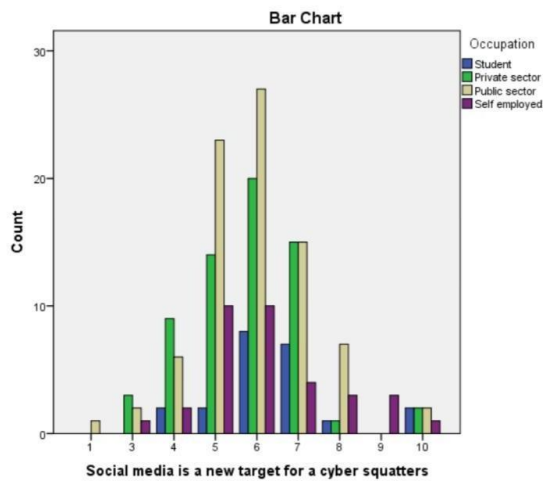
Occupation of the respondent and higher rates of demand by cyber squatters than the ones they paid for

Legend:

Occupation of the respondent and higher rates of demand by cyber squatters than the ones they paid for

Figure 17:

Figure 17:



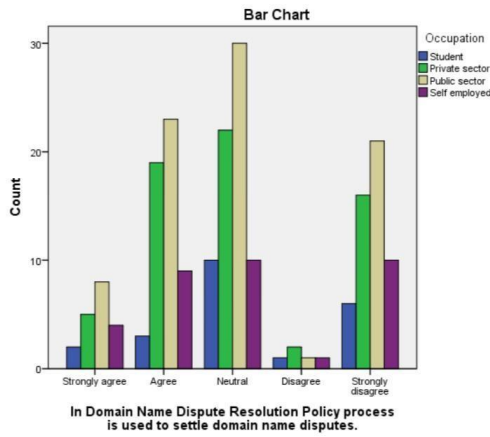
Legend:

Occupation of the respondent and social media is the best target for cyber squatters

Legend:

Occupation of the respondent and social media is the best target for cyber squatters

Figure 19



Legend:

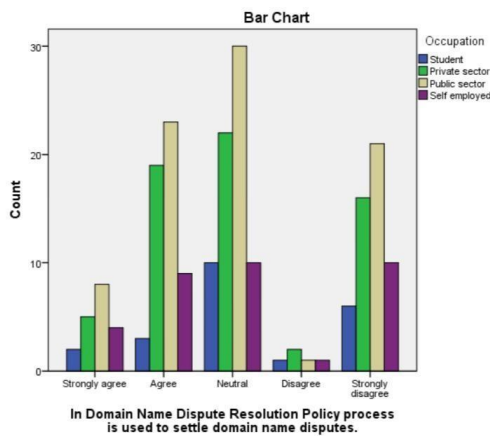
Occupation of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Legend:

Occupation of the respondent and best remedy available for cyber squatting under trademarklaw.

Figure 19

Figure 19



Legend:

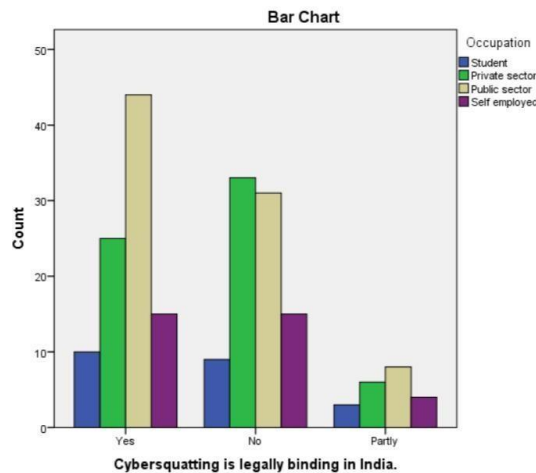
Occupation of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Legend:

Occupation of the respondent and domain name dispute resolution policy process is used to settle domain name disputes.

Figure 20:

Figure 20:



Legend:

Occupation of the respondent and cyber squatting is legally binding in India.

Legend:

Occupation of the respondent and cyber squatting is legally binding in India.

RESULT:

Figure 1 represents that the maximum option is chosen for neutral by the age group between 36-40. Figure 2 represents that the maximum chosen scale was 6 and it was opted by the respondents of age group between 36-40. Figure 3 represents that the maximum choose option was it can send a cease and desist notice to the cyber squatter between the age group of 26-35 years. Figure 4 represents that the maximum chosen option was neutral and opted maximum by the respondents between the age of 26-35. Figure 5 represents that the maximum chosen option was yes and opted maximum by the respondents whose age is between 26-35. Figure 6 represents that the maximum option is chosen for neutral by the female respondents. Figure 7 represents that the maximum chosen scale was 6 and it was opted by the female respondents. Figure 8 represents that the maximum choice option was it can send a cease and desist notice to the cyber squatter by female respondents. Figure 9 represents that the maximum chosen option was neutral and opted maximum by the female respondents. Figure 10 represents that the maximum chosen option was yes and opted maximum by the female respondents. Figure 11 represents that the maximum option is chosen for neutral by the respondents whose income is between 26,000-30,000. Figure 12 represents that the maximum

chosen scale was 6 and it was opted by the respondents whose income is 26,000-30,000. Figure 13 represents that the maximum choice option was it can send a cease and desist notice to the cyber squatter by respondents whose income is between 26,000- 30,000. Figure 14 represents that the maximum chosen option was neutral and opted maximum by the respondents whose income is 26,000-30,000. Figure 15 represents that the maximum chosen option was yes and opted maximum by the respondents whose income was between 26,000-30,000. Figure 16 represents that the maximum option is chosen for neutral by the respondents whose occupation is public sector. Figure 17 represents that the maximum chosen scale was 6 and it was opted by the respondents whose occupation is Public sector

. Figure 18 represents that the maximum choice option was it can send a cease and desist notice to the cyber squatter by respondents whose occupation is public sector. Figure 19 represents that the maximum chosen option was neutral and opted maximum by the respondents whose occupation is public sector. Figure 20 represents that the maximum chosen option was yes and opted maximum by the respondents whose occupation is public sector.

DISCUSSION:

Figure 1 represents that the maximum option is chosen for neutral by the age group between 36-40 because respondents awareness on the particular raised question was lesser therefore it was not easy to decide either it as a agree or disagree. Figure 2 represents that the maximum chosen scale was 6 and it was opted by the respondents of age group between 36-40 because respondents think that the new target for cyber squatters is average range and not too high or low. Figure 3 represents that the maximum choose option was it can send a cease and desist notice notice to the cyber squatter between the age group of 26-35 years because respondents think that among the 3 options the most best choice is to cease and desist. Figure 4 represents that the maximum chosen option was neutral and opted maximum by the respondents between the age of 26-35 because respondents think that the awareness of respondents is not that clear on the raised question. Figure 5 represents that the maximum chosen option was yes and opted maximum by the respondents age is between 26-35 because respondents think that the awareness of respondents are clear on the raised question. Figure 6 represents that the maximum option is chosen for neutral by the female respondents because respondents' awareness on the particular raised question was lesser therefore it was not easy to decide either it as a agree or disagree. Figure 7 represents that the maximum chosen scale was 6 and it was opted by the female respondents because respondents think that the new target for cyber squatters is average range and not too high or low. Figure 8 represents that the maximum choice option was to send a cease and desist n.otice to the cyber squatter by female respondents because respondents think that among the 3 options the most best choice is to cease and desist. Figure 9 represents that the maximum chosen option was neutral and opted maximum by the female respondents because respondents think that the awareness of respondents is not that clear on the raised question. Figure 10 represents that the maximum chosen option was yes and opted maximum by the female respondents because respondents think that the awareness of respondents are clear on the raised question. Figure 11 represents that the maximum option is chosen for neutral by the respondents whose income is between 26,000-30,000 because respondents' awareness on the particular raised question was less,

therefore it was not easy to decide either it as an agree or disagree. Figure 12 represents that the maximum chosen scale was 6 and it was opted by the respondents whose income is 26,000-30,000 because respondents think that the new target for cyber squatters is average range and not too high or low. Figure 13 represents that the maximum choice option was to send a cease and desist notice to the cyber squatter by respondents whose income is between 26,000- 30,000 because respondents think that among the 3 options the best choice is to cease and desist. Figure 14 represents that the maximum chosen option was neutral and opted maximum by the female respondents whose income is 26,000-30,000 because respondents think that the awareness of respondents is not that clear on the raised question. Figure 15 represents that the maximum chosen option was yes and opted maximum by the female respondents whose income was between 26,000-30,000 because respondents think that the awareness of respondents are clear on the raised question. Figure 16 represents that the maximum option is chosen for neutral by the respondents whose occupation is public sector because respondents awareness on the particular raised question was lesser therefore it was not easy to decide either it as a agree or disagree. Figure 17 represents that the maximum chosen scale was 6 and it was opted by the respondents whose occupation is Public sector because respondents think that the new target for cyber squatters is average range and not too high or low. Figure 18 represents that the maximum choice option was to send a cease and desist notice to the cyber squatter by respondents whose occupation is public sector because respondents think that among the 3 options the most best choice is to cease and desist. Figure 19 represents that the maximum chosen option was neutral and opted maximum by the female respondents whose occupation is public sector because respondents think that the awareness of respondents is not that clear on the raised question. Figure 20 represents that the maximum chosen option was yes and opted maximum by the female respondents whose occupation is public sector because respondents think that the awareness of respondents are clear on the raised question.

CONCLUSION:

The domain of Cyber Law in India is yet to expand as compared to western countries. So, in India it is a fact is that there is no exclusive law which makes the cybersquatting illegal and prevents the unethical practice of obtaining the registration of domain names and their owning by the cybersquatters in greed of money. The only way by which domain names can be protected in India is through their registration as Trade Marks. But obtaining the registration of a Trade Mark is not an easy task. They are certain complex conditions as explained in earlier sections which require to be fulfilled in order to obtain the registration of Trade Marks. Sometimes unregistered marks too can be protected can be protected by way of passing off but it all depends upon the fulfilment of specific conditions as explained. The other ways by which disputes and conflicts of domain names is resolved are by following UDRP which has been adopted by ICANN. Here, the disputes and conflicts of domain names are resolved and judgement is given through practice of arbitration facilitated by service providers of dispute resolution, like WIPO. Since India is not a follower of UDRP, so the disputes of domain names having extension '.in' are resolved only through the .IN Domain Name Dispute Resolution Policy (.INDRP) which has been adopted by National Internet

Exchange of India (NIXI). The grounds of complain, process of resolution and the remedies available, all are almost same as that of under UDRP.

REFERENCES:

1. Alok, Kumar. 2010. Squatting with Dignity: Lessons from India. SAGE Publishing India.
2. Clemson, Andrew. 2019. A Practical Guide to the Law of Domain Names and Cybersquatting.
3. Dasgupta, M. 2009. Cyber Crime in India: A Comparative Study.

4. Davidson, Alan. 2009. *The Law of Electronic Commerce*. Cambridge University Press.
5. Dewani, Nisha Dhanraj, Zubair Ahmed Khan, Aarushi Agarwal, Mamta Sharma, and Shaharyar Asaf Khan. 2022. *Handbook of Research on Cyber Law, Data Protection, and Privacy*. IGI Global.
6. Elias, Stephen, and Patricia Gima. 2001. *Domain Names: How to Choose & Protect a Great Name for Your Website*. NOLO.
7. Fishman, Stephen. 2022. *Trademark: Legal Care for Your Business & Product Name*. Nolo.
8. Levine, Gerald M. 2015. *Domain Name Arbitration: A Practical Guide to Asserting and Defending Claims of Cybersquatting*.
9. Lindsay, David. 2007. *International Domain Name Law: ICANN and the UDRP*. Bloomsbury Publishing.
10. Mambi, Adam J. 2010. *ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community*. African Books Collective.
11. Neupane, Pallavi. 2019. *An Overview of Cyber-Crimes and Cyber Law in India and Nepal: A Comparative Study on ETA Act 2063 of Nepal and IT Act 200 of India*. GRIN Verlag.
12. Rockman, Howard B. 2004. *Intellectual Property Law for Engineers and Scientists*. John Wiley & Sons.
13. Ryder, Rodney D., and Ashwin Madhavan. 2014. *Intellectual Property and Business: The Power of Intangible Assets*. SAGE Publishing India.
14. Sharma, Vakul. 2011. *Information Technology Law and Practice*. Universal Law Publishing.
15. Thomas McCarthy, J. 1996. *McCarthy on Trademarks and Unfair Competition*. Clark Boardman Callaghan.
16. *Trade-Mark Practice in Canada*. 2011. Borden Ladner Gervais LLP.
17. United States. Congress. House. Committee on the Judiciary. 1999. *Trademark Cyberpiracy Prevention Act: Report (to Accompany H.R. 3028)*.
18. Wolfe, Jennifer C., and Anne H. Chasser. 2012. *Domain Names Rewired: Strategies for Brand Protection in the Next Generation of the Internet*. John Wiley & Sons.
19. World Intellectual Property Organization. 2002. *Intellectual Property on the Internet: A Survey of Issues*. WIPO.
20. ———. 2004. *WIPO Guide on the Licensing of Copyright and Related Rights*. WIPO.

