EMERGING TRENDS OF VIOLATION OF TRADEMARK AND PROTECTIVE MEASURES IN CYBERSPACE: A CRITICAL STUDY

'Dissertation submitted in partial fulfilment of the requirement for the award of the degree of'

LL.M.

Submitted by:

TANISHA SINHA

ENROLMENT NO.- 23102070019

Supervised by:

Dr. SONIKA

ASSISTANT PROFESSOR OF LAW

SCHOOL OF LAW

GALGOTIAS UNIVERSITY

GREATER NOIDA

(2023-2024)

DECLARATION

I, hereby declare that the dissertation entitled 'EMERGING TRENDS OF VIOLATION OF TRADEMARK AND PROTECTIVE MEASURES IN CYBERSPACE: A CRITICAL STUDY' is based on original research undertaken by me and it has not been submitted in partially or fully or otherwise in any University for any degree or diploma.

Place: Greater Noida

Date:

Signature of the student

Tanisha Sinha

23102070019

CERTIFICATE

This is to certify that the dissertation entitled 'EMERGING TRENDS OF VIOLATION OF TRADEMARK AND PROTECTIVE MEASURES IN CYBERSPACE: A CRITICAL STUDY' has been prepared by Tanisha Sinha, pursuing LL.M from School of Law, Galgotias University under my supervision and guidance. I recommend it for evaluation.

Place: Dr. Sonika

Date: Assistant Professor

ACKNOWLEDGEMENT

I thank Almighty for His countless blessings. This dissertation is the result of the pertinent efforts and contributions of many people around me. I have taken sincere efforts to complete the dissertation, enjoying most of the research works, finding clueless amidst and finally relieved, proud and content to complete it. First, I would like to thank, Dr. Sonika, for her guidance and support. I have been going through a hard phase, if it was not for her kindness, patience and encouragement, the dissertation would have remained incomplete. I am deeply indebted for the consistent efforts Ma'am has taken for widening my perception and improving my work.

Words fall short to express my love and gratitude to my parents, friends and family members for sticking through my side all the way. I feel blessed to have this circle of well-wishers who have always known ways to keep my spirits high.

TANISHA SINHA

LIST OF ABBREVIATIONS

AC	Appellate Cases
ACPA	Anti-cybersquatting Consumer Protection Act
AIR	All India Reporter
CCTLD	country code top-level domain
CJEU	Court of Justice of the European Union's
CTM	Community trademark
DNS	Domain Name System
EC	European Council
EU	European Union
FTDA	Federal Trademark Dilution Act
HTTP	Hypertext Transfer Protocol
HTML	Hypertext Markup Language
INDRP	Indian Domain Name Dispute Resolution Policy
IANA	The Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Number
IPC	Indian Penal Code
NIXI	National Internet Exchange of India
OECD	Organisation for Economic Co-operation and Development
PPC	Pay Per Click
SERP	Search engine results pages
SLD	Second Level Domain
TLD	Top Level Domain
TRIPS	Trade Related Aspects of Intellectual Property Rights
UDRP	Uniform Dispute Resolution Policy
W3C	World Wide Web Consortium
www	World wide Web
WIPO	World Intellectual Property Organization

LIST OF CASES

Other Authorities

TABLE OF CONTENT

CHAPTER–1: INTRODUCTION

1.1 INTRODUCTORY

The internet has gained many synonyms, the virtual world that facilitates communication over computer networks is known by various names, such as Cyberspace, Cyberia, the Web, the Net, the Matrix, and so on. The virtual world of cyberspace is a consensus reality devoid of the traditional physical underpinnings of the actual world. Cyberspace transactions do, however, occur in the real world and have real-world

consequences, Cyberspace can be thought of as a conceptual collage where all of the world's information sources are harmoniously integrated.

All objects observed in cyberspace, whether they are representations of actual objects or not, are composed of data that is entirely informational. Cyberspace is made up of information, much like the legal profession is made up of cases.

Every computer added to the Internet was given a unique identifier, often known as an IP address or Internet Protocol number. By entering the IP address of the other computer, information from one computer could be transmitted to another. The data will be divided into many packets, each of which will have an IP address that may be used to locate the intended computer. This allowed the different computers connected to the Internet, the network of networks, to share a wide range of information. Among Internet communication platforms, the most well-known is the World Wide Web (WWW or Web). Hypertext Transfer Protocol (HTTP) is a specific protocol that allows users to search and retrieve content from the Web, which is a network of websites[1].

Modern technology has made it possible for nations to build and broaden their communication networks, facilitating quicker and simpler networking and information exchange. As a result, the corporate sector needs to transition to this new era as conventional business is evolving into e-business, with old platforms giving way to online ones for marketing, sales, and advertising. In which cyberspace is the new reality, a parallel universe generated and maintained by computers and communication links, according to Michael Benedikt in his book Cyberspace[2].

The age of information technology has strengthened our law enforcement system and led to the emergence of e-courts in India where cases are filed and heard electronically. So, we see that information technology has influenced all areas of human life. The phenomenal development of the Internet as a commercial medium has created new challenges in the field of intellectual property[3]. The development of e-commerce, brands are still essential for gaining a competitive edge in an increasingly globalized market. To get recognition for their abilities to create value, brands rely on their symbolic power to attract attention, With the spread of email and the World Wide Web, an unanticipated brawl over Internet addresses has broken out in the trademark sphere. The issue is of two versions, first trademark owners who want to use their brands as domain names have discovered that the preferred version of these names is already taken. On the other hand, trademark holders have discovered that unapproved parties are utilizing their marks as domain names, frequently intending to profit from the goodwill of the mark's proprietor[4].

Technically it is possible to assign multiple domain names to a website[5], Multiple domain names can point to the same website. Using multiple domain names for a single website can increase the number of

[1] Fortinet, https://www.fortinet.com/resources/cyberglossary/what-is-ip-address, (last accessed on Feb. 20, 2024).
[2] MICHAEL BENEDIKT, CYBERSPACE (The MIT Press 1992).
[3] Id at 1.
[4] Kenneth Sutherlin Dueker, *Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses*, 9 Harv. J. L. and Tech. 483 (1996).
[5] Washington Speakers Bureau, Inc. v. Leading Authorities, Inc., 33 F. Supp. 2d 488,491- 92 (E.D. Va. 1999).

potential visits to a company's website by increasing the likelihood that someone searching for a company will enter the domain name that points to the company's website. Generally, the World Wide Web and other forms of Internet communications in current technology rely on the use of domain names to locate specific computers and networks on the Internet[6].

In addition to the domain name there are other trademark problems in cyberspace which include Linking and Framing which is used to violate the rights of other website owners, including deep links, frames, and other visuals on your website. For example, deep linking enables users to navigate straight to an internal page from the home page, avoiding the content and ads there. Although there isn't a legislation addressing linking concerns, for example, the *Svensson case*[7] established that hyperlinking to publicly available works does not amount to trademark infringement.

In the *GS Media Case*[8], the CJEU further concluded that an act that would violate an author's rights would be the making of a work freely available without the author's consent and providing links to the work in order to pursue financial advantage.

Since linked to websites frequently rely on the volume of visitors that arrive through their home page, they may experience a decline in revenue of the company. It could give users the false impression that the two linked websites support one another[9], framing is a method that lets a user see a website's content while it's framed by content from another website. According to trademark law, framing can lead to a dispute since a framed site may change the way the content appears and give the impression that its owner approves of the framer or voluntarily chooses to interact with them[10].

The most frequent problem with domain names is 'cybersquatting'. 'Cybersquatting' is defined as the registration, trafficking, or use of a domain name with the malicious aim of making money from the goodwill of another person's brand. Cyber squatters most frequently block the domain names of well-known brands that are protected by trademarks to trade them for millions of dollars from the trademark owners. Owing to limitations in technology, stylistic characters or spaces are not permitted in domain names[11]. This has a big impact on how courts evaluate matters involving trademarks.

A closely related term to 'cybersquatting' is 'typo-squatting', in which a person registers a domain name that is a variation of a well-known brand. In the Rediff case[12], the respondents registered radiff.com, a domain name that was identical to the plaintiff's rediff.com, the court decided in the plaintiff's favour and acknowledged the domain name as trademark protection.

---

[6] Id.
[7] Svensson v. Sverige C-466/12 (2014).
[8] GS Media BV v .Sanoma Media Netherlands BV and Others C-160/15 (2016).
[9] Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc, 75 F. Supp. 2d 1290 (D. Utah 1999).
[10] Futuredontics Inc. v. Applied Anagramic Inc., 1997 46 USPQ 2d 2005 (C.D. Calif. 1997).
[11] Fortinet, https://www.fortinet.com/resources/cyberglossary/cybersquatting (last accessed on 1 May 2024).
[12] Rediff Communication Limited v. Cyberbooth and another (AIR 2000 Born 27).

Top Level Domain (TLD) squatting and gripe sites also amount to trademark infringement on the Internet. Briefly, TLD-squatting refers to top-level domain name squatting. For instance, www.yahoosucks.com would be a gripe site for www.yahoo.com[13].

Another significant issue for the owners of trademarks is Meta-Tagging. In short, 'Meta' refers to a tag in HTML, which is the foundation of the World Wide Web. The words, keywords, and web page content are all contained in the Meta-Tag. Trademark breaches result from overzealous web designers manipulating Meta tags. In reality, Meta Tags play a major role in how search engines, such as Google and Yahoo, perform searches. The owners of the websites often use modified Meta tags in an attempt to maximize the number of hits on their pages[14]. The browsing habits also contribute to the increase in trademark infringements in cyberspace. Many users try to derive a domain name based on a company and its brand or business name and enter the brand into the browser, hoping to connect directly to the company and website pages. Alternatively, if users cannot derive the correct domain name, they rely on search engines to search for keywords or phrases related to the desired site.

The World Trade Organisation (WTO) recognised intellectual property rights in connection with trade with the TRIPS agreement. As a formal agreement between the WTO member states, the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Accord was developed. The agreement became operative on January 1st, 1995. Regarding intellectual property rights, the agreement is seen as a historic and comprehensive one. Trademarks are covered in Section-15 of the Trademark Act, 1999[15], which also establishes directory information for their protection. India ratifies the TRIPS agreement. India's trademark laws are governed by the Trade Marks Act, 1999 wherein Section-2(1) (zb) of the Act defines 'trademark'[16].

Trade and business have become more globalised, allowing goods and services to be accessible outside of specific borders or legal jurisdictions. It is found to be cross-border. This situation has been made worse by the COVID-19 pandemic and the growing reliance on e-commerce platforms for the acquisition of goods and services. Illegal activity on the Internet has global consequences and confusion regarding the territorial jurisdiction of the crime cause the parties tend to the exchange without coming into contact with one another physically. The ability to browse the options without time or restriction, compare prices of various products, and make their decision to buy a thing only after fully satisfying themselves have made the internet a favoured alternative for customers. Even if the territorial issue is resolved, the political problem is to seek the arrest of the accused if he is a citizen of another country. National and international courts have

---

[13] Whitney C. Gibson, *New '.sucks' domain name gives rise to extortion claims, future online reputation attacks,* LEXOLOGY, (May, 22, 2015), https://www.lexology.com/library/detail.aspx?g=78893456-c62c-4f0a-b9ae-73b32ffda09c.

[14] Llewelyn, David and Reddy, Prashant, Metatags Using Third Party Trade Marks on the Internet, https://ssrn.com/abstract=3683824 (Last accessed on May 1, 2024).

[15] Trade marks Act 1999, Sec 15.

[16] Trade Marks Act, 1999, (Act No. 47 of 1999) Sec-2(1)(zb): mark capable of being represented graphically and which is capable of distinguishing the good and service of one person from those of others and may include the shape of goods, their packaging, and combination of colours.

developed various principles and rules to effectively determine jurisdiction over cybercrime[17]. However, due to the complexity of cyberspace, it is very difficult to accept and adopt a uniform rule in global law.

According to Section-28 of the Trade Marks Act, 1999[18], a person or business shall be held liable for trademark infringement if it causes consumers to believe that a trademark that has been registered in the territory or in India by another proprietor or individual is deceptive or confusing.

Section-27 of The Trade Marks Act, 1999 deals with Passing Off action[19]: It is founded on the idea that a person should not sell his goods with the representation that they belong to someone else. A trader who has previously used a trademark has to be shielded from those who might unfairly benefit from the goodwill he has built by registering the mark before him. It makes no difference in a passing-off action whether the deception comes from an unregistered or registered owner of a trademark[20]. Therefore, owners who are not registered in India may pursue the remedies provided by Section-27 of trademark Act, 1999 to stop others from profiting off of their reputation.

One of the major problems with the domain name system is cybersquatting, which is the intentional and fraudulent registration of domain names containing well-known trademarks with the intention of selling them to the owners of such trademarks at a high price. By selling these domain names to anyone else, cyber squatters may be able to make money while 'diluting' a well-known brand or trade name[21].

The Information Technology Act was passed into law nationally in 2000. The subject of intellectual property breaches in cyberspace remained unaddressed, even following changes to the Act in 2008. But the void is being slowly filled by a slew of non-judicial measures such as the adoption of the Internet Domain Name Dispute Resolution Policy (INDRP) and the legal method of applying the Trade Marks Act, 1999 and Common Law protection against passing-off of goods and services to domain name disputes on the Internet. The resentful party may file a lawsuit in court regardless of the disputed domain names TLD, even though the INDRP is an administrative-level arbitration procedure created specifically to handle domain name disputes for Country Code Top Level Domain (ccTLD).

The US government established the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. ICANN is a separate entity that oversees the coordination of IP addresses, autonomous system numbers, and domain names for the global Domain Name System. The Uniform Dispute Resolution Policy (UDRP), which was adopted by the ICANN, has been used as a benchmark for handling complaints pertaining to e-commerce. The UDRP offers guidelines for settling disputes between third parties claiming an interest in registered domain names and registered holders of those names. There are problems with this policy on its own. First of all, since it's not a law, the countries cannot be required to use this particular

[17] Mr. Atul Satwa Jaybhaye, *Cyber Law and Ipr Issues: The Indian Perspective,* BLR 166, 185 (2016).

[18] Trade Marks Act, 1999, S.28: Subject to the other provisions of this Act, the registration of a trade mark shall, if valid, give to the registered proprietor of the trade mark the exclusive right to the use of the trade mark in relation to the goods or services in respect of which the trade mark is registered and to obtain relief in respect of infringement of the trade mark in the manner provided by this Act.

[19] Trade Marks Act, 1999, S.27: No person shall be entitled to institute any proceeding to prevent, or to recover damages for, the infringement of an unregistered trade mark.

[20] N.R. Dongre And Ors v. Whirlpool Corporation And Anr, (1996) 16 P.T.C. 476 Del (DB).

[21] Stephen Koenig v. Arbitrator, National Internet Exchange of India 2012(49) PTC304(Del).

conflict resolution method. In addition, the decisions made by the arbitral bodies under the UDRP are not final, which means they do not establish a precedent, and the parties to the arbitration may file a new complaint in any other court with jurisdiction. As a result, the main objective of the UDRP, which was to provide time-bound dispute resolution, has been achieved[22].

The swift development of Internet technology and the exponential expansion of cyberspace have given rise to a range of new trademark rights concerns that will significantly affect how trademark law is applied on the Internet. The topics cover a wide spectrum, from Internet-specific problems to more conventional cases of trademark infringement. There isn't a broad agreement between domain name registrars, trademark owners, Internet users, ICANN, and judges on how to handle these unforeseen challenges. Undoubtedly, companies need to feel secure that their trademarks will be safeguarded if they want the Internet to serve as a productive commercial marketplace. However, the demands of the Internet community as a whole, not only trademark owners, must be met by Internet management. Therefore, the legal community will need to adapt to an environment where old boundaries are disintegrating, even while the extent and direction of the consequences caused by the Internet remain unpredictable[23].

Almost all of the main nations have responded to the ongoing issues brought by volatile technology after realizing how urgent it is to govern the Internet. While the others are in the midst of doing the same, some of them have passed explicit new cyber laws or changed the current laws to make them cyber-compliant. In general, there are three different Meta-visions of how the Internet and law interact:

(i) the Internet as a separate jurisdiction (theoretical vision);

(ii) the Internet as a no-law Internet (utopian vision); and

(iii) Internet law as translation (practical project).

Cyberspace is seen as a domain that challenges the traditional application of trademark laws as a regulatory tool. In the realm of the internet, existing trademark regulations that uphold conventional agendas may not be directly applicable. However, an alternate perspective suggests that some form of laws or guidelines are necessary and appropriate for governing trademarks in the online space. While cyberspace may require its own distinct jurisdiction, the very technological features that make it resistant to traditional laws also create circumstances where new legal frameworks are needed. Translating 'internet trademark law' would involve utilizing legal instruments to achieve balanced protection of trademark interests on the internet, similar to the physical world.

In essence, this research highlights the tension between the perceived immunity of cyberspace from traditional trademark laws and the need for developing new legal mechanisms to address trademark issues in the online environment. It recognizes the challenges posed by the unique nature of cyberspace while

[22] Draft rules for Uniform Domain Name Dispute Resolution Policy, (29 September 1999).

[23] David Yan, *Virtual Reality: Can We Ride Trademark Law to Surf Cyberspace,* 10 Fordham Intel. Prop. Media and Ent. L.J. 773 (2000).

acknowledging the necessity of adapting legal frameworks to maintain a balance of interests regarding trademarks on the internet.[24].

1.2 STATEMENT OF PROBLEM

Despite all of the benefits the Internet has brought to the intellectual property sector, it has also brought about a frightening array of drawbacks. The laws governing trademark protection are constantly changing, both globally and specifically in India. This is particularly true concerning arbitration procedures and territorial jurisdiction. Therefore, the laws must be appropriately amended to ensure the protection of trademarks in cyberspace. This will allow for the prevention of trademark infringement in cyberspace as well as the resolution of trademark infringement disputes through compensation to the victims of infringement and the punishment of those found guilty.

Trademark infringement can have significant effects on e-commerce sites. Various e-commerce platforms may be held liable for trademark infringement if they facilitate the sale of counterfeit or unauthorized goods, exposing them to legal action from trademark owners. This can result in economic damages and reputation loss for the trademark owners. The prevalence of counterfeit goods in e-commerce can undermine the reliability of brands, damage consumer confidence, and cost legitimate IP owners a substantial amount of money. The enforcement of trademark infringement in e-commerce poses new challenges, as it can be difficult to locate the source of infringing goods, and sellers need to ensure the authenticity of the goods they sell. In the e-commerce domain, trademark infringement can take various forms, such as difficulty in locating the source of infringing goods.

Due to the global nature of e-commerce and the ability for sellers to operate anonymously or from remote locations, it can be challenging for trademark owners to identify and locate the source of counterfeit or infringing goods. Ensuring the authenticity of goods sold as E-commerce platforms and sellers need to implement measures to verify the authenticity of the products they sell, as counterfeit goods bearing infringing trademarks can easily be listed and sold online.

1.3 REVIEW OF LITERATURE

1. **(Kenneth Sutherlin Dueker)[25]:** Dueker studied how the then-emerging Internet technology affected trademark protection in cyberspace. Following a brief historical overview of the evolution of trademark laws and regulations in the United States, particularly the Federal Trademark Dilution Act

[24] Justin Hughes, The Internet and The Persistence of Law, 44 B.C.L. Rev. 359 (2003).
[25] Supra note 24 at 8.

of 1995 and the Lanham Act of 1946, Dueker examined the definitions of trademark dilution and violation under these laws, "*If a company uses another party's trademark or service mark as part of its corporate title and name, that company may be liable for trademark infringement"*[26]. Dueker places a strong focus on the examination of domain names as the sole cause of trademark infringement in cyberspace. Domain name conflicts unquestionably compose the majority of the case-law jurisprudence that has developed over time and serve as the foundation for several non-judicial arbitration-based dispute resolution processes. However, when it comes to trademark infringement in cyberspace, domain names are not the end-all-be-all. Trademark infringement on the Internet is exacerbated by a few other elements as well, such as pop-ups, frames, hyperlinks, Meta tags, and Search Engine ads.

The statement provides a brief historical overview of trademark laws and regulations in the United States, specifically mentioning the Federal Trademark Dilution Act of 1995 and the Lanham Act of 1946. This context helps understand the legal framework within which trademark issues in cyberspace are examined. The author, Dueker, places a strong emphasis on examining domain names as the sole cause of trademark infringement in cyberspace. This narrow focus on domain names is identified as a potential loophole or limitation in addressing trademark issues in the online realm. The recognition that trademark infringement on the internet is exacerbated by elements beyond just domain names suggests that existing laws and regulations may not adequately account for these factors. This insight can help policymakers, legal professionals, and stakeholders explore ways to close these loopholes and develop more comprehensive legal frameworks or guidelines to address trademark infringement in cyberspace effectively.

2. **(David Yan)[27]:** Yan conducted an in-depth review of several issues pertaining to online trademark infringement. Yan goes into length on a number of substantial topics, including as framing, keying, linkages, cybersquatting, reverse hijacking, Meta tags, typo-sites, spam, and faked spamming. Yan also covered the procedural rules defining internet jurisdiction, as established and used by US courts in various contexts. However, Yan submitted that the collective weight of case law shows that trademark law remains a foundation and serves as a last resort to resolve disputes in cyberspace. Courts, however, need to consider policy implications because the Internet is a new medium of communication that forces trademark law to evolve. In the actual world, the same names or marks may coexist under trademark registration in several product and/or service categories and in several legal countries. Nonetheless, the Internet offers a singular situation in which two identical domain names cannot coexist. For example, there can only be a single microsoft.com domain name, which is universally accessible from any location in the globe as long as the device being used to view the

[26] Id.
[27] Supra note 13 at 5.

website has an active Internet connection. Yan further observed that in the Internet age, technology advances significantly within months, rather than years, and even Moore's Law[28] seems outdated. Consequently, legal decisions will not be viable without balancing policy implications.

By acknowledging the diverse forms of online trademark infringement, jurisdictional challenges, the unique nature of the internet, and the rapid pace of technological change, Yan's statement helps identify potential loopholes or limitations in using existing trademark laws and frameworks to effectively address trademark violations in cyberspace. These insights can guide efforts to adapt and develop more robust legal mechanisms tailored to the online environment, while considering the policy implications and balancing the interests of stakeholders.

3. **(Prof. Michael Geist)[29]:** Professor Geist researches the jurisdictional issues courts encounter when resolving disputes via the Internet. The chance that a website owner may be called before a court in a distant jurisdiction is more than just a theoretical thought since websites are accessible from anywhere in the globe. Consumers anxious to purchase online must also balance the promise of unlimited choice, greater access to information, and a more competitive, global marketplace with the prospect that they will not benefit from the security normally afforded by local consumer protection laws. Although such laws exist online just as they do offline, their effectiveness is severely undermined if consumers do not have recourse to their local court system or if enforcing a judgment requires further proceeding in another jurisdiction. The most difficult hurdle for the courts to overcome in any case involving an online trademark infringement is, in reality, jurisdiction. Because of the Internet's global character by design, obtaining respondent custody in a trademark dispute involving parties who live in separate nations may include political factors rather than just judicial ones. In the absence of international political agreement among the nations to cooperate in such judicial affairs, it is extremely difficult to get the respondent's actual attendance in court hearings in other nations.

   By highlighting the global accessibility of websites, consumer protection concerns, jurisdictional hurdles, and the need for international cooperation, Geist's statement exposes several potential loopholes or limitations in addressing online trademark infringement effectively. These loopholes stem from the borderless nature of the internet, which challenges traditional notions of jurisdiction and enforcement mechanisms.

   To address these loopholes, Geist's analysis suggests the need for international cooperation and agreements among nations to establish clear jurisdictional rules and enforcement mechanisms for resolving online trademark disputes. Additionally, it highlights the importance of adapting consumer

[28] John Markoff, A Renaissance in Computer Science: Chip Designers Search for Life After Silicon, N.Y. TIMES, July 19, 1999.
[29] Prof. Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L.J. 1345 (2001).

protection laws and legal frameworks to account for the unique challenges posed by the digital environment.

4. **(Ashwani Kumar Bansal)[30]:** It is a comprehensive work on trademark-related topics. An overview of the foundations of the Indian trademark system is provided in this book. The book's opening chapter discusses the idea of intellectual property and its various applications in the modern world. There are thirty-two chapters in the book that describe trademarks and the Trademark Act of 1999. The several authorities established by the Act; reasons for registration and refusal to register; passing off and infringement; judicial jurisdiction; and the offences and sanctions specified by the Act. The book's appendices provide a list of all pertinent domestic and international statutes as well as signed international trademark treaties.

   While the statement itself does not directly highlight loopholes, the lack of explicit coverage or detailed analysis of trademark issues specific to cyberspace could be considered a potential limitation. As the digital landscape continues to evolve, addressing trademark violations in the online environment may require a more comprehensive understanding of the unique challenges, jurisdictional complexities, and the need for international cooperation and harmonization of laws.

5. **(Thomson West)[31]:** It provides a definitive discussion of Internet legal issues and developments. It discusses the development of legislation and jurisprudence. The book contains various articles by different authors on different issues of the internet and law ranging from Anti cybersquatting, Consumer Protection Act to online liabilities. The book consists of five parts. The first part of the book contains a brief history of the Internet. The second part deals with many areas of online business such as taxation, advertising, antitrust, etc. The third part deals with legal issues such as jurisdictional issues, electronic information, and the application process. The fourth Section deals with Internet issues related to intellectual property rights, such as copyright issues, trademark infringement, and unfair competition, anti-cyber occupation law, Dilution Law of 1995, ICANN dispute resolution rules, patent law, trade secrets, etc. Section-5 deals with certain general legal matters. On the Internet, such as free Internet expression, cybercrime, protection, etc.

   This book addresses the unique challenges posed by the global nature of the internet, cross-border enforcement mechanisms, and the harmonization of laws across different jurisdictions could shed light on potential gaps or areas that require further legal development or international cooperation.

6. **(Sally M. Abel)[32]:** Researcher examines several concerns that impact the safeguarding of trademarks in the online realm and explores the approaches taken by both U.S. and non-U.S. courts to tackle

[30] ASHWANI KUMAR BANSAL, THE LAW OF TRADEMARKS (3rd ed. 2014).
[31] THOMSON WEST, INTERNET LAW AND PRACTICE (18th ed. 2002).
[32] Sally M. Abel, *Trademark Issues in Cyberspace: The Brave New Frontier*, 5 Mich. Telecomm. and Tech. L. Rev. 91 (1999).

these matters. Abel, for alia, finds that users regularly attempt to guess a company's Internet location by typing in the name of the company followed by the ubiquitous .com top level domain. This prevalent practice of guessing at domain names makes an obvious domain name a valuable organisational asset. One thing that clearly arises out of the examination of numerous factors connected to trademark breaches on the Internet by Abel is that technology is the underlying cause of the issue at hand. Without the development of Internet technology, no trademark violation concern would've occurred in cyberspace. As a consequence, without domain names, Internet wouldn't have become as popular as it is. Since bad faith domain name registration is a key source of trademark breaches in cyberspace, any meaningful solution to the problem cannot be reached without the involvement of technology.

By identifying the user behavior of domain name guessing, the underlying role of technology, the challenges posed by bad faith domain name registration, and the need for technological involvement in solutions, Abel's article highlights potential loopholes or limitations in effectively addressing trademark violations in cyberspace using traditional legal frameworks alone.

7. **(Uniform Domain-Name Dispute-Resolution Policy)[33]:** In the generic top level domains (gTLDs) (such as.biz,.com,.info,.mobi,.name,.net, and.org) and those country code top level domains (ccTLDs) that have voluntarily adopted the UDRP Policy, the Uniform Domain Name Dispute Resolution Policy (the UDRP Policy) lays out the legal framework for the resolution of disputes between a domain name registrant and a third party (i.e., a party other than the registrar). The UDRP Policy was approved by the ICANN Board of Directors, mostly based on suggestions made in the WIPO Internet Domain Name Process Report and feedback from registrars and other interested parties. Any individual or organisation that wants to register a domain name in the relevant gTLDs and ccTLDs must agree to the UDRP Policy's terms and conditions.

The Uniform Domain Name Dispute Resolution Policy (UDRP Rules), which outline the protocols and additional requirements for every phase of the administrative dispute resolution process, was approved by the ICANN Board on October 24, 1999. ICANN-accredited dispute resolution service providers oversee the process. One organisation that offers these services for resolving disputes is the WIPO Arbitration and Mediation Centre (WIPO Centre).

While the UDRP Policy aims to establish a legal framework for resolving domain name disputes, the statement highlights potential loopholes or limitations in its scope, compliance mechanisms, dispute resolution process, service provider accreditation, and the scope of remedies available. These limitations may leave room for trademark infringement cases to fall through the cracks or for bad faith actors to exploit loopholes in the system.

33

8. **(Gulafroz Jan)[34]:** Online business and e-commerce are now a part of the contemporary economy. It's important to remember that the internet is the dominant force in this millennium, in addition to the importance of trademarks and their role in modern company. Nowadays, as businesses sell and promote their goods online, they use domain names to make themselves easier to find. In order to succeed, it is now imperative for any commercial business to have a website and an online presence. Because websites require an address in order to be found, domain names were developed for this reason. As long as physical barriers separate the market's channels, two distinct dealers may use the same brand on the same items, according to trademark law. Political boundaries have disappeared in cyberspace, making it challenging for trademark law to take into account the potential of one mark, two owners. In addition to this, a number of other trademark-related problems have emerged and are pending court decisions.

   By highlighting the territoriality principle, domain name conflicts, emerging trademark-related issues, and the lack of specific guidance, the statement by Gulafroz Jan highlights potential loopholes or limitations in applying traditional trademark laws to the online environment. These loopholes stem from the unique characteristics of cyberspace, such as its borderless nature, the importance of domain names, and the emergence of new forms of trademark infringement and challenges.

9. **(D Rowland and E Macdonald)[35]:** The absence of a defined global regulatory framework and the lack of focused legislation to resolve disputes and stop cyber squatters are the most important difficulties surrounding trademark infringement through cybersquatting. The United States has implemented the Anti cybersquatting Act 1999 as a unique law to safeguard consumers and trademark owners against cybersquatters. In addition to encouraging cyber squatters, the lack of a legal framework in some nations, such as India, leads to violations of both private and public rights. Therefore, efforts must be made to pass a particular law to address the emerging branding problem. Any legislation aimed at controlling the domain name system and prohibiting cybersquatting must be careful to avoid two risks. Underregulating is the first. Overregulating is the second. Overregulation will impede the market's flexibility of operation, which is perhaps its strongest quality. This will hinder the growth of electronic commerce and make it easier for businesses to establish themselves in jurisdictions with less stringent regulations.

   By identifying the lack of a global regulatory framework, insufficient legislation, the encouragement of cybersquatting due to legal gaps, the risks of under- and overregulation, and jurisdictional challenges, the statement by Rowland and Macdonald highlights several potential loopholes or

[34] Gulafroz Jan, *Applicability of Trademark Laws to Cyberspace: An Analysis*, IJLMH, 463-498 (2021).
[35] D ROWLAND AND E MACDONALD, INFORMATION TECHNOLOGY, (Cavendish Publishing 2005).

limitations in addressing trademark infringement through cybersquatting and regulating the domain name system effectively.

10. **(H. Brian Holland)[36]:** By its very nature, the Internet breaks the connection between these validating principles and national boundaries. In particular, because of its decentralised architecture, sovereign states with geographical boundaries are deprived of the authority to control online behaviour. Moreover, there is no notification of shifting (and competing) regulatory regimes in a network devoid of geographical identifiers. Territorially-based sovereigns lose the ability to establish legal rights and obligations within the space they seek to regulate in the absence of these validating relationships between geographic limits and that space.

    He criticises their narrow understanding of sovereignty and over-reliance on the connection between physical proximity and territorial implications on a broad scale. Three arguments are made against the validity of enforcement power: first, it exaggerates the difficulty of regulation, confounding cost for ability; second, they overlook the deterrent effect of local enforcement on extraterritorial actors, targeting end users and network components within the territory; and third, they confuse the legitimacy of regulation with a level of nearly perfect enforcement.

    Researcher statement provides valuable insights into the need to re-evaluate traditional notions of sovereignty, jurisdiction, and enforcement in the context of cyberspace. Addressing these loopholes may require a paradigm shift in legal and regulatory approaches, emphasizing the development of new frameworks that align with the unique characteristics of the internet and the global nature of cyberspace.

11. **(Aaron L. Melville)[37]:** The link between the UDRP and the ACPA is examined in this article. It draws attention to some worries about the effects on other countries and the ability of litigants to manipulate the outcome of legal issues involving generic Top-Level Domains. The investigation shows how easy mark owners can have an impact on the national forum, which hears and decides objections to UDRP rulings. Concerns are also expressed in the article about the current legal framework, which permits mark owners to take UDRP cases to US federal courts when foreign marks are at issue and are decided in accordance with US trademark law.

    By highlighting these concerns and potential loopholes, Melville's article draws attention to the need for a more harmonized and balanced approach to addressing trademark infringement and cybersquatting in the domain name system. The identified loopholes suggest that the existing legal framework may require further refinement and international cooperation to ensure fair and consistent

[36] H. Brian Holland, *The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. Marshall J. Computer and Info. L. 1 (2005).

[37] Aaron L. Melville, *New Cybersquatting Law Brings Mixed Reactions from Trademark Owners*, 6 B.U. J. Sci. and Tech. L. 13 (2000).

enforcement of trademark rights across different jurisdictions and to prevent potential manipulations or undue influences in the dispute resolution process.

12. **(Mr. Atul Satwa Jaybhaye)[38]:** The Model Law on Electronic Commerce on International Trade Law was adopted by the General Assembly of the United Nations (UNCITRAL) on January 30, 1997, and this resolution led to the creation of the Information Technology Act of 2000. One of the crimes with the fastest global growth is cybercrime. Although the Act has been successful in laying out the framework for legislation in cyberspace and addressing several urgent issues related to technological misuse, there are also significant gaps that have not been addressed, such as issues with intellectual property. Knowledge or information in any form that has a commercial value is referred to as intellectual property. Intellectual property rights are a combination of ideas, innovations, and creations; examples of these include copyright, patents, trademarks, and designs. Since these are products of the human mind, they are referred to as intellectual property. The Information Technology Act of 2000 makes no mention of intellectual property protection, despite the fact that intellectual property infringement is one of the most difficult issues in the online world. While violations of copyright and domain names do happen online, the Trade Mark Act of 1999 and the Copy Right Act of 1957 are mute on the matter. As a result, we lack the enforcement tools necessary to guarantee the online protection of domain names. The time has arrived for us to pass specific legislation to safeguard intellectual property online.

    This highlights the need for a more comprehensive and dedicated legal framework to address intellectual property rights, particularly trademarks, in the online environment. These loopholes stem from the lack of explicit provisions, enforcement tools, and specific legislation tailored to the unique challenges of the digital age.

13. **(Justin Hughes)[39]:** The three different conceptions of the Internet's relationship to law that emerged in the 1990s are initially discussed in this article: the no-law Internet, the Internet as a separate jurisdiction, and Internet law as translation. Presently, the third one essentially rules talks on Internet law and policy in practice. Translation projects entail more than just bringing conventional legal ideas into the online sphere; they frequently involve an effort to translate into cyberspace social, political, and economic interests that have been determined and approved in the real world. The article criticizes American legal experts for their failure to recognize the global issue of online legal norms and how the Internet is driving some degree of legal norm convergence amongst heterogeneous national systems. The article goes on to suggest a rough taxonomy of the processes involved in developing convergent legal standards for the Internet. By addressing these issues, the

[38] Mr. Atul Satwa Jaybhaye, *Cyber Law and Ipr Issues: The Indian Perspective,* BLR 166, 185 (2016).
[39] Justin Hughes, The Internet and The Persistence of Law, 44 B.C.L. Rev. 359 (2003).

legal system can better protect trademarks and other intellectual property in the digital environment, while ensuring fair and consistent application of laws across jurisdictions.

14. **(Intellectual Property Rights and Global Capitalism):**[40] This paper examines the genesis and implications of the Trade-Related Intellectual Property Rights (TRIPS) agreement reached during the Uruguay Round of GATT negotiations. The main theme is that the TRIPS agreement is not in the best interests of poorer countries, and that its imposition by richer countries is motivated by the exercise of political and economic power rather than the positive economic benefits claimed by the agreement's supporters. To back up this claim, the book objectively evaluates economic evidence on the influence of intellectual property rights on key factors such as export performance, foreign investment, and economic growth.

    The author gives a political economic study of why poorer nations joined the TRIPS agreement, using case studies from two significant areas where the conflict over intellectual property is particularly intense: pharmaceutical and agricultural biotechnology sectors. The book, designed for advanced undergraduate and graduate courses in international political economy and international relations theory, provides a radical perspective on the globalization process. As, one can approach the analysis of trademark protection in cyberspace with a critical perspective, looking for potential areas where political, economic, and social dynamics may create loopholes or weaknesses in enforcement mechanisms. This might include examining how power dynamics between different countries or entities influence the development and enforcement of trademark regulations, as well as identifying specific industries or sectors where conflicts over intellectual property are especially pronounced and may reveal vulnerabilities in trademark protection strategies.

1.4 OBJECTIVE OF RESEARCH

The objective of this critical study is to delve into the evolving landscape of trademark infringement within cyberspace, aiming to identify emerging trends in violations and assess the efficacy of protective measures including:

i. The potential improvements in the legal frameworks and regulations governing trademark protection in cyberspace, considering the challenges faced by trademark owners in the digital era.
ii. Legal frameworks and regulations governing intermediaries' liability and exemption from liability in cyberspace, as well as how courts in various jurisdictions have dealt with these issues.

[40] DONALD G. RICHARDS, INTELLECTUAL PROPERTY RIGHTS AND GLOBAL CAPITALISM: THE POLITICAL ECONOMY OF THE TRIPS AGREEMENT (Routledge, 2004).

iii. It also emphasizes the challenges encountered by trademark owners globally in the digital era, to protect their intellectual property rights in cyberspace.

iv. To evaluate the roles and responsibilities of e-commerce platforms in preventing and addressing trademark violations committed by third-party sellers and the legal frameworks governing e-commerce liability for trademark infringement in cyberspace.

1.5 HYPOTHESIS

Adoption of stringent legislative measures are required for effective protection and efficient regulation of trademarks in cyberspace.

1.6 RESEARCH QUESTIONS

The research seeks to uncover the tactics and strategies employed by infringers to circumvent trademark regulations in the digital realm. Furthermore, it aims to evaluate the adequacy of existing protective measures, and enforcement mechanisms, in mitigating trademark infringement by delving into these questions:

i. What are the underlying factors driving the emergence of new challenges in trademark protection in cyberspace, and how do they impact the effectiveness of protective measures?

ii. How do issues such as domain name squatting, keyword advertising, and counterfeit goods impact the substantive aspects of trademark enforcement online?

iii. How do factors such as jurisdictional complexities, and the global nature of the internet influence procedural challenges in trademark enforcement?

iv. What legal frameworks govern e-commerce liability for trademark infringement in cyberspace, and how do they vary across jurisdictions?

1.7 SCOPE AND LIMITATION OF STUDY

The present study will exclusively focus on trademark protection in cyberspace, excluding other intellectual property rights, such as copyrights, patents, and trade secrets, and further, the researcher has specifically restricted herself to existing legal frameworks and emerging trends of trademark protection in cyberspace. The scope of the study is to highlight the need for a comprehensive legal framework to address these issues and to help policymakers and scholars in understanding the need for a comprehensive legal framework to address these issues. It will provide insights into the evolving nature of trademark law and the challenges and opportunities it presents in the digital age globally while focusing on India.

1.8 RESEARCH METHODOLOGY

The present study is based on a doctrinal method of research. It is based on primary and secondary data, wherein an analysis of the national and international legal instruments, judicial interpretations, and other non-judicial policies and frameworks has been made.

Data Collection: The primary source of information and data used for the study mostly consist of scholarly publications, and research papers published in national and international journals and periodicals. Further, literature pertaining to the subject area is consulted to gain a comprehensive understanding of the fundamental principles associated with the study. Further, e-newspaper is accessed to collect data about trademark violations and actions undertaken by the concerned stakeholders.

Mode of Citation: The mode of citation used in this study is Bluebook 20th edition.

CHAPTER 2: SUBSTANTIVE CHALLENGES OF TRADEMARK IN CYBERSPACE

2.1 INTRODUCTORY

A trademark is an identifiable phrase, word, symbol, or insignia that designates a particular product and legally sets it apart from all other items of the same sort. A trademark acknowledges the firm's ownership of the brand and uniquely identifies a product as being owned by that company[41]. The advent of the internet and the rise of cyberspace have presented numerous challenges to trademark protection and enforcement. Additionally, the global nature of cyberspace means that businesses can face infringement and counterfeiting issues across different jurisdictions. This chapter aims to explore the challenges faced by trademark owners in cyberspace and e-commerce and discuss various strategies and solutions to combat these issues.

Trademark law protects trademarks from infringement by third parties to guarantee that consumers can identify the true source of their products and are shielded from fraud and confusion, as well as to enable

[41] WIPO, https://www.wipo.int/trademarks/en/ (last accessed on Apr. 9, 2024).

producers and manufacturers to build reputations and safeguard their goodwill, the two main forms of infringement that are pertinent to the trademark/domain name dispute are those that lessen the value of a trademark and those that increase the likelihood of confusion[42].

The first kind of infringement occurs more frequently, a plaintiff must demonstrate that the defendant's mark is so similar to their own that is likely to confuse consumers about the origin of the goods, when assessing a likelihood of confusion claim, a court will consider several factors, none of which is dispositive on its own. These factors include the strength or weakness of the marks; the similarity of the marks in terms of appearance, sound, and meaning; the similarity of the goods in question; the intent or bad faith of the defendant in adopting a similar mark; the closeness of the goods' marketing, distribution, and advertising channels; the level of sophistication of the goods' customers; and concrete proof of consumer confusion. The likelihood of confusion between two marks can be ascertained by considering any evidence that a mark has impacted the overall impression that a potential buyer of a certain product is given[43].

The subject of trademarks has been discussed extensively, due to its vastness and scope. Cyberspace presents several challenges pertaining to trademark and trademark-related matters. The most significant and well-known are those of 'Domain Name'. A domain name is a component of a website's online address and location. Although trademarks have been in use for a considerable amount of time, domain names are a relatively new idea gaining popularity.

The Internet has become a global and commercial platform, and as a result, a domain name has gained recognition and goodwill. Domain names are now widely utilized not only in cyberspace but also in the physical world. It can be seen on magazine covers, TV advertising, bus sides, and other places.

Internet Protocol, also known as an IP address in a common language and is utilized for computer-server communication, is the fundamental building block of the Internet. Thus, to dissect such a problem the concept of domain names has been discussed, it functions well as an IP address substitute[44].

Domain names are what a user uses when we type something like 'Facebook.com' or 'Google.com' into our web browser. They are essential in helping people, companies, and organizations create an internet presence. Consider domain names to be the online equivalent of a website's address. It makes webpage access easier by acting as a human-readable label.

Top-level domain names are administered by the Internet Corporation of Assigned Names and Numbers (ICANN), a domain name regulatory body. To obtain a domain name, one must first get in touch with the TLD administrator. The administrator will only authorize a name if it is similar to what has been sought and has not already been assigned to someone else. There is a particular registration procedure to

[42] Joshua Quitmer, Billions Registered: Right Now, There Are No Rules to Keep You from Owning a Bitchin' Corporate Name as Your Own Internet Address, WIRED, Oct. 1994 at 54.
[43] Polaro id Corp. v. Polarad Elect. Corp., 287 F.2d 492 (2d Cir. 1961).
[44] Huey-Ing Liu, *Mobile domain name system: an alternative for mobile IP*, 2 ICCS 830, 834-838 (2002).

follow. The central body responsible for allocating IP addresses and domain names across the Internet is called the IANA (Internet Assigned Numbers Authority)[45].

Another international organization aimed at ensuring the protection of intellectual property rights globally is the World Intellectual Property Organization (WIPO). By continuously pushing the boundaries of science and technology and enhancing the fields of literature and the arts, this international protection catalyzes human creativity. It also greases the wheels of global trade by offering a stable environment for the selling of Intellectual property goods. It also emphasizes how intellectual property laws should be used differently in online e-commerce and how new standards should be established in this area. Since several challenges impact various facets of society and government, both domestically and globally, WIPO seeks to facilitate coordination and guarantee the development of effective and uniform solutions to shared problems[46].

The current information age requires intellectual property laws to catch up with and proactively regulate unfolding technological realities. The dynamic advances in the domain of the Internet have thus necessitated corresponding changes in intellectual property laws, specifically concerning trademarks.

This commercialization has resulted in the emergence of numerous online platforms, marketplaces, and social media channels where businesses can promote their products and services. However, this proliferation of digital spaces also presents the risk of trademark infringement and counterfeiting. It is an indisputable fact that businesses need to feel confident in their ability to defend their trademarks for cyberspace to operate as a profitable commercial marketplace. However, the demands of the Internet community as a whole, not just trademark owners, must be met by Internet management. Thus, even though the scope and direction of the effects brought about by the Internet are yet unknown.

The substantive challenges of trademarks in cyberspace which are dealt with in this chapter majorly include domain registration and search engine advertising and some other miscellaneous issues arising cause of the same. In India, domain registration is governed by the Indian Domain Name Dispute Resolution Policy (INDRP) and the National Internet Exchange of India (NIXI) which is subject to the INDRP[47] and the jurisdictional issues arising from the universal nature of domain names. In terms of search engine advertising, trademark holders face challenges in enforcing their rights in the digital space, existing mechanisms for resolving conflicts between trademark owners and domain name holders are often viewed as expensive, cumbersome, and ineffective. India has its legal framework to address these issues, including the Indian Trade Marks Act, 1999 and the Information Technology Act, 2000.

The sheer number of instances precludes many trademark owners from filing multiple suits in one or more national courts, these issues arise due to the global nature of the Internet and the territorial nature of

[45] Sourabh Ghosh*, Domain Name Disputes and Evaluation of The ICANN's Uniform Domain Name Dispute Resolution Policy*, 9 JIPR. 424 (2004).

[46] Dev Agrawal, *UDRP (Domain Name) Arbitration: Enforceability and Relevance under Alternate Dispute Resolution Framework,* 5 JIPR. 135 (2022).

[47] Registry, https://www.registry.in/domaindisputeresolution (last accessed on April 19, 2024).

trademark laws[48]. The tension between the largely unregulated system of registering Internet domain names and the highly regulated system that protects intellectual property rights is another challenge. The value of a website derives from it getting noticed, and web surfers generally search by entering famous names, leading to the frequent establishment of websites under domain names that incorporate variations on prominent trademarks and corporate names. These are just some of the substantive challenges trademarks face in cyberspace.

Cybersquatting, linking, and framing are further examples of trademark challenges in cyberspace. When different companies trading under the same mark in different parts of the world have different domain names, trademark law which has territorial influence can be violated.

Linking and framing strategies create circumstances in which a possible and occasionally an evident trademark infringement occurs. The Internet's core function is linking, or hyper-linking. What distinguishes the Internet as 'a network of networks'[49] is the linking technology. Without linking technologies, we would not have witnessed such advancements in cyberspace.

The framing technique enables site managers to open another web page on a single page and build frames on the page itself. Frames are susceptible to infringements on intellectual property rights by their sheer nature[50]. In addition, a variety of additional things influence trademark regulations in the online sphere.

2.2 TRADEMARK INFRINGEMENT

The Trade Marks Act, 1940 is the primary piece of legislation in India that addresses the notion of trademarks. It was introduced into the statute book and established specific laws on the issue; nevertheless, it was abolished by the Trade and Merchandise Marks Act, 1958 after serving its purpose for forty years. Nevertheless, the Trade and Merchandise Marks Act, 1958 lacked a definition of 'registration' and a mechanism for trademark service registration. Beyond this, changes in trade and business practices, the growing globalization of business and trade, the need to promote investment and technology transfer, the need to simplify and harmonize trade, and the fulfilment of GATT and TRIPS requirements[51].

The Trade Marks Act, 1999 was enacted to replace the previous Trade and Merchandise Marks Act of 1958, which had replaced the Trade Marks Act, 1940. The need for the new Act arose due to the globalization of commerce and the increasing value of brand names, trade names, and marks, necessitating

[48] Thomas R. Lee, *In Rem Jurisdiction in Cyberspace,* Wash. L. Rev. 97 (2000).
[49] Id.
[50] Mondaq, https://www.mondaq.com/india/trademark/525188/legality-of-metag-ing-linking--framing (last accessed on April 9, 2024).
[51] BANANAIP, https://www.bananaip.com/ip-news-center/history-and-evolution-of-trademark (last accessed on April. 20, 2024)

consistent minimum standards of protection and effective enforcement mechanisms. The Trade Marks Act, 1999 was enacted to comply with the TRIPS (Trade-Related Aspects of Intellectual Property Rights) agreement recommended by the World Trade Organization. It unified the Merchandise Marks Act of 1889 and various regulations about trademarks found in the Indian Penal Code, Criminal Procedure Code, and Sea Customs Act into a single piece of legislation. The main features of the Trade Marks Act, 1999 include:

i. Allowing the registration of service marks
ii. Enabling the filing of multiclass applications
iii. Extending the period of registration of a trademark to ten years
iv. Recognizing the concept of well-known marks
v. Providing the police with the power to arrest in cases of trademark infringement
vi. Defining the term "infringement" and prescribing punishments and penalties for offenders

The Act aims to grant protection to trademark users, define the conditions of trademark ownership, and provide legal remedies for the enforcement of trademark rights.

The holder of a trademark has the sole right to use it in connection with the products or services for which it is registered under the trademarks Act of 1999. Additionally, it grants the owner the right to pursue legal action against the infringement party to obtain an injunction, damages, or other remedies[52]. Nevertheless, the Act's restrictions and conditions will apply to this privilege.

In contrast to passing-off proceedings, where the plaintiff must demonstrate that he is the user of the mark that has become distinctive of his products or services and merely registering that entity gives the plaintiff the right to sue[53]. Section-29 of the Trademark Act of 1999[54] outlines the various circumstances under which a registered trademark can be considered infringed. It defines infringement as the unauthorized use of a mark in a way that could confuse consumers or dilute the distinctiveness of the registered mark. The criteria for infringement include the similarity between the infringing mark and the registered trademark, the likelihood of confusion among consumers, and the potential for unfair advantage or detriment to the reputation of the registered trademark including the following factors:

a) Use in the course of trade**:** Infringement occurs when a person uses a mark in the course of trade without authorization, in connection with goods or services similar to those covered by the registered trademark.
b) Likelihood of confusion: If the use of a mark is likely to cause confusion among the public regarding its association with the registered trademark, it constitutes infringement. This presumption applies particularly if there is identity between the marks and the goods or services they represent.

[52] Id.
[53] Singer Manufacturing Co. v. Loog, 18 U.S. 395, 412 (1880).
[54] Trademark Act of 1999 S.29(1): A registered trademark is infringed by a person who, not being a registered proprietor or a person using by way of permitted use, uses in the course of trade, a mark which is identical with, or deceptively similar to, the trade mark in relation to goods or services in respect of which the trade mark is registered and in such manner as to render the use of the mark likely to be taken as being used as a trade mark.

c) Reputation of the trademark: If an identical or similar mark is used in connection with goods or services unrelated to those covered by the registered trademark, and the registered trademark has a reputation in India, infringement can occur if the use takes unfair advantage of or is detrimental to the distinctive character or reputation of the registered trademark.
d) Trade name usage: Infringement also occurs if a person uses the registered trademark as part of their trade name or business concern name in relation to goods or services covered by the trademark registration.
e) Modes of usage: Various forms of usage, including affixing the mark to goods, offering goods or services under the mark, importing or exporting goods under the mark, and using the mark in advertising or on business papers, constitute infringement.
f) Unauthorized application: Applying the registered trademark to materials without proper authorization from the proprietor or licensee also constitutes infringement.
g) Unfair advertising practices: Advertising that takes unfair advantage of the trademark, is contrary to honest practices, or is detrimental to the distinctive character or reputation of the mark constitutes infringement.
h) Spoken use: In cases where the distinctive elements of a registered trademark include words, infringement can occur through the spoken use of those words, in addition to their visual representation.

2.2.1. Non-Infringement of Registered Trademark

Section-30 of Trademark Act, 1999 establishes exceptions to the general prohibition on using registered trademark[55] to identify one's own goods or services. As a result, the following uses of a registered trademark are not allowed to violate it:

i. Use in line with ethical standards in business and industry affairs, so as not to unfairly exploit or damage the reputation or distinctive qualities of the trademark.
ii. Use to indicate the kind, quality, amount, intended use, value, place of origin, timing of the manufacturing of commodities or the provision of services, as well as any additional attributes of the respective items or services.
iii. Use in connection with products or services for which the trademark has been legally applied, or in situations in which the registered owner has granted permission to use the trademark.
iv. Using a registered trademark, which is the exercise of the right to use one, two, or more trademarks that are identical or strikingly similar to one another and are registered under the Act.
v. The transfer of a registered trademark to a third party does not impact the owner's ability to resell or trade legally acquired items carrying the mark.

[55] Trademark Act, 1999, S. 30 "*Limits on effect of registered trade mark*".

This clause, however, does not apply if the items circumstances alter or deteriorate after they are placed on the market.

2.2.1.2 Judicial Principles on Infringement of Trademarks

In addition to the laws, the Indian judiciary has established certain guidelines for resolving trademark infringement cases in various rulings:

In S. M. Dyechem Ltd. v. Cadbury (India) Ltd[56], The Supreme Court of India observed that the primary characters of each mark could be taken into consideration while determining whether or not two marks are similar. Even still, the majority of the key components in each may convey rather diverse messages. However, a thorough examination of the two markings could reveal many differences, but even so, the overall impression that would be left on anyone viewing them separately over time might be the same. Therefore, it is evident that a mark is violated if the key characteristics or details of it are copied[57]. The Apex Court further acknowledged that certain laws place more focus on common characteristics than on necessary characteristics and concluded that

> *"where common marks are included in the rival trademarks, more regard is to be paid to the parts not common and the proper course is to look at the marks as a whole but at the same time not to disregard the parts, which are common"*[58].

Taking it a step further, the Supreme Court established a two-point standard to assess trademark infringement[59]:

(i) Is there a distinctive aspect of the common feature that has been replicated?

(ii) How are the components assembled differently, i.e., are the differences enough to cause the mark to differ?

Further, the *Supreme Court in Satyam Infoway Ltd vs Sifynet Solutions Pvt Ltd*[60] has observed that

> *"the distinction lies in the manner in which both, the trademark and a domain name operate. A trademark is protected by the laws of a country where such a trademark may be registered. On the other hand, a domain name is potentially accessible irrespective of the geographical location of the consumers. The outcome of this potential for universal connectivity is not only that a domain name would require worldwide exclusivity but also that national laws might be inadequate to effectively protect a domain name, although the operation of the Trade Marks Act, 1999 itself is not extraterritorial and may not allow for adequate protection of domain names, this does not mean that domain names are not to be legally protected to the extent possible under the laws relating to passing off."*

---

[56] M/S S.M. Dyechem Ltd v. M/S Cadbury Ltd, 5 S.C.C. 573 (2000).
[57] Supra note 14 at 7.
[58] Id.
[59] Supra note 47 at 20.
[60] Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd, AWC 2366 SC (2004).

In this case, it was observed that the distinction between a trademark and a domain name lies in their operational nature. A trademark is protected by the laws of a country where it is registered, whereas a domain name is accessible globally, regardless of the geographical location of consumers. This universal connectivity requires worldwide exclusivity for domain names, which national laws might not be able to effectively protect. Although the Trade Marks Act, 1999 is not extraterritorial and may not provide adequate protection for domain names, it does not mean that domain names should not be legally protected to the extent possible under laws relating to passing off.

In Allergan Inc. v. Milment Oftho Industries and others[61], the Calcutta High Court noted that even in the absence of any business activity, a plaintiff with a well-established international reputation may file a lawsuit in this nation to seek protection. The Court further held that in cases where the two products in question were pharmaceutical preparations with identical names, the foreign manufacturer company was the one who chose the name first and used it on its product in several countries worldwide, except for India, where the Indian company may be prevented from using the trademark after the foreign company, along with some Indian pharmaceutical companies, established a joint venture company to sell its product in India and applied to the Registrar of Trademarks for registration of the disputed mark.

In Maekawa Bearing Manufacturing Co. Ltd. v. Onkar Bearing Industries[62], the High Court of Delhi noted that in the case of honest concurrent use, the Registrar may, if deemed appropriate, allow the registration of multiple identical or nearly resembling marks, regardless of whether any such trademark has previously been registered or not, for the same goods or a description of goods, subject to any restrictions or conditions the Registrar deems appropriate. It would be impossible to characterize the Registrar's use of discretion as wicked or random.

In Parle Products (P) Ltd. v. J.P. and Co[63], the standards to ascertain whether the marks misleading resemblance qualified as an infringement were established by the Supreme Court. To determine if two marks are confusingly similar, it is necessary to take into account both of their main characteristics. To determine whether there are any design differences and, if so, whether those differences are distinct enough to keep one design from being confused with the other, they shouldn't be positioned side by side. If the contested mark and the registered mark are sufficiently similar overall, it should be sufficient to fool someone who typically deals with one into accepting the other if it were shown to them.

2.3 DOMAIN NAME

With the growing dominance of cyberspace in the corporate world, the significance of domain names and trademark law is amplified.

[61] Allergan Inc. v. Milment Oftho Industries, S.C.C. 624 (2004).
[62] Maekawa Bearing Manufacturing Co. Ltd. v. Onkar Bearing Industries, PTC (18) 300 (1998).
[63] Parle Products (P) Ltd. v. J.P. and Co, AIR 1972 SC 1359.

Every webpage possesses a distinct address that serves the purpose of not only identifying the business and its branding, but also distinguishing it from competitors in the market. Domain names facilitate the process of website retrieval for internet users by providing a more memorable and accessible alternative to manually entering the long binary IP address.

A domain name is an exclusive identifier for a website, comprising three components. The initial component is referred to as the third-level domain and typically includes the term 'www'. This signifies that the website is reachable through internet search engines and is linked to the worldwide web. The second component, which includes the company's unique name, holds the utmost significance, 'Facebook', are example of second level domain[64]. The final component is referred to as the top-level domain name, and it might be a country code, generic code, special top-level domain name, or restricted use domain name[65].

i. If it is a country code, like '.in' for India or '.jp' for Japan, it designates that specific nation.
ii. If a business selects generic codes like '.com,' '.org,' or '.edu,' it signifies deployment to all classes of organisations and is governed by the Internet Corporation for Assigned Names and Numbers, or ICANN.

In common parlance, unique top-level domain names are usually available in the form of: '. lawful,' app,' etc. As the name implies, restricted top-level domain names are not available for general use like '.biz,' 'arpa,' etc[66]. The allocation of these domain names follows a case-by-case procedure. Either a first-come, first-served policy might apply, or a company with a valid business claim over another company name would be granted precedence.

Domain name systems are very important in the ever-evolving world of e-commerce, and disputes resulting from them are unabated[67]. This implies that a certain regulatory body is required. Since the domain name plays a significant part in identifying the source of the product, they should be treated similarly to trademarks for the purposes of legal protection and recognition, as doing otherwise may result in trademark infringement[68].

Over the last ten years, domain names have evolved into online equivalents of real-world brand names or trademarks, they can be thought of as 'e-commerce marks' or digital business addresses, which are points of contact or transaction for businesses. In essence, domain names are a simpler way to remember websites addresses than their more complicated numerical addresses, also known as Internet Protocol or IP numbers[69].

Domain name registration in India is facilitated by various reputable domain registrars offering services like web hosting, domain registration, and more. The cost of registering a domain name in India typically ranges from Rs. 350 to Rs. 900 per year, with renewal prices potentially higher. Some of the best

[64] Supra note 47 at 21.
[65] Supra note 35 at 17.
[66] A Froomkin, *The collision of trademarks, domain names, and due process in cyberspace*, 40(2), CACM 91-97 (2001).
[67] Richard L. Baum and Robert C. Combow*, First Use Test in Internet Domain Name Disputes*, NATL. LJ 30, (1996).
[68] Supra note 36 at 17.
[69] THOMSON WEST, INTERNET LAW AND PRACTICE (18th ed. 2002).

domain name registrars in India include GoDaddy, Namecheap, BigRock, Google Domains (now Squarespace Domains), Name.com, Hostinger, and Bluehost[70].

In addition to providing a distinctive identity for a product, trademarks are now used by many businesses as a kind of digital branding. In order to draw more visitors to their websites, businesses frequently combine two languages, multiple fonts, and colour schemes into their fancy, distinctive domain names. As a result, domain names are a crucial instrument for business-to-business communication[71]. In contrast to domain names, which belong to a single person in the virtual world and may be used for a company that offers a variety of goods and services, trademarks in the real world can be held by two individuals from different countries for goods and services.

In Doe v. Unocal Corp[72]*.,* it was decided that in cases where an exercise of personal jurisdiction is contested, the burden of proof rests with the plaintiff and also in *Burger King Corp. v. Rudzewicz*[73]*,* it was decided that the exercise of personal jurisdiction over an out-of-state defendant must comply with constitutional due process.

The Indian domain name registration landscape is constantly evolving. With the increasing popularity of regional languages online, there is a growing demand for domain names with regional language characters. Additionally, the introduction of new generic top-level domain (gTLDs) which is an initiative coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN) that is enabling the largest expansion of the domain name system which provides businesses with more options for establishing their online presence. The interface between trademarks and domain names is one of the most significant difficulties to trademark law brought about by the growth of the Internet.

According to paragraph 4(b) of the UDRP Policy[74], an Administrative Panel may determine that the following circumstances demonstrate the registration and use of a domain name in bad faith[75]:

(i) Circumstances demonstrating that you purchased or registered the domain name primarily with the intent of selling, renting, or otherwise transferring its registration to the complainant, who is the owner of the trademark or service mark, or to a competitor of the complainant, for an amount exceeding your documented out-of-pocket costs directly related to the domain name; (ii) If you have engaged in a pattern of such behavior, as you registered the domain name to prevent the trademark or service mark owner from using the mark in a related domain name.

(iii) Domain name registration primarily intended to harm a competitor's business; or

(iv) By using the domain name, you have intentionally attempted to use it to attract users to your website or other online location in order to profit from it. This is done by increasing the likelihood that users will

[70] ANDRÉ BRUNEL and MAY LIANG, *Trademark Troubles with Internet Domain Names and Commercial Online Service Screen Names: Road running Right into the Frying Pan,* 5.1 IJLIT, 1-24 (1997).
[71] Pope, Michael and Warkentin, Merrill and Mutchler, Leigh and Luo, Robert, *The Domain Name System: Past, Present, and Future,* 30 Communications of the AIS, 251 (2012).
[72] Doe v. Unocal 395 F.3d 978 (9th Cir. 2003).
[73] Burger King Corp. v. Rudzewicz 471 U.S. 462 (1985).
[74] Uniform Domain Dispute Resolution Policy A. 4(b) *Evidence of Registration and Use in Bad Faith.*
[75] ICANN, https://www.icann.org/resources/pages/policy-2012-02-25-en (last accessed on May 1, 2024).

mistakenly associate the complainant's mark with your website or location and think it is the source, sponsorship, affiliation, or endorsement of your website or location, or of a good or service that you offer.

UDRP Policy outlines circumstances demonstrating bad faith registration and use of domain names, including intent to sell, pattern of blocking trademarks, undermining competitors, and creating likelihood of confusion for commercial gain.

2.3.1 Classification of Domain Names:

Generally, the domain names are classified into the following categories[76]:

i. Top-level domain (TLD): At the end of a domain name, such as.com, .net, or.org, is the top-level domain. Uniform resource locators (URLs), domain suffixes, and domain extensions are other names for TLDs. TLDs are an essential component of every company's internet marketing plan. Each domain name ends in a top-level domain. Websites are identified, arranged, and classified by the top-level domain according to their location, purpose, and content. For example, business websites use.com domains, whereas educational websites use.edu domains. TLDs give consumers and search engines insight on your website's background, industry, and location[77].

ii. Second-level domain (SLD): A second-level domain (SLD) is the part of a domain name that comes before the top-level domain (TLD). For example, in the domain name ‘example.com’, ‘example’ is the SLD and ‘.com’ is the TLD.[78]

iii. Sub-domain (SD): An extra bit of information appended to the front of a website’s domain name is called a subdomain name. It enables websites to arrange and divide material for a particular purpose from the rest of their website, such as a blog or an online store[79].

SLD is positioned ahead of the TLD and indicates the particular entity or brand[80]. For instance, the word ‘Google’ is the SLD in the domain name ‘Google.com.’ Subdomains can also come before the SLD, which helps to further organize and segment online content, a smaller domain name is a subdomain. For instance, ‘blog.website.com’ can be a subdomain created especially for the blog Section if ‘website.com’ is the primary domain[81]. It facilitates easier navigation across website Sections for users. Subdomains are frequently used for things like forums, blogs, and multilingual website editions. They increase the versatility with which website owners can arrange their material and enhance user experience.

2.3.2 Categories of Domain Name Dispute

Domain name disputes are generally categorised into four types as follows:

---

[76] Supra note 35 at 17.

[77] Nikita Tambe and Aashika Jain, *What Is a Top-Level Domain (TLD),* FORBES, (Mar. 20, 2024, 5:52 pm), https://www.forbes.com/advisor/in/business/software/top-level-domain/ .

[78] LISA KA 1Z JONES, *Trademark.Com: Trademark Law in Cyberspace, file:///C:/Users/DELL/Downloads/alr,+37-4_8_Katz_Jones.pdf (last accessed on 1 May 2024).*

[79] Id.

[80] Id. At 10.

[81] Supra note 26 at 10.

i. Cyber Squatter: A 'cyber squatter' is a person who has registered or otherwise obtained a domain name speculatively intending to sell, rent, or in some other way transfer the domain name registration to the complaint, who is the mark or service mark owner. Parties may register names to sell them at auction to the highest bidder[82].

The owner of the trademark is unable to register his trademark as a domain name as long as a cyber-squatter is the owner of the domain name. In doing so, a cyber-squatter violates the owner of a trademark's right to use it. It is important to remember that reserving a domain name is a perfectly valid procedure. Cyber squatters frequently register words or phrases they believe future businesses will find appealing[83].

The American Court determined in *Card Service International Inc. v. McGee*[84] that the domain name serves the same serve as a trademark and is not just meant to be built as an address since it identifies a website to those who access it, much like a person's name identifies a certain individual.

The defendants in *Mark and Spencer v. One-in-a-million*[85] had registered several well-known trade names connected to major firms with which they had no affiliation as domain names. Then, for a fee, they made them available to the businesses connected to each name. The Court ruled that a person should anticipate becoming the target of an injunction to stop the threat of passing off when they knowingly register a domain name because it is similar to the name, brand name, or trademark of an unaffiliated commercial business.

ii. Cyber Parasite: A cyber parasite is a type of domain name dispute in cyberspace that involves registering a domain name similar to a well-known trademark with the intent of using it to make a profit rather than selling it. The goal is to deceive consumers into using the cyber parasite's domain name instead of the original trademark's, and then to profit from the use of the domain name. For example, someone might register a domain name like www.faceook.com to trick people into going to their site instead of the original www.facebook.com.[86].

In Akash Arora and Others v. Yahoo[87], In this instance, the Delhi High Court used the passing off remedy to successfully safeguard a domain name for the first time in India. The plaintiff in this action is the owner of the domain name yahoo.com– as well as the trademark yahoo–. For a comparable service, the defendant registered the domain name yahooinida.com, therefore a passing off was filed by the plaintiff.

This case played a pivotal role in shaping the legal landscape for trademark protection in cyberspace in India. It established the principle that domain names can be considered intellectual property, subject to the

---

[82] Pranjalig, *Cyber-Squatting and Trademark Issues,* SCRIBD (Nov. 5, 2017), https://www.scribd.com/document/363557362/cyber-squatting-and-trademark-issues

[83] Jacqueline D. Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 Wake Forest Law Review 1361 (2005).

[84] McGee v. International Life Ins. Co., 355 U.S. 220 (1957)

[85] Marks and Spencer PLC v. One in a Million Ltd EWHC (November 28, 1997)

[86] Muragendra B. T, *Copyright and Trademark in Cyberspace,* 3 IJSER 1,4 (2012)

[87] Akash Arora and Others v. Yahoo! Inc 78 DLT 285 (1999)

same legal principles as traditional trademarks. This case paved the way for further judicial interpretations and legislative developments in adapting trademark laws to the ever-evolving digital environment.

In Rediff Communication Ltd. v. Cybertooth and Others[88], the plaintiff filed a passing-off lawsuit against the defendant, claiming that the defendant's adoption of the domain name rediff.com as part of their trading style was confusingly similar to the plaintiff's domain name, reddiff.com. According to the plaintiff's favorable court ruling, the defendant and plaintiff shared a common activity, both operated online, supplied comparable information, and provided a chat line as a result. One common man can own an Internet domain name, but different people may own the link between the two Since the defendants were found to have registered the domain name radiff.com intending to profit on the plaintiff's reputation, the court banned them from using the name.

This case further strengthened the legal framework for protecting trademarks in cyberspace. It reinforced the application of traditional principles of passing off and emphasized the importance of considering the parties' online activities, services, and the potential for consumer confusion. This case also highlighted the court's commitment to safeguarding established brands from unfair exploitation and demonstrated the willingness to grant effective remedies, including domain name transfers, in cases of trademark infringement in the digital domain.

iii. Cyber Twins: When there is a legitimate claim to the domain name, both the owner of the name and the person contesting it have a "cyber twin" situation. In the 2018 case, the domain name iffco.com was in question. *Indian Farmers Fertilizer Cooperation Ltd v. International Foodstuffs Co*[89],prior to the WIPO Center for Arbitration and Mediation. When using the domain name in this case, the defendant was operating in good faith. The complainant had a rightful stake in the domain because it was linked to iffco.com. The complainant said that the defendant was allegedly directing traffic. Since both parties had legitimate interests, the arbitration center dismissed the complaint because the complainant could not show that the defendant was using the domain name in bad faith.[90].

This Case demonstrates the nuanced approach taken by dispute resolution bodies in balancing the interests of parties involved in domain name disputes. It emphasizes the need for careful consideration of good faith registration and use, legitimate interests, and the provision of sufficient evidence to establish bad faith. This case contributes to the ongoing development of jurisprudence in the realm of trademark protection in cyberspace, particularly concerning the resolution of domain name conflicts.

iv. Reverse Domain Name Hijacking: It is an ill-intentioned attempt by the trademark owner to take over a domain name from another party that is entitled to use it. According to Rules 15(e) of the Uniform Domain-Name Disputes Resolution Policy (UDRP), if a complaint is lodged with the primary intention of harassing the domain name registrant, the panel may find that the complaint was filed in bad faith and amounted to an abuse of administrative processes. Reverse domain name hijacking is typically done by

[88] Rediff Communication Ltd. v. Cybertooth and Others (AIR 2000 Bombay 27)
[89] Indian Farmers Fertilizer Cooperation Ltd v. International Foodstuffs Co AIR 2018 SC (CIVIL) 1444.
[90] Supra note 32 at 13.

big businesses and individuals to either suppress slander and defamation or to safeguard their legal trademarks.[91].

In Digital Consulting Inc. v. Data Concepts Inc[92]*.,* Data Concepts Inc. decided to register a domain name in 1993, it chose 'dci.com', which was derived from the company's three initials. 'DCI' was the trademark registration of another company, Digital Consulting Inc. which was established in 1987. Nine years later, in 1996, Digital Consulting attempted to acquire dci.com but discovered it was three years out of date. Digital Consulting filed a complaint in the court of NSI. As anticipated, NSI wrote Data Concepts a letter with a 30-day deadline, siding with the challenger. The matter was referred to a magistrate, who recommended that the challenger be granted ownership of the 'dci.com' domain name after finding that the domain name owner violated the Lanham Act. The magistrate did not appear to consider the length of time that the dci.com domain name had been in use without any infringements occurring. Additionally, the domain name owner presented evidence that hundreds of companies bore the initials 'DCI' and that numerous companies had trademark registrations for 'DCI.' The district judge heard an appeal from the owner of the domain name, but he or she accepted the magistrate's findings and suggestions. The challenger received the dci.com domain name as a result of a court order.

Data Concepts filed an appeal with the Sixth Circuit Court of Appeals after losing ownership of the dci.com domain name. Reviewing the eight-trademark likelihood-of-confusion elements, the appellate court noted that the magistrate, and consequently the district judge, had committed multiple mistakes. The testimony of several other users of the 'DCI' mark was ignored by the court below with regard to the first criteria (strength of the mark). For example, the Sixth Circuit conducted its own investigation and discovered that the letters 'DCI' are frequently used in Internet domain names. The Court of Appeals further stated that the lower court had misunderstood and performed an insufficient analysis of the relatedness of services, the similarity of the marks, and the likelihood of buyer care.

In conclusion, it highlights a practice that has come to be known as 'reverse domain name hijacking', in which the owner of a trademark covets an already-registered domain name and attempts to obtain it by bringing a challenge in the court of NSI, where the challenger nearly always prevails without taking the merits into account. This show that the initial disadvantage caused by NSI's policy can be overcome by the innocent domain name owner who is ready and able to finance a lawsuit by having the challenge evaluated on its merits by a regular court. The trademark owner who participates in reverse domain name hijacking is likewise cautioned by the cds.com and dci.com cases that the result could be a court ruling that damages the trademark.

2.4 SEARCH ENGINE ADVERTISING

Internet users rely on search engines to find information. According to some scholars,

[91] Id.
[92] Data Concepts, Inc. v. Digital Consulting, Inc. 150 F.3d 620 (6th Cir., August 4, 1998)

"When the search engine software finds pages that match the search request, it presents the user with brief descriptions and clickable links to the web page.[93]"

The phrase "*the world's largest repository of content*"[94] is accurately applied to the Internet. The average Internet user may now access billions of web pages owing to the Search Engine. These days, Internet users may access and search for the information they need using popular search engines like Google, Microsoft, Yahoo, and others with only a few searches.

The practice of leveraging search engines for advertising through a variety of channels, such as offering keywords for sale to the highest bidder in exchange for a higher ranking in the search results, and selling keyword-linked banner ads on websites, is known as search engine advertising. If a user wants to buy clothes, for example, all he has to do is type a few keywords like product or color in the search box, and all the relevant pages that contain that item are shown in the search engine results page (SERP) in descending order of relevancy, which is determined by the specific search engine's algorithm. However, the majority of users only examine a small portion of the highly-ranked search results that a search engine returns[95].

The primary factor behind search engine marketing's widespread appeal is its exceptional capacity to tailor an advertisement to the exact phrase that a buyer is searching for. This personalization draws targeted users who may want to make purchases from the advertisers' websites. Search engine marketing, keyword advertising, and paid or sponsored search are among other names for this very well-liked form of online advertising[96]. According to statistics, the United States alone accounted for $10.7 billion in 2009, or 47% of the total worldwide expenditure on web advertising[97]. This form of advertising has become the largest source of revenue for search engines.

The well-known search engines sell keywords to prospective advertisers through pay-for-placement programs, realizing the commercial potential of their websites and guaranteeing high-ranking in-search results for particular search terms. Nonetheless, these sponsored placements are typically marked and separated from the regular search results on the search page in order to preserve the 'integrity' of the search engine. Keying, sponsored listings, paid search advertisements, banner ads, pay for placement, pay for performance, CPC listings (Cost-Per-Click), and PPC listings (Pay-Per-Click) are some other terms used to describe these paid placements[98]. In *Playboy Enterprises, Inc. v. Netscape Communications Corporation*[99], the Ninth Circuit defines the process thus:

"Keying allows advertisers to target individuals with certain interests by linking advertisements to pre-identified terms. To take an innocuous example, a person who searches for a term related to gardening may be a likely customer for a company selling seeds. Thus, a

---

[93] DIANE POREMSKY, GOOGLE AND OTHER SEARCH ENGINES 60 (Peachpit Press 2004).
[94] David M. Fritch, *Click Here for Lawsuit-Trespass to Chattels in Cyberspace*,9 J. TECH. L. and POL'Y 31,32 (2004).
[95] KEVIN LEE and CATHERINE SEDA, SEARCH ENGINE ADVERTISING: BUYING YOUR WAY TO THE TOP TO INCREASE SALES 964 (New Riders, 2009).
[96] Supra note 79 at 27.
[97] Nadia Abou Nabout, *Return on Quality Improvements in Search Engine Marketing,* J. Interact. Mark, 26 (2020).
[98] Id.
[99] Playboy Enterprises, Inc. v. Netscape Communications Corp., 354 F.3d 1020 (9th Cir. 2004).

seed company might pay to have its advertisement displayed when searchers enter terms related to gardening. After paying a fee to the defendants, that company could have its advertisements appear on the page listing the search results for gardening-related terms: the advertisement would be 'keyed' to gardening-related terms. Advertisements appearing on search result pages are called 'banner advertisements' because they run along the top or side of a page much like a banner. However, not all banner advertisements are keyed. Some advertisers buy space for their banner advertisements but only pay to have their advertisements displayed randomly. Such advertisements cost less because they are un-targeted and are, therefore, considered less effective.[100]"

2.4.1 Trademark and Keyword Advertising

Because Search Engines rely heavily on descriptive phrases to perform their jobs, websites will unavoidably want to include trademarks even those of other companies into the descriptive shorthand used for Internet navigation. Similar to the real world, the context greatly influences whether using these trademarks in cyberspace amounts to infringement. Advertisers are free to use any combination of terms including terms that are trademarked by others as the key phrase for their ads[101]. The owners of trademarks may object to such use, but the courts are unlikely to find the search engines guilty of infringement or diluting trademarks[102]. For the most part, search engines rely on advertising to make money. It is well known that for an effective advertisement, advertisers will pay more. The effectiveness of advertising seems to rise with targeted or tailored content. As a result, problems with keyed banner ads, paid placement, and other types of targeted advertising are probably going to persist[103].

The way keyword advertising operates is that when consumers type keywords into search engine bars, they get two different kinds of results: sponsored and unsponsored. Natural or unsponsored search results are based on how relevant the results are. In contrast to the sponsored search results (which are displayed on the upper right-hand side), where advertisers pay for each click on their advertisement, the display of natural results is free of charge. The keyword auction determines the cost and position paid for each click. Two dominant players in the industry with comparable auction designs are Yahoo and Google[104]. Advertisers typically bid for each keyword for each click, and the search engine provider assigns a value to the bid based on the quality of the advertisement, as determined by the proprietary quality score. These days, a significant portion of many well-known search engines' revenue comes from selling ads that are displayed on search result sites. AdWords is also how Google makes the majority of its revenue[105].

---

[100] Id.
[101] Heidi S. Padawer, *Google This: Search Engine Results Weave a Web for Trademark Infringement Actions on the Internet*, 81 WASH. U. L. Q. 1099 (2003).
[102] Gunmala Suri, *Intellectual Property Rights Management: Emerging Cyberspace Issues in Knowledge Society: A Critical Analysis*, UBS PU, 256 (2019), https://csi-sigegov.org.in/critical_pdf/29_256-262.pdf.
[103] Supra note 37 at 14.
[104] Supra note 84 at 28.
[105] Megan Graham and Jennifer Elias, *How Google's $150 billion advertising business works,* CNBC, OCT. 13, 2021

2.4.2 Google ad revenues (2013–2023)

Growth in Google's ad income year over year is unmistakable proof of the platform's appeal. Industry analysts recently released a report stating that Google's advertising income in 2023 was $237.86 billion, 6% more than 2022's figures. It is the weakest annual rise in almost ten years, notwithstanding the expansion. Google has seen annual growth in ad income since at least 2013. Google's ad income for that year was $51.07, up 16.9% over the previous year. This rose to $59.62 billion in 2014 and then to $67.39 billion in 2015[106].

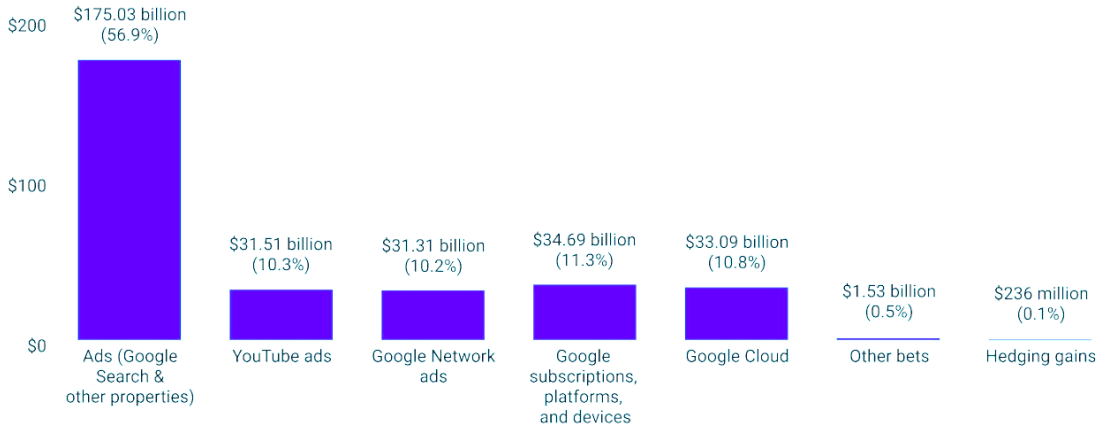

Figure 2.1:Google Revenue Breakdown

Source: Alphabet[107]

Google's parent firm Alphabet recently released its earnings report, stating that the company's total worldwide revenue in 2023 was $307.39 billion, with $237.86 billion coming from Google advertising. This covers money made from YouTube advertisements, Google network ads, and Google search revenue. This amounts to more than 75 percent (77.4%) of the total revenue generated by the business.

[106] Oberlo at https://www.oberlo.com/statistics/google-ad-revenue (last accessed on 22 April 2024)
[107] Supra note 89 at 29

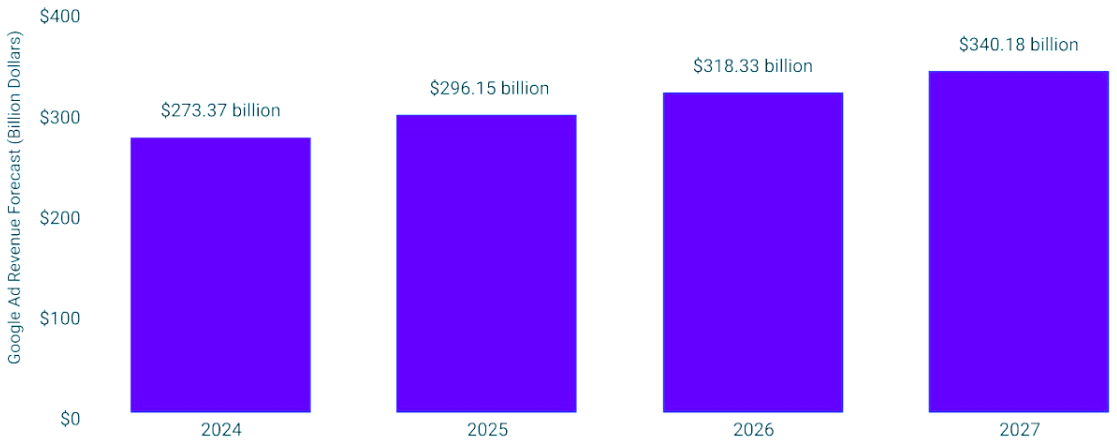

Figure 2.2:Google Ad Revenue Forecast (2024-2027)

Source: Statistica[108]

By analysing both figure 2.1 and 2.2 it was clear that Google's success in generating ad revenues heavily relies on the recognition and value of its trademark and brand. As a dominant player in the online advertising industry, Google's brand reputation and consumer trust are crucial factors that attract advertisers to its platform. Google's advertising business model relies on the use of domain names and keywords in search engine advertising. As Google's advertising platform expands, the risk of trademark infringement through sponsored ads or keyword advertising increases[109]. Advertisers may use trademarked terms or brand names without authorization, leading to potential consumer confusion and dilution of brand value.

Google's AdWords system allows advertisers to bid on trademarked keywords, leading to situations where competitors may display ads when users search for a specific brand. This practice has raised concerns about trademark infringement and unfair competition[110]. As online advertising and e-commerce activities have grown, the need for effective brand protection in the digital space has become increasingly important.

As Google's ad revenue continues to grow, it highlights the need for robust legal frameworks, effective enforcement mechanisms, and collaborative efforts between technology companies, brand owners, and regulatory bodies to protect trademark rights in the digital advertising landscape. It is crucial for Google and other online advertising platforms to prioritize trademark protection and maintain a balanced approach that respects intellectual property rights while enabling legitimate advertising practices.

---

[108] Id.

[109] Anamika, *Google can't claim safe harbour if use of trademarks in Ads Programme violates trademark: Delhi HC,* ETtech (Aug 12, 2023, 11:32:00 AM), https://economictimes.indiatimes.com/tech/technology/google-cant-claim-safe-harbour-if-use-of-trademarks-in-ads-programme-violates-trade-mark-delhi-hc/articleshow/102653776.cms?from=mdr.

[110] Id.

2.4.3 Pop-Ups, Pop-Unders, and Pop-Overs

> *"Pop-up advertisements are used as marketing tools designed to capture consumers' attention, and are based on software designed to track users' online activity and then deliver targeted advertising based on their preferences."*
>
> -WIPO[111]

Pop-ups, Pop-unders, and Pop-overs are technological subsets that are developing at a rate that makes it harder for the law to keep up. Pop-ups are little or occasionally larger windows that appear on their own without any input from the user. These obtrusive pop-ups, pop-unders, and pop-overs are essentially more of a bother than a usefulness.

When a person is watching content on the Web, a pop-up is a little window that pops out of nowhere and is shown on top of the other windows on the screen. Any application can show new information by using a pop-up window. The technique of making an advertisement 'pop up' on a webpage is commonly employed. Pop-unders are ads that show up in a different window beneath the user's Internet browser window, where they remain visible even after the user closes the browser window. Advertisements known as 'pop-overs' appear and behave like pop-up windows, but in reality, they are shown in a new layer[112].

Pop-ups, etc., generally fall into three categories:

(i) those that show up when a user clicks on something on a webpage

(ii) those that show up at random

(iii) those that show up on their own without the user's input

Although the legality of displaying pop-ups on a website is still up for debate, there is no denying that pop-ups are incredibly bothersome to the majority of Internet users. A lot of ads feature trademarks or point to other websites with trademark displays. Furthermore, trademarks are frequently included in the programming code causing the appearance of customized ads. Pop-up ads do not display the mark of the website owner; instead, they overlay a rival trademark over the owner's website and trademark. Furthermore, pop-ups employ website URLs to launch pop-up ads; nevertheless, the courts are at odds over whether this kind of use constitutes trademark infringement or a 'pure machine-linking function' similar to a phone number[113]. Whether or not customers are likely to be confused about the adverts' source determines whether pop-up advertisements breach trademark rights. Plaintiffs should win their trademark infringement lawsuits to the extent that they can show pop-up ads are not simply bothersome but also likely to confuse consumers.

In the previous case, *the Washington Post. News Week Interactive Company, LLC, et al. v. The Gator Corporation*[114], the court granted a preliminary injunction, prohibiting defendant Gator Corporation (Gator)

---

[111] WIPO, at http://www. wipo.int/exportsites/www/copyright/en ecommerce/pdf/survey. Pdf. (last accessed on 22 April 2024).

[112] Joseph Tiffany and Robert B. Burlingame, *Trademarks on The Internet - Fair Play or Fair Game?* PILLSBURY LAW (Apr. 22, 2024) https://www.pillsburylaw.com/images/content/2/4/v2/2492/11F15.pdf.

[113] Id.

[114] Washington Post News Week Interactive Company, LLC, et al. v. The Gator Corporation C.A. No. 02-909-A (E.D. Va., July 12, 2002).

from inducing pop-up advertisements to show on a user's computer screen when the user is navigating any of the sixteen websites run by the news organizations that filed the lawsuit. The Gator software that was installed on the user's computer caused these adverts to show up. It appears that Gator's software monitors the user's online activities and presents ads on his computer that the defendant thinks the user will find interesting based on the user's previous online activity. The webpage that also appears on the user's screen is partially obscured when these ads show up. Gator did not obtain consent from the plaintiffs to display advertisements in this manner. The court determined that the plaintiffs would probably win their case that forcing pop-up ads to appear in this way violates their trademarks because the trademarks are located on the websites that the pop-up ads partially obscure. In light of this, the court granted a preliminary injunction prohibiting the defendant from carrying out this behaviour on the plaintiff's websites[115].

2.5 BRAND DILUTION AND COUNTERFEITING:

The internet has transformed trade, but it has also created opportunities for illicit actions that threaten trademarks. Two major concerns in this area are counterfeiting and brand dilution. Let's examine each of these ideas in more detail and see how they manifest in cyberspace.

Online marketplaces breed ground for counterfeit goods in various forms, such as deceptive websites that mimic the look and feel of legitimate brand websites, selling counterfeit products, third-party platforms like auction sites that unintentionally host counterfeit listings, and counterfeiters using social media platforms to advertise and sell their products. Counterfeiting is the creation and sale of imitation products that bear a substantial likeness to a registered trademark. These products are often of low quality and can be harmful to consumers[116].

Products that are produced and sold illegally in violation of a patent, trademark, copyright, or other intellectual property rights are known as counterfeits. Trade in counterfeit goods has the potential to harm businesses, impede economic growth, and change international competition[117]. It also presents a risk to public safety because it can produce goods that evade safety laws and regulations and support criminal activity.

For methodological reasons, mapping the quantity and dynamics of counterfeit goods in the economy is a challenging endeavour. However, it seems that the evidence that is now available indicates a significant and expanding trend in the trading of counterfeit goods. The most recent and thorough assessment states that counterfeit goods account for roughly 2.5% of all international trade, with the percentage in the European Union being twice as high at 5%. According to recent studies, counterfeiting is also increasingly happening for high-tech products including memory sticks, solid state drives, sound equipment, video games, and related items, moving beyond the traditionally targeted industries like cigarettes, watches, and clothing

[115] Supra note 95 at 31
[116] Manisha Singh and Puja Tiwari, *Tackling Illicit Trade: Smuggling and Counterfeiting, MONDAQ* (5 DECEMBER 2023), https://www.mondaq.com/india/trademark/1397688/tackling-illicit-trade-smuggling-and-counterfeiting
[117] Id.

(BSA, 2016). In fact, it was projected that the global trade in counterfeit goods within the ICT industries was valued at USD 143 billion in 2013, which equates to 6.5% of the industry's global commerce[118].

When a trademark is used without a license, even if it is not for counterfeit goods, its distinctiveness and value are reduced, and buyers are confused. Dilution of a trademark is especially challenging in the digital realm, as cybersquatters register domain names that are confusingly similar to registered trademarks and divert traffic. Dishonest websites employ trademarked terms as meta tags and keywords to rank better in search engine results, misinforming customers. Negative brand mentions, parodies, or unauthorized usage of trademarks on social media can lower the value of a trademark.

2.6 CONCLUSION

The emergence of the digital age has brought forth numerous challenges for trademark owners in protecting their intellectual property rights in cyberspace. While the internet has opened up new avenues for businesses and commerce, it has also created opportunities for trademark infringement, cybersquatting, and other forms of trademark misuse.

One of the primary challenges lies in the domain name system, where cybersquatters may register domain names containing well-known trademarks with the intent of profiting from them. Additionally, the classification and categorization of domain name disputes have become increasingly complex, requiring dedicated dispute resolution mechanisms.

Another significant challenge arises from search engine advertising and keyword advertising practices. The use of trademarks as keywords by competitors or unauthorized parties can lead to consumer confusion and potential trademark infringement issues. Furthermore, the proliferation of intrusive online advertising techniques, such as pop-ups and pop-unders, can dilute brand value and contribute to a negative user experience.

Brand dilution and counterfeiting pose substantial threats to trademark owners in the digital realm. The ease of creating and disseminating counterfeit goods online, coupled with the difficulty in detecting and enforcing against such activities, can severely undermine the integrity and value of legitimate brands.

To effectively address these challenges, trademark owners must proactively adopt a multifaceted approach. This includes actively monitoring and enforcing their rights, collaborating with online platforms and regulatory bodies, and employing legal measures when necessary. Ultimately, the substantive challenges of trademarks in cyberspace highlight the need for continuous adaptation and evolution of legal frameworks, technological solutions, and collaborative efforts among stakeholders. Effective protection of trademarks in the digital age is crucial for maintaining consumer trust, preserving brand equity, and fostering a fair and competitive online marketplace.

[118] Supra note 99 at 32

CHAPTER 3: PROCEDURAL CHALLENGES OF TRADEMARK IN CYBERSPACE

3.1 INTRODUCTORY:

Internet service providers are a brand-new industry that has formed as a result of the extraordinary growth in traffic and users that has occurred since the use of the Internet for business purposes was legalised. The Internet has expanded significantly since it was made available for commercial use because it offers businesses the ability to reach customers. In an attempt to realise the internet's immense potential, retailers, publishers, and entertainment providers are swarming to it. The World Wide Web's introduction in the 1990s marked a turning point in the development of e-commerce by offering a simple technological solution for a difficult task such as the publication and distribution of information, creation of online storefronts and e-commerce platforms, enabling businesses to establish an online presence and sell their offerings directly to customers. By facilitating communication and transactions between third parties, internet intermediaries offer the fundamental platform and infrastructure of the Internet. The internet has grown to such a large extent that it now permeates every facet of life and the economy[119].

E-commerce websites facilitate online transactions between customers and sellers, facilitating not just the sale of goods and services but also related transactions including supply chain management, payment processing, delivery, and service management. Great ease and a vast selection of products are available to customers with only a click because of the availability of e-commerce, which also gives micro sellers nationwide visibility and reach[120]. Legislators, citizens, and law enforcement may become concerned of these online players, including privacy and data protection, infringement on intellectual property rights, consumer protection, content regulation, taxation, and jurisdiction.

The liability of online intermediaries, including those acting on their behalf, for content that is distributed over the internet and that may violate someone's rights arising from a contractual obligation or criminal offences such as defamation, copyright infringement, fake advertisement, fraudulent misrepresentation, and many other offences. Internet intermediaries' responsibility is largely determined by their knowledge of and control over the material. Intermediaries, such as e-commerce platforms, can be held liable for trademark infringement if they do not meet certain conditions. Under the Information Technology Act 2000 in India, intermediaries must observe due diligence, not abet or induce unlawful acts, and remove or disable access to infringing content upon notice[121]. However, determining whether an e-commerce platform is merely an intermediary or is providing value-added services that give it knowledge of infringement is a matter for the courts to decide.

---

[119] Supra note 4 at 3.

[120] Digital Millennium Copyright Act, 1998, 512, 105th United States Congress.

[121] Mondaq, https://www.mondaq.com/india/trademark/873366/the-rise-of-e-commerce-and-intermediary-liability (last accessed on 1 May 2024).

The Direct Selling Guidelines in India are binding on e-commerce platforms and sellers, prohibiting the sale of products that infringe on intellectual property rights. Courts have found that even the sale of genuine goods without the brand owner's consent can constitute infringement if the condition of the goods is impaired[122].

In case of *Amway India Enterprises vs. Union of India*[123] The issue concerned claims that major online retailers like Amazon and Flipkart had tampered with the agreements between direct selling organizations and their independent sales people. One of the main questions investigated was whether or not e-commerce platforms had to follow the 2016 Direct Selling Guidelines and whether or not their activities violated trademarks. Finally, the case of Amway India Enterprises highlights how the dynamics of commerce are changing in the digital age and how important the legal system is to maintaining fair competition, consumer safety, and intellectual property protection. This case sheds light on the way toward an ethical, open, and safe online marketplace in India as business environments change.

Another problem of defamation in cyberspace became more and more prominent as the number of people using the internet grew, and as the network gradually spread to distant places, becoming a mass media and communication tool that could be found anywhere in the world[124]. Under the applicable provisions of the Indian Penal Code, the victim has the right to sue the accused party if a firm, blogger, or other third party posts a defamatory statement on a website. The Information Technology Act of 2000 established a 'notice and takedown' system[125].

Procedurally, brand owners face challenges in getting e-commerce platforms to temporarily freeze or suspend the accounts of sellers of counterfeit goods, as courts in India generally do not issue such orders. This is in contrast to practices in some other jurisdictions like the United States[126]. Even industrialized nations consistently struggle with the problems associated with selling counterfeit goods on online marketplaces. In the United States, brands usually apply for a temporary restraining order (TRO) to block the seller's earnings on e-commerce websites. They do this by claiming that if the order is not granted, the brand will incur irreversible harm and loss.

While the current framework requires e-commerce platforms to act in IP cases only after obtaining actual knowledge from the IP holders, a common counterargument is that these platforms ought to be forced to designate an investigative body to conduct a preliminary review of any infringing content uploaded on them. Since almost all intermediaries utilize technology to keep an eye on internet data, they can use that technology to monitor and, to a limited extent, analyze content that is supplied to their resources. While some e-commerce companies expressly state in their conditions of use that merchants are not permitted to

---

[122] Id.
[123] Amway India Enterprises v. Union of India (Uoi) And Anr. 182CTR(KER)297 (2003).
[124] J. Lakshmi Charan, *A Critical Analysis on Cyber Defamation in India: Laws and Issues in Present Scenario,* 2(6):192 (2023).
[125] The Information Technology Act of 2000, S79.
[126] SCC Times, https://www.scconline.com/blog/post/2023/05/25/implementation-of-ip-vis-vis-it-law-and-e-commerce-in-india/ (last accessed on 1 May 2024).

offer things that are stolen or counterfeit or to violate any patent, trade mark, or other property rights of a third party, but it is ground implementation is different.

3.2: PROCEDURAL CHALLENGES IN THE INDIAN RETAIL INDUSTRY

The objective of the Trademarks Act of 1999 recognizes the rights of registered trademark owners and aims to prevent fraudulent exploitation of their marks by unauthorized parties. The Supreme Court has established a test to determine continuous prior use in trademark-related cases to prevent such violations[127]. The court has observed that even small-scale use of the mark can establish priority, with the test being to determine the volume of sales or the degree of familiarity of the public with the mark. Bona fide marketing, promotional gifts, and experimental sales in small volumes can establish continuous prior use of the mark. Therefore, it is crucial to protect trademarks and prevent their misuse to maintain the credibility of the market and safeguard the rights of trademark owners[128].

In Uniply Industries Ltd. v. Unicorn Plywood Pvt. Ltd[129], the Supreme Court has established criteria for determining continuous previous use while granting temporary injunctions. It has been noted that many courts have indicated that even previous small-scale items bearing the mark are adequate to prove priority; the test is to ascertain the number of sales and the degree of public familiarity with the mark, as well as continuous prior users. To prove a consistent prior use of the mark, promotional gifts, small-scale experimental sales, and a legitimate test of marketing may be enough.

Online transactions between unconnected parties are facilitated by internet intermediaries. They either provide internet-based services to other parties or allow third parties to host, transfer, and index content, goods, and services that were developed by other parties.

3.2.1 Domain Name Conflicts and Cybersquatting

The inter-relationship between trademarks and cyberspace was developed in exclusive association with the concept of domain names[130]. In simple words, domain names represent the IP address used in surfing the World Wide Web.

'Cybersquatting' refers to the practice of registering domain names that are exact replicas of well-known trademarks or confusingly similar to them in an attempt to make a fortune on confusion. Due to the high expense and duration of domain name disputes, commercial establishments must take preventive actions such as keeping an eye on domain registrations, utilizing the Uniform Domain-Name Dispute-Resolution Policy (UDRP), and mailing cease-and-desist letters[131].

---

[127] Syed Mohiden v. P. Sulochana Bai CIVIL APPEAL NO.2758 (2015).
[128] PETER DRAHOS, A PHILOSOPHY OF INTELLECTUAL PROPERTY 45 (ANU, 2016).
[129] Uniply Industries Ltd. V Unicorn Plywood Pvt. Ltd 5 SCC 95 (2001).
[130] Mayuri and Subhasis, *Trademark Issues in Digital Era,* 13(2) JIPR. 118 (2008).
[131] Supra note 102 at 34.

Different forms of cybersquatting exist. Typo squatting is the most popular form of cybersquatting, in which a cybersquatter registers domain names that are variations of well-known trademarks. Typo squatters anticipate that users of the internet will type domain names incorrectly into their web browsers.

Typical instances of typosquatting include the following[132]:

i. the domain name wwwexample.com is missing the "."
ii. The intended website is sometimes misspelled as exemple.com
iii. An alternative domain name would be examples.com.
iv. Example.org is an alternative top-level domain.

Consequently, if a domain name is related to the provision of services and falls inside the purview of Section-2(z) of The Trade Marks Act, 1999[133], it may be licensed and protected as a trademark. All of the rights that are typically accorded to trademark owners in the Indian subcontinent will be conferred upon the trademark owner upon registration. Along with these rights, there will be the ability to take legal action for infringement and rights of action against any individual who passes off.

i. Right to file a lawsuit for infringement: The owner of a trademark would be the only one permitted to use it in connection with the goods or services for which it has been granted a license. They would also be entitled to file a lawsuit for infringement and demand compensation[134]. Section-29 of the Trade Marks Act, 1999 holds a person accountable for trademark infringement if they use a domain name that is licensed as a trademark without authorization and are not the trademark owner.
ii. Rights of action against anyone for passing off: If certain conditions are satisfied, an owner of a mark that is not registered as a trademark may also be entitled to trademark protection. The trademark owner should, first and foremost, cultivate goodwill or a reputation for his product. The trademark owner must also demonstrate that another party has misrepresented his products in a way that either deceives the relevant public or will deceive them in the future[135]. Lastly, the trademark owner must demonstrate that his goods and services have suffered a loss as a result of the defendant's goods and services being mistaken for the plaintiff's.

[132] Supra note 131 at 43.

[133] The Trade Marks Act, 1999 S.2(z):service means service of any description which is made available to potential users and includes the provision of services in connection with business of any industrial or commercial matters such as banking, communication, education, financing, insurance, chit funds, real estate, transport, storage, material treatment, processing, supply of electrical or other energy, boarding, lodging, entertainment, amusement, construction, repair, conveying of news or information and advertising

[134] The Trade Marks Act of 1999, S2(zb):trade mark" means 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.

[135] Reckitt and Colman Products Ltd. v. Borden Inc. and Ors., MANU/UKHL/0012/1990.

3.2 JURISDICTION:

The ability of a State to impose rules on its citizens behaviour through law, court decisions, and enforcement is known as jurisdiction. The only topic covered in this current Section is the adjudicative jurisdiction of courts that the state designates to settle disputes and determine parties' obligations.

Simply, cyber jurisdiction is the application of international jurisdictional principles to the digital realm. There are no real, national borders in cyberspace. It is a dynamic, exponentially expanding area that never stops. Any website can be accessed from anywhere in the world with just a single click of the mouse. Transactions with any of the websites would tie the user to the 'terms of service' agreements, privacy policies, and disclaimers that are included, subject to their respective domestic laws. Additionally, 'private international law' may be used as a remedy in the event of a dispute[136].

The Latin term 'juris-diction,' which means "*the saying or speaking of the law,*[137]*"* is where the word jurisdiction originates. It shows the significance, articulation, and validity. The territorial theory of state and sovereignty theory are the sources of the idea of a court's jurisdiction. A court's jurisdiction is defined as its ability to hear cases and decide disputes concerning people, property, and other subjects. The government's legislative branch makes laws, while its judicial or administrative branches carry out the task of enforcing those laws[138]. As a result, a state's application of jurisdiction principles cannot go beyond the bounds set by international law on its jurisdiction. The ability of a court to hear a case and decide a disagreement regarding a person, piece of property, or topic matter is known as jurisdiction. A State's constitution contains these jurisdictional principles as part of its jurisdictional sovereignty. All sovereign, independent states have jurisdiction over all individuals, objects, and causes, both civil and criminal.

Generally, there are three kinds of jurisdiction[139] i.e. Adjudicative, legislative, and enforcement jurisdiction. The ability of a State to establish normative guidelines for the control of its citizens is known as jurisdiction to legislate. When determining its jurisdiction over non-territorial bodies, the State must, nevertheless, take into account the limitations of international law. The State does not want to prescribe action for which there is no practical justification, hence its prescriptive power is not unrestricted.

In reality, the other State's sovereign sovereignty will be gravely threatened by an unrestricted prescription measure arsenal. International customary rules require a state to refrain from meddling in another state's internal or exterior affairs, under any circumstances.

i. General Jurisdiction: A person is subject to the authority of the relevant court on any potential cause of action under the 'general' jurisdiction. Historically, it has been predicated on the individual having extremely close ties to the state, either through physical presence in the state during the process of

---

[136] Supra note 112 at 37.
[137] Prof. Michael Geist*, Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L.J. 1345 (2001).
[138] John Tehranian, *Infringement Nation: Copyright Reform and the Law/Norm Gap,* Utah Law Rev 150, 537 (2007).
[139] Id at 138.

serving process, residency or domicile inside the state, or some other significant "continuous and systematic" interaction with the forum state.

ii. Particular Jurisdiction: The term 'specific' jurisdiction describes the authority of the relevant court to consider a specific cause of action in light of a certain set of 'minimum contacts' that the forum state has with respect to that cause of action.

iii. Subject Matter Jurisdiction: A court's capacity to consider and rule on a specific matter that comes before it.

iv. Original Jurisdiction: The power of a court to hear a case and make a decision before other courts have the competence to do so is known as original jurisdiction. Trial courts, for instance, frequently have original jurisdiction over cases.

v. European Personal Jurisdiction Approach: There are notable differences between the European and American approaches to personal jurisdiction in international issues. The Council of the European Union developed the "Brussels Regulation," which lays out the rules for determining whether country's courts have jurisdiction over a defendant[140]. This new rule updates the Brussels Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters, a 1968 convention among European nations.

vi. The Brussels Regulation lays forth the rules for jurisdiction and how they should be applied in an online setting. Subject to the rules of this Regulation, individuals who reside in a Contracting State may be sued in the courts of that State, regardless of their nationality. In addition, a resident of one Contracting State may be sued in a contract-related action in a court for the location where the relevant obligation is performed in a different Contracting State. Moreover, the domicile of a company, association, or partnership is its statutory seat, also referred to as its registered office, central administration, or principal place of operation. In reference to sales and promotions, the Regulation stipulates that the customer may file a lawsuit domestically if the trader conducts business in their home country or in any manner brings such business there.[141].

3.2.1 International:

Presently, not only the conventional laws but also the modern laws are deceived by the internet, the internet poses a challenge to the jurisdiction, the fundamental building block of any justice delivery system that grants a specific court the authority to hear a given case.

In the United States of America, precedents are necessary to comprehend how various courts have applied the traditional principles of jurisdiction such as personal jurisdiction, local state long-arm statutes,

[140] Council Regulation (EC) No 44/2001

[141] Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matter 1968 A. 2 *"Subject to the provisions of this Convention, persons domiciled in a Contracting State shall, whatever their nationality, be sued in the courts of that State. Persons who are not nationals of the State in which they are domiciled shall be governed by the rules of jurisdiction applicable to nationals of that State".*

and the due process clause of the US Constitution to resolve disputes pertaining to e-commerce. Due to their transitory nature, cybercrimes raise several challenging jurisdictional issues. Assume that a hacker using a computer in nation 'A', accesses a database in nation 'B', routes the data across multiple nations, and then initiates an event in nation 'C'. All claims against the defendant pertaining to issues connected to the forum state are decided by the courts under general jurisdiction[142]. US Constitution stipulates a minimal amount of communication between the forum state and a prospective defendant.

In Washington, v. The lex locus delicit[143]*,* or the rule that the site of injury is the place of suing, was followed in tort cases. However, with the Internet's ever-expanding limits, the defendant is now subject to universal jurisdiction in the cases[144].

The minimum contacts rule states that if the action is brought against a person in personam, the defendant must have minimal contact, and if the action is taken against a thing, the object in rem must have minimum contact. If a claim for jurisdiction is filed in rem, it can be supported by an email storage box or saved file on a computer server located inside the forum jurisdiction. The jurisdiction for minimum contacts has been established by consent and domicile. Nonetheless, the internet and the transactions made through it have no bearing on one's domicile. In order to determine if there are enough minimal contacts before a certain court to assert jurisdiction, the minimum contact test in internet transactions is satisfied by establishing the Internet-related actions, which are but certain electronic transmissions.

Consequently, electronic transmission into or other electronic linkages with the forum jurisdiction has been recognised by US courts as the foundation for jurisdiction. However, certain courts have determined that using an electronic network does not automatically subject a person to jurisdiction everywhere. In US, the critical question of whether personal jurisdiction extends to online acts is being discussed. The judiciary has stated that having a website does not establish the minimum contact necessary for jurisdiction to be exercised over it. Before the exercise of legitimate jurisdiction, other contacts in the forum state must also be established, as per *Hoarst Corpn. v. Goldberger*[145].

Additionally, an administrative panel is made up of one or three impartial individuals selected by the dispute resolution service provider. This panel is not connected to the registrars, the service provider, ICANN, or any other parties. Panelists with a track record of impartiality, discernment, and experience in fields including international trademark law, e-commerce, and Internet-related matters are available through the WIPO Center. The list is multinational, with more than 400 panelists from more than 50 countries[146]. The Administrative Panel is selected either by the response date or upon filing of the answer. Five days following the deadline for answer filing, a case with one panelist is scheduled. It often takes fifteen days in a panel of three.

---

[142] Supra 29 at 11.
[143] Washington, v. The lex locus delicit 93 W. Va. L. Rev. (1991).
[144] Dogan, S and Lenley, M 'Trademarks and Consumer Search Costs on the Internet'. Houston Law Review.
[145] Hoarst Corpn. v. Goldberger 1997 US Dist LEXIS 2065(SDNY).
[146] WIPO, https://www.wipo.int/amc/en/domains/panel.html (last accessed on 1 May 2024).

3.2.1.1 Jurisdiction based on Online Contract:

Terms of service and disclaimer provisions are common in online contracts. These agreements place limitations on the user's choice of forum and legislation. According to federal law, this norm is applicable whether the condition was negotiated between two business entities or whether it is part of a contract that a company offers to a customer with no further obligations. In *Bremen v. Zapata Off-Shore Co*[147]., the judicial view arrived at was that:

> "*such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be 'unreasonable' under the circumstances"*.

(i) Forum Selection Clauses: Click-trap Contracts: It is a wise legal measure to limit online service providers' exposure to a single jurisdiction. Filing lawsuits in several different places can be costly and annoying. As a result, the internet service provider is forced to abide by a single set of regulations and relevant legislation. The user must click an on-screen button that says 'I Agree,' 'I Accept,' or 'Yes' to accept the terms and conditions set forth by the service provider. According to the ruling in *Steven J. Caspi et al. v. The Microsoft Network, L.L.C., et al.*[148], the user had to click the 'I agree' button adjacent to a scrollable window that contained the terms of use to utilise Microsoft Network. By selecting the 'I agree' button to access Microsoft Network, each plaintiff consented to be bound by the terms of the subscriber agreement, resulting in the formation of a legally binding licence agreement, In this case, the Microsoft Network subscriber agreements forum selection clause was deemed to be legitimate and enforceable by the Superior Court of New Jersey.

(ii) Jurisdiction based on Location of a Web Server: The forum state may be required to exercise its jurisdiction over the defendant if it is claimed that the defendant uses its website hosted by a service provider whose IT infrastructure is located in the forum state. The plaintiff filed a defamation lawsuit in a California court in *Jewish Defence Organisation, Inc. v. Superior Court*[149]. The defendant's sole business dealings with California were related to agreements they had with ISPs 'based in California' to host a website they managed from their New York home. The defendant's computerised contracts with Internet service providers who might be California firms or might have offices or databases in California were found to be insufficient by the court to qualify as a purposeful ailment.

3.2.1.2 Anti cybersquatting Consumer Protection Act:

Anti Cybersquatting Consumer Protection Act (ACPA) 1999 is a U.S. law that addresses cybersquatting specifically. Cybersquatting is the malicious practice of registering domain names that are confusingly close to or identical to trademarks to make money off of them. The ACPA provides trademark owners with legal recourse against cybersquatters[150]. A court may order the infringement domain name to be either transferred

[147] Bremen v. Zapata Off-Shore Co 407 U.S. 1 (1972)
[148] Steven J. Caspi et al. v. The Microsoft Network, L.L.C 732 A.2d 528 (1999)
[149] Jewish Defence Organisation, Inc. v. Superior Court 72 Cal.App.4th 1045, 85
[150] Anti Cybersquatting Consumer Protection Act 1999 15 U.S.C. § 1129.

to the legally owned trademark or forfeited if the ACPA is found to have been broken[151]. Cybersquatting was a serious issue before the ACPA, Cybersquatters may register domain names that contain well-known trademarks and then either park the domain name with advertisements from the trademark's competitors, sell the domain name to the trademark owner for a large price, or redirect people to irrelevant, possibly malware-filled websites.

The ACPA prohibits registering, trafficking in, or using a domain name that is:

i. Identical to a trademark
ii. Confusingly similar to a trademark
iii. Dilutive of a famous trademark

The ACPA aimed to:

i. Deter cybersquatting through legal consequences.
ii. Protect consumers from confusion and potentially harmful websites
iii. Promote the growth of e-commerce by ensuring a fair and predictable online marketplace

Congress created the ACPA in 1999 after realizing that cybersquatting causes consumer fraud, public confusion, hinders e-commerce, robs legitimate trademark owners of income and goodwill, and burdens trademark owners. Cybersquatting had no obvious disincentive prior to the ACPA. Although the Federal Trademark Dilution Act proved to be an effective tool in combating cybersquatters, Congress felt that further legislation was required. As a result, the ACPA was passed into law in November 1999, making it unlawful to register, use, or traffic in another person's domain name if it is a well-known or distinctive mark or confusingly similar to one.[152]. A limited immunity from liability is offered to domain name registrars who suspend, cancel, or transfer domain names in response to a court order or in the course of enforcing a lawful policy that forbids cybersquatting.

In February 2000, the Court of Appeals for the Second Circuit became the first appellate court to apply and interpret the ACPA in *Sporty's Farm L.L.C. v. Sportsman's Market, Inc*[153].Sportsmen first used the "sporty" emblem in the 1960s, and in 1985, they filed 'Sporty's' trademark application with the U.S. Patent and Trademark Office. 'Sportys.com' is the domain name that Omega registered. The co-owner of Omega was familiar with the 'Sporty's' trademark. 'Sporty's Farm', an entirely-owned subsidiary of Omega, purchased the domain name. 'Sporty's Farm' filed a lawsuit to keep using Sportys.com after Sportsman's reported the registration of Sportys.com in 1996. Under the Federal Trademark Dilution Act (FTDA), Sportsman's counterclaimed for trademark infringement and dilution. As a result of the district court's ruling that Sporty's Farm had violated the FTDA, Sporty' Farm was ordered to give up all rights to Sportys.com. The ACPA was passed while the appeal was underway; the court of appeals applied the Act, holding that the statute in effect at the time of the appeal is the one that should be followed. The Court had to first decide if 'Sporty's' is a distinctive or well-known brand before applying the ACPA.

[151] Sen. Rp. 106-1410, at 5 (1999).
[152] Id.
[153] Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489 (2000)

According to the court, it is both. Next, the Court had to determine if the domain name "Sportys.com" was the same as the 'Sporty's' mark or confusingly similar. According to the judge, they are very similar. The court's next task was to ascertain whether there was a bad faith intent to benefit.[154]. The *Sporty's Farm L.L.C. v. Sportsman's Market, Inc. case* played a pivotal role in shaping the early jurisprudence surrounding the ACPA and its application to domain name disputes involving trademark infringement and cybersquatting. It guided key factors such as trademark distinctiveness, confusing similarity, and bad faith intent, which have become essential considerations in subsequent cases dealing with the emergence of trademark rights in the digital realm.

3.2.1.3 WIPO Joint Recommendation

The primary international framework for the protection of trademarks in cyberspace is the WIPO (World Intellectual Property Organization) Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, adopted in 2001[155].

This Joint Recommendation provides guidelines and principles for member countries to establish legal frameworks for the protection of trademarks and other industrial property rights in the context of the internet and domain names. It covers various aspects, as follows:

1. Use of trademarks on the Internet- The recommendation affirms that the use of a sign on the internet constitutes use in commerce and should be protected as such under trademark laws.

2. Domain name registration and dispute resolution- It suggests establishing administrative dispute resolution procedures for resolving disputes related to abusive registration and use of domain names that infringe on trademarks.

3. Licensing and assignment of trademarks- The recommendation provides guidelines for the licensing and assignment of trademarks concerning their use on the internet.

4. Liability of online service providers- It addresses the issue of liability of online service providers for trademark infringement by their subscribers or users.

While the WIPO Joint Recommendation is not a binding treaty, it serves as an influential framework for member countries to develop or update their national laws and policies regarding trademark protection in cyberspace. Additionally, the WIPO Internet Domain Name Process (1998-2001) led to the establishment of the Uniform Domain Name Dispute Resolution Policy (UDRP), which is an important mechanism for resolving disputes related to the abusive registration and use of domain names that infringe on trademarks[156]. Other international agreements, such as the Paris Convention for the Protection of Industrial Property and the TRIPS Agreement, while not specific to cyberspace, also provide principles and minimum standards for the protection of trademarks that are relevant in the digital context[157].

---

[154] Aaron L. Melville, *New Cybersquatting Law Brings Mixed Reactions from Trademark Owners*, 6 B.U. J. Sci. and Tech. L. 13 (2000).

[155] WIPO, https://www.wipo.int/edocs/pubdocs/en/wipo-pub-1081-1-en-introduction-to-the-international-intellectual-property-legal-framework.pdf (last accessed on April 23, 2024)

[156] Supra note 45 at 17.

[157] Id.

The laws pertaining to search engine advertising and trademark infringement are constantly changing. The trademark laws in the United States and the United Kingdom direct the respective courts when they decide matters involving trademark infringement.

> *"To secure to the business community the advantages of reputation and goodwill by preventing their diversion from those who have created them to those who have not*[158]"

It was one of the initial goals of the Lanham Act 1946. These kinds of 'bait and switch tactics,' even when they are carried out via a search engine, are definitely attempts to capitalize on the trademark of another person. Even when a search engine is used as a middleman, diversion of a trademark's goodwill should be prosecuted as trademark infringement.

The most significant decisions clarifies the legal status of search engine advertising with respect to trademark law. The defendants in *Playboy Enterprises, Inc. v. Netscape Communications Corporation*[159] offered banner advertising on its search engine pages that were targeted to particular terms. Netscape mandated that ads pertaining to pornographic content must be connected to a list of more than 400 phrases, such as 'Playboy' and 'Playmate', which are trademarks held by the plaintiff. Consequently, if someone entered 'Playboy' or 'Playmate' as a search keyword, these other companies adult banner advertisements would appear on the search results page.

Because the defendant would receive payment from the advertisers for each click-through, regardless of whether the clicks were performed by inexperienced Web users, he personally benefited from this uncertainty. The Playboy court reversed the lower court's award of summary judgment and remanded the case for further hearings because of significant questions of material fact about possible trademark infringement resulting from Netscape's use of Playboy's trademarks. In rendering its decision, the Court pointed out that the primary problem with Netscape's keyword targeting of Playboy's trademarks in banner ads was that Netscape made money off of the initial confusion users experienced when they clicked on these banner ads, mistakenly thinking they were sponsored by Playboy, thus taking advantage of Playboy's goodwill.[160].

Along these lines, the Court noted that had the banner ads been clearly identified its source or, even better, overtly compared to Playboy's products to the sponsor's own, no confusion would occur. Perhaps as a result of the court's insightful remarks, popular websites like Google, Yahoo, and others now prominently display a notice next to each of their "sponsored" links. For example, sponsored links appear at the top of search results on Yahoo.com in a darkened Section designated as such, or they appear along the right side of the results page as "sponsored links." It is argued, therefore, that even while these adverts are identified as "sponsored" in the search engine results, there is still a chance of confusion because the trademarked phrase is used in the context of the search engine[161].

---

[158] Robert G. Bone, *Hunting Goodwill: A History of The Concept Of Goodwill In Trademark Law,* Boston Univ. J, 548, 595 (2006).
[159] Playboy Enterprises, Inc. v. Netscape Communications Corp., 354 F.3d 1020.
[160] Supra note 39 at 15
[161] Id.

Through changes and judicial outreach, several nations, including India, have attempted to broaden the application of classical trademark law to the Internet sphere. Nevertheless, the United States of America has taken the lead in resolving domain name conflicts by appropriately proposing new laws and broadening the scope of already-existing ones through judicial activism. The rise of cyber jurisprudence in the international arena can be attributed in large part to the courts in the United States and the United Kingdom.

The Lanham Act 1946, which among other things forbids a variety of actions such as trademark infringement, trademark dilution, and false advertising, has been the most significant piece of legislation pertaining to trademark infringement in the United States. Three main legal avenues are available to trademark owners under the Lanham Act to defend their rights[162]:

(1) trademark infringement- "Trademark infringement occurs when a third party uses a mark that is confusingly similar to a registered trademark in a manner that is likely to cause consumer confusion". The trademark owner can pursue legal action against the infringer to prevent unauthorized use of the mark and seek remedies such as injunctive relief and monetary damages.

(2) unfair competition- The unfair competition provisions of the Lanham Act protect against false or misleading representations that are likely to cause confusion, deception, or misrepresentation about the origin, sponsorship, or approval of goods or services. Unfair competition claims can be brought against parties engaged in practices that create consumer confusion or unfairly compete with the trademark owner's products or services.

(3) dilution- It provides protection against trademark dilution, which occurs when a third party's use of a mark, even without causing consumer confusion, lessens the capacity of a famous mark to identify and distinguish goods or services

Traditionally, trademark infringement cases are resolved by using the 'likelihood of confusion' test, which was created by the courts. This test requires examining the case's facts from several angles. These variables include:

i. Mark strength
ii. Product proximity
iii. Mark resemblance
iv. Real confusion evidence
v. Potential for gap closure
vi. Customer sophistication
vii. Good faith on the side of the purported infringer.

Nonetheless, the Lanham Act of 1946 permits the use of a trademark more than once as long as it is not utilized in the same market and there is no likelihood of confusion of products[163]. By providing these legal avenues, the Lanham Act 1946 allows trademark owners to safeguard their valuable intellectual property

[162] LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/lanham_act, (last accessed on April 20, 2024)
[163] Id.

rights and prevent unauthorized parties from capitalizing on the goodwill and reputation associated with their trademarks

3.2.2 NATIONAL

The ability of a court to resolve a dispute is known as jurisdiction. The topic, financial stakes, and local boundaries all play a role in the Court's decision-making process. The territorial connection between the defendant and the cause of action typically determines the court's jurisdiction.[164]. The competence of the Court in matters pertaining to both national and foreign concerns is incorporated into the Code of Criminal Procedure and Civil Procedure in India. The Code of Civil Procedure, 1908, contains the general jurisdiction laws for India. The Code of Civil Procedure, 1908, Sections 16 through 18 of Code of Civil Procedure, 1908, contains special jurisdiction regulations pertaining to moveable and immovable property.[165]. The lex situs rule-the law of the forum in where the property is situated-predominates in the case of immovable property, whereas the jurisdictional rule in the case of moveable property is primarily defendant-centric. The international jurisdiction is covered under Section-20 of the Code of Civil Procedure, 1908, which has been interpreted in instances involving the internet.

3.2.2.1 Authority under the Information Technology Act 2000:

The Information Technology Act of 2000, is the main source of cyber law in India. Its goals are to enable the preservation of electronic documents with the government and to give legal status to e-commerce. The prescriptive jurisdiction of the State is primarily reflected in its legislative enactments. For instance, the IT Act, 2000 establishes prescriptive jurisdiction by stating that

> "*The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality*[166]."

Furthermore, this Act covers any person who commits an offense or violation outside of India if the action or act that constitutes the offense or violation makes use of an Indian computer, computer system, or computer network. Enacting laws is the legislative duty of the government; enforcing such laws is the judicial and/or administrative function.

The Indian Information Technology Act 2000, which punishes a variety of cybercrimes and imposes severe penalties, incorporates the effect test of jurisdiction under Sections-1(2) and 75 of Indian Information Technology Act 2000. As a result, certain provisions of the Act confer jurisdiction upon courts to try cases pertaining to cybercrimes both inside and outside of India. The IT Act contains the following provisions:

---

[164] Live Law, https://www.livelaw.in/law-firms/articles/concept-of-jurisdiction-173713 (last accessed on 29 April 2024).
[165] Code of Civil Procedure, 1908 S 14-18.
[166] The Information Technology Act, 2000 S75: Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Section-1 of Indian Information Technology Act 2000 describes the extent to which the legislation is applicable, saying that: It shall apply to the whole of India, unless this legislation specifies otherwise; it also applies to any offence or violation thereunder committed by any person outside of India[167].

Section-75 of Indian Information Technology Act 2000discusses the provisions of the Act that are applicable to crimes or offenses committed outside of India. For the purposes of the Indian Information Technology Act 2000, sub-section (1) shall apply to any offense or violation committed by an individual outside of India if the behavior or act in question includes a computer, computer system, or computer network situated in India. It further specifies that the provisions of this act shall apply to any offense or violation committed outside of India by any individual, regardless of his nationality, subject to the provisions of sub-section -[168].

Section-46 of the Indian Information Technology Act 2000 confers the power to make decisions in situations where any of its provisions are broken on the Cyber Appellate Tribunal. In order to do this, the Act calls for the appointment of an adjudicating officer with the same authority as civil courts.[169]. Section 48 calls for the creation of a Cyber Appellate Tribunal: The Cyber Regulations Appellate Tribunal will be the name of one or more appellate tribunals that the Central Government will create by notification.

Section-61of Indian Information Technology Act 2000indicates that civil courts have no jurisdiction over any matter that an adjudicating officer or the Cyber Appellate Tribunal is authorized to determine under this Act. This means that no civil court shall have jurisdiction to entertain any suit or proceeding in relation to any matter that a court may grant an injunction in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.[170].

Section-62 of Indian Information Technology Act 2000 talks about the High Court's Appeal. Within sixty days after the day the judgment or order was conveyed, anyone who believes they have been mistreated by a Cyber Appellate Tribunal decision or order may initiate an appeal with the High Court. Any factual or legal question emerging from the order may be the subject of the appeal, and the High Court may allow it to be filed within an extra sixty days if it determines that there is sufficient justification to keep the petitioner from making the appeal within the allowed time frame.[171].

The Information Technology Act of 2000 appears comprehensive in terms of resolving disputes involving Indian citizens and offences or violations committed in India, as Indian courts operate under the doctrine of lex foris, which translates to ‘the law of the land.’ However, it still causes ambiguity

[167] The Information Technology Act, 2000 S 1
[168] Supra note 2 at 9
[169] The Information Technology Act, 2000 S 46
[170] The Information Technology Act, 2000 S 76: Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation.
[171] The Information Technology Act, 2000 S 62: Any person aggrieved by any decision or order of the 1 [Appellate Tribunal] may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the 1 [Appellate Tribunal] to him on any question of fact or law arising out of such order: Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

when attempting to exercise extraterritorial jurisdiction over offences committed outside of India or by non-citizens. For example, if an American citizen defamed an Indian politician by posting obscene remarks on social media, and the enraged party sought redress from an Indian court.

The above instance indicates that Section-79 of the IT Act 2000 provides some immunity to ISPs from liability for third-party content hosted on their platforms, as long as certain conditions are met. This means that even if an American citizen posts defamatory content about an Indian politician on social media, the ISP hosting the content may not be held directly liable unless it can be proven that the ISP conspired, abetted or aided in the unlawful act. The search results also highlight that while the individual who posted the defamatory content can be held liable for cyber defamation, the people who shared or re-posted the content can also be held liable. However, the legal recourse against the ISP itself may be limited due to the provisions in Section-79 of Indian Information Technology Act 2000[172].

This demonstrates a loophole in cyber laws, as it can be challenging to hold the ISP accountable for defamatory content posted by users, even if the content causes harm to the reputation of an individual. The search results suggest that addressing this loophole and clarifying the liability of ISPs in such cases could be an area for improvement in India's cyber laws.

The ITA (Information Technology Act, 2000) and ITAA (Information Technology Amendment Act, 2008), which introduced significant changes and amendments to the existing IT Act, enhancing provisions related to cyber-crimes, data privacy, electronic signatures, and other aspects of cyber law in India, do not adequately address jurisdiction, a major issue. Sections 46, 48, 57, and 61 of the IT Act, 2000 discuss jurisdiction in relation to the adjudication process and the appellate procedure associated with it. Section 80 of the Indian Information Technology Act, 2000 also mentions jurisdiction in relation to police officers' rights to enter and search public spaces for evidence of cybercrime, among other things. Although extraterritorial jurisdiction is clearly provided by the IT Act, 2000, the question remains as to how effectively an American citizen may be brought to India for a cyber defamation trial given that the American citizen is not covered by the Act.

3.2.2.2 Criminal Procedure Code 1973:

Section-1(2) of the Information Technology Act 2000 discusses the idea of the Act's extraterritorial application, stating that it covers the entirety of India and any offense or violation committed by anyone outside of the country. According to the interpretation of the aforementioned clause, the offender's country has no bearing on whether the IT Act is applied. The jurisdictional problem in cases of cybercrimes in India is resolved by the Information Technology Act 2000 and the Criminal Procedure Code.

Section-75 Criminal Procedure Code 1973 explains further that the jurisdiction is applicable to any offense or violation committed outside of India by any individual, regardless of nationality, as long as the

[172] Live Law, https://www.livelaw.in/columns/cyber-defamation-libel-slander-section-79-it-act-internet-cyberspace-social-media-205264 (last accessed on 1 May 2024).

act involves a computer, computer system, or computer network that is located in India. As a result, the court's jurisdiction is now recognized under the impact principle of jurisdiction. Additionally, the authority of the Court is covered by Sections 177 to 189 of the Criminal Procedure Code 1973. According to Section 177 of the Criminal Procedure Code of 1973, the court whose local jurisdiction the offense was committed will try the defendant. According to Section 178, a court with jurisdiction over any of these local areas may hold a trial if the offense is ongoing or divided into separate territories. The Criminal Procedure Code of 1973, Section 179, establishes the idea that the court has jurisdiction in cases where an offense is committed or consequences have been incurred.

The Criminal Procedure Code of 1973 includes the nationality concept of jurisdiction in Section-188 of the act, which states that an offence committed by an Indian citizen outside of the country is subject to Indian court jurisdiction. It is significant to remember that any court with local jurisdiction over the messages in question must hear a case involving deception by means of telecommunication under Section 182 of the Criminal Procedure Code 1973. Even if the criminal lives within the jurisdiction but commits the crime outside of it, the regional court where he dwells has the authority to investigate the offense as though it were done there. Section 179 of the Criminal Procedure Code 1973 addresses the penalty for offenses committed in Indian territory. Even so, an offence committed overseas by an Indian citizen is susceptible to Indian court jurisdiction, as stated in Section 188 of the CrPC 1973.

These provisions in the IT Act 2000 and the CrPC establish a comprehensive framework for determining the jurisdiction of Indian courts in cybercrime cases, taking into account various principles such as the effect principle, nationality principle, territorial jurisdiction, and residency principle. This approach aims to ensure effective enforcement and adjudication of cybercrime offenses, regardless of the location of the offender or the computer systems involved.

3.2.2.3 Authority under the Indian Penal Code 1860:

The IPC is considered a monumental legal achievement and a testament to the codification efforts of the British colonial administration in India. It continues to serve as the foundation for criminal jurisprudence in India, ensuring a consistent and unified approach to defining and prosecuting criminal offenses across the country.

- Section-3 of Indian Penal Code 1860: Penalties for offences committed outside India but that the law permits to be tried within the country. Any individual subject to a trial under any [Indian law] for an offence committed outside the country will be dealt with under the guidelines of this Code for any act outside the country in the same way as if it had been committed inside the country[173].

[173] Indian penal code 1860 S 3 *"Any person liable, by any [Indian law], to be tried for an offence committed beyond [India] shall be dealt with according to the provisions of this Code for any act committed beyond [India] in the same manner as if such act had been committed within [India]".*

- Section-4 of Indian Penal Code 1860: Code Extension to Extraterritorial Offences - This Code's provisions also extend to any offence committed by any of the following: (1) Indian citizens abroad; (2) individuals on ships or aircraft registered in India, wherever they may be; and (3) anyone abroad who commits an offence directed at an Indian computer resource[174].

While there is currently no Universal Convention on Extradition—in the event that one does not exist, extradition between States is facilitated by bilateral agreement—the conversation indicates that the Criminal Procedure Code and the Information Technology Act address jurisdiction issues in great detail. When an out-of-state offender commits cybercrime that affects the local court's territory, the court's jurisdiction is ineffective until the offender is no longer under the purview of any local court.

3.2.3 India and The Global Agreement on Cyber Jurisdiction:

On November 23, 2001, the Council of Europe signed the Budapest Convention on Cybercrime, which is also known as the Convention on Cybercrime, in Strasbourg, France, Canada, Japan, the Philippines, South Africa, and the United States. India has been reassessing its position on the convention since 2018, even though several nations, like Brazil and India, declined to adopt it because they were not involved in its preparation.[175]. The Convention on Cybercrime is the first international treaty that addresses cybercrime and the Internet by taking into account national laws, enhancing international cooperation, and improving investigative techniques.It was the first global agreement on crimes perpetrated against or with the help of computer networks, including the Internet. The Convention's primary objective is to pursue:

> *"a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation[176]."*

It focuses on offenses like copyright infringement, fraud using computers, child pornography, and security-related offenses. It also includes a number of procedural authorities, including the ability to search and intercept content on computer networks.

According to Article-22 of the Convention on Cybercrime, 2001[177], A nation may assert its jurisdiction over a cybercrime perpetrated on its soil, by a national, on a ship flying its flag, on an aircraft registered under its laws, or if the offense is punishable by local criminal law or outside the territorial jurisdiction of any State. Although the Indian government might yet grant extradition, however, as it was held in *Rambabu Saxena v. State*[178] that :

> *"if the treaty does not enlist a particular offence for which extradition was sought, but authorises the Indian government to grant extradition for some additional offences by inserting a general clause to this effect, extradition may still be granted."*

The Convention on Cybercrime provides guidelines for countries to exercise jurisdiction over cybercrimes committed within their territory, by their nationals, or in certain other circumstances. However, as per the

[174] Indian penal code 1860 S 4.
[175] Law Docs, https://lawdocs.in/blog/understanding-jurisdictional-issues-in-cyberspace, (last accessed on 30 April 2024).
[176] Conseil De L'Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention (last accessed on 30 April 2024).
[177] Convention on Cybercrime, art. 22, Nov. 23, 2001, CoE.2004
[178] Rambabu Saxena v. State AIR 1950 SC 155

Indian Supreme Court's decision in Rambabu Saxena v. State, even if an offense is not specifically listed in an extradition treaty, the Indian government may still grant extradition if the treaty contains a general clause allowing extradition for additional offenses.

3.3 NATIONAL FRAMEWORK

India has developed a national framework to address the protection of trademarks in cyberspace through various legal provisions, policies, and court decisions. Indian national framework for trademark protection in cyberspace:

i. The National Internet Exchange of India (NIXI): NIXI is in charge of the ICANN, and has given India a.in ccTLD. On July 19, 2003, the Department of Information Technology (DIT) in collaboration with the Internet Service Providers Association of India (ISPAI) launched NIXI[179], a not-for-profit company created under Section-25 of the Companies Act, 1956, on behalf of the Government of India. The main goal of NIXI's establishment was to provide a framework for Internet service providers (ISPs) to peer with one another in order to route local traffic within the nation rather than sending it all the way to other nations, such as the USA. This will contribute to obtaining improved service quality by lowering latency and bandwidth costs for Internet Service Providers (ISPs) by saving on International Bandwidth.

ii. Trademarks Act, 1999: The Trademarks Act, of 1999, along with subsequent amendments, forms the primary legal framework for trademark protection in India, including provisions relevant to the online context.

Section-29 of The Trademarks Act, of 1999 prohibits the use of a registered trademark in the course of trade in a manner that renders it likely to cause confusion or deception[180].

iii. Domain name dispute resolution policy: India has adopted the Uniform Domain Name Dispute Resolution Policy (UDRP) established by ICANN for resolving disputes related to the abusive registration and use of domain names that infringe on trademarks. The .in Domain Name Dispute Resolution Policy (INDRP) governs disputes involving .in domain names[181].

iv. Guidelines and practices of the Trademark Registry: The Indian Trademark Registry has issued guidelines and established practices for examining and registering trademarks intended for use on the internet and in e-commerce. The Registry considers the use of a trademark on a website or in online advertising as valid use for the purpose of registration and maintenance[182].

v. Industry self-regulation and best practices: Various industry associations and stakeholders have developed self-regulatory frameworks, codes of conduct, and best practices for the use of trademarks

[179] National Internet Exchange of India, https://nixi.in/ (last accessed on April 20, 2024)
[180] INDIAN KANOON, https://indiankanoon.org/doc/1005493/, (last accessed on April 20, 2024).
[181] INTELLECTUAL ASSET MANAGEMENT, https://www.iam-media.com/article/securing-domain-name-protection-in-india, (last accessed on April 20, 2024).
[182] Id.

in e-commerce and online advertising, complementing the legal framework. While the Indian national framework for trademark protection in cyberspace continues to evolve, it provides a combination of statutory provisions, dispute resolution mechanisms, administrative guidelines, court decisions, and industry self-regulation to address the challenges posed by the use of trademarks in the digital environment.

Unlike many developed countries, in India, we have no Separate Domain Name Protection Law, and cybersquatting cases are decided and dealt with under the Trade Mark Act, of 1999. The Hon'ble Supreme Court in *Satyam Infoway Ltd vs Sifynet Solutions Pvt. Ltd*.[183] had observed that:

> "*As far as India is concerned, there is no legislation which explicitly refers to dispute resolution in connection with domain names. But although the operation of the Trade Marks Act, 1999 itself is not extraterritorial and may not allow for adequate protection of domain names, this does not mean that domain names are not to be legally protected to the extent possible under the laws relating to passing off*".

3.3 JUDICIAL APPROACH: INDIA AND USA

The court used the USA Court's effect test in the case of *India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc and Ors*[184]. The dispute relates to the March 2004 debut of the well-known TV network 'INDIA TV.' The plaintiff claims that the mark was adopted on December 1, 2002, and on January 22, 2004, they submitted an application for registration of the same mark. Without any complaints, the mark was released in 2006 within the stipulated time frame. After discovering the website through an internet search, the plaintiff sued the defendant, requesting a permanent injunction to prevent the defendant from using the mark. The defendant said that they were American entities and neither lived nor worked for profit in India, casting doubt on the court's jurisdiction.

In addition, in the case of *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*[185], the defendants were from Hyderabad, and the plaintiff company was in the hospitality industry. The defendants adopted the mark 'Banyan Tree' and used it as a device and maintained a website since 1996. However, the defendants did not have a registered mark in the state of the land because their application was pending. The defendants started the project under the name 'Banyan Tree Retreat' and advertised it online. The plaintiff filed a case in Delhi High Court, accusing the defendant of being dishonest. The court raised some significant questions and responded to them by using the jurisdiction rules of the US court.

In the *Hakam Singh v. Gammo (India) Ltd*[186]. case, the court established two crucial requirements for the use of autonomy to determine the court's jurisdiction.

---

[183] Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd, 2004 (3) AWC 2366 SC.

[184] India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc and Ors MIPR2007(2)396, 2007(35)PTC177(DEL)

[185] Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy CS OS. NO. 894/2008

[186] Super Cassettes Industries ltd. v. Myspace Inc. and others AIR 1971 SUPREME COURT 740

1) First, inherent jurisdiction should be granted to the court chosen by consensus.
2) Second, more than one court should have jurisdiction to implement the forum agreement; however, if the parties have not chosen or applied their autonomy with regard to the court's jurisdiction, jurisdiction may be determined based on the 'cause of action,' which appears in the following contexts:
   i. The location where the contract was formed, or the place where it was entered;
   ii. The site of performance, which is the location where the contract is carried out or must be carried out in accordance with its conditions;
   iii. The location where the decision is made.

The US Supreme Court established the effects test, also known as the Calder Effect Test, in *Calder v. Jones*[187],stating that jurisdiction may be based on the defendant's deliberate actions outside the forum state that are intended to harm the plaintiff inside the forum state. The defendant's knowledge that his actions would harm the plaintiff in the forum state, where the plaintiff corporation had its major place of business, satisfied the criteria of purposeful availability, and this test was applied to online behavior, which was sufficient to establish jurisdiction. *Zippo Manufacturing Co. v. Zippo.Com Inc.*[188] comprehensively and The sliding scale approach is stated formally. The effects test is utilized in addition to sliding scale theory to determine jurisdiction. The sliding-scale theory is more useful in resolving disputes primarily pertaining to economic activity, copyright or trademark infringements, or intellectual property issues than the effects test, which is more advantageous in criminal instances.

According to the ruling in *Ballard v. Savage*[189], The following points can be proven by the plaintiff in order to meet the burden of proof. By claiming the benefits and protections of the forum state's legislation, the defendant purposefully exploited the right to conduct business in the forum state;

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra [190]is India's first case of online defamation. When the defendant worked for the plaintiff's company, he would send derogatory, pornographic, vulgar, and abusive emails to his employers and the company's many international branches. The emails were sent with the intention of harming the company's and its managing director's reputation on a worldwide scale. When it came to communications that defame company names, the Delhi High Court exercised its authority and issued an ex parte injunction. In *SIL Import v. Exim Aides Silk Importers*[191], the court adjudicated:

> *"Necessity for the judiciary to interpret the statute in light of recent technological advancements. In the absence of specific legislation pertaining to Indian courts jurisdiction over Internet disputes, or unless India is a signatory to an international treaty that specifies the national courts jurisdiction and the conditions under which it can be exercised, Indian*

[187] Calder v. Jones, 465 U.S. 783 (1984)
[188] Zippo Manufacturing Co. v. Zippo.Com Inc. 952 F supp 1119(WD Pa 1997).
[189] Ballard v. Savage 65 F.3d 1495 (9th Cir. 1995).
[190] SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra 1279/2001.
[191] SIL Import v. Exim Aides Silk Importers (1999) 4 SCC 567.

courts will be required to interpret the existing statutes broadly in order to resolve Internet disputes".

3.4 International Registration of Trademarks

i. The Madrid Agreement Concerning the International Registration of Marks: It was the first attempt to create an international system for expediting trademark registration in numerous countries worldwide. It was concluded in 1891 and went into force in 1892. It modifies the geographical scope of trademark laws and makes it possible to file, register, and preserve trademark rights internationally across numerous nations.[192].

ii. Trademark Law Treaty: The Trademark Law Treaty was adopted on October 27, 1994, during a diplomatic conference in Geneva. It went into effect on August 1, 1996, and its main goal is to streamline and harmonize the administrative processes related to national applications and mark protection without addressing the substantive aspects of trademark law that deal with mark registration. The World Intellectual Property Organization (WIPO), situated in Geneva, Switzerland, is also responsible for overseeing the Trademark Law Treaty. Additionally, as of 2024, there are 51 signatories in total (one intergovernmental body and 50 states)[193].

3.5 CONCLUSION:

The internet, with its multitude of features and services, Online intermediaries are contributing significantly to the advancement of technology and the growth of the online environment. Online intermediaries' regulated activities shouldn't be implemented in a confusing or constrictive manner. Any advancement could be hampered by this legislation, which would prevent middlemen from developing additional facilities. However, it's also important to consider the possibility that the services offered by internet middlemen could be used illegally. Lawmakers continue to ignore these issues, which somewhat halts the advancement of technology. It is clear that this industry needs regulation immediately, and any new laws should include the interests of all parties involved, including the users and owners of rights of intermediaries. In order to prevent an atmosphere of ambiguity and arbitrariness, it is imperative that newly emerging online intermediary activities be regulated through the establishment of explicit norms or rules. A detailed investigation into the criminal responsibility of the different players on the internet in India forces the conclusion that the law's hold over it is still shaky.

Addressing the question of state and judicial jurisdiction is the first step towards controlling the internet. Traditional ideas of jurisdiction from the State's legislative jurisdiction to the Court's adjudicative jurisdiction have been called into question by cyberspace. While it is quite tough to track down an offender or defendant, it is not that difficult to conduct crimes and violate the law. Specifically, the transnational character of the offenses poses a major obstacle to regulation. Given the unbounded nature of cyberspace, it

[192] WIPO, https://www.wipo.int/treaties/en/registration/madrid_protocol/ (Last accessed on April. 20, 2024).
[193] WIPO, https://www.wipo.int/treaties/en/ip/tlt/ (Last accessed on April. 20, 2024)

is essential to create a special law that may be utilized to resolve cybercrime cases without difficulty or misunderstanding.

CHAPTER 4: E-COMMERCE LIABILITY FOR TRADEMARK INFRINGEMENT

4.1 INTRODUCTORY:

India has seen an exponential increase in online marketplaces and e-commerce. Customers may now have a whole new and distinct kind of shopping experience since the E-Commerce system makes it simple for them to exchange goods and services using smartphones, competitive pricing, enticing discounts, and quick delivery. However, all of these resources also encourage counterfeiters to take advantage of the internet and e-commerce to advertise and sell their phony products in order to profit on the goodwill of other businesses in the marketplace[194].

The internet has become ubiquitous, leading to the emergence of many risks associated with the digital era. The utilisation of the Internet for commercial reasons has brought about a significant metamorphosis in the corporate landscape. Several organisations have achieved success in their company and commerce by adapting to changing marketing trends and the shift from physical markets to e-commerce.

E-commerce sites may intentionally or unintentionally encourage the selling of counterfeit goods. E-commerce platforms have made extensive use of the term 'intermediary liability.' This liability is based on the idea that since the service provider acts as an intermediary in the online sale of counterfeit goods and services, the provider will be held accountable for any trademark infringement that takes place on their platform. According to recent studies, India's E-Commerce industry is further expected to grow rapidly, from US$ 70 billion in 2022 to US$ 325 billion by 2030.It is anticipated that this development pattern will persist, contributing to the 27% compound annual growth rate (CAGR) rise of e-commerce in India.[195].

The use of registered trademarks is restricted by trademark law because it can lead to misunderstandings among prospective consumers about the true nature and source of the goods or services in question. It has also been used to settle disputes between trademark owners and computer users who purchase Internet domain names. The negative effects of the shifting economy include cyber-squatting, typo-squatting, mega-tagging, renewal snatching, and other unfavourable results coming from the migration to cyberspace.

4.2 ASSESSING THE INFRINGEMENT

Evaluating the infringement of a trademark can be challenging. Not only about which court has jurisdiction but also about the identity of the person responsible for the infringement. Due to the difficulty in identifying or prosecuting the principal conduct, trademark owners occasionally go to unaffiliated third parties who may have participated in the infringement. For example, they could be serving as the host for the illegal content

[194] Meenakshi Duggal, and Gaganpreet Kaur Ahluwalia. *"Assessing the Growth of E-commerce in India: A Study of Flipkart's Performance, Viability, and Future Prospects."* 11(2) TOJDEL, 135-148 (2023).
[195] IBEF, https://www.ibef.org/industry/ecommerce, (Last accessed on 1 May, 2024).

or acting as a platform for the sale of fake items. Direct liability and secondary liability are the two categories of liability that apply to e-commerce websites.

4.2.1 Primary Liability

An investigation into whether the platform committed direct acts of infringement is necessary to determine whether it bears direct liability.

For instance, in *L'Oreal v. eBay*[196], eBay was accused of bidding on keywords that promoted connections to products that violated L'Oreal's trademark, and as a result, eBay was held accountable by L'Oreal for selling counterfeit goods. The Court of Justice of the European Union, or CJEU, ruled that the proprietor of the website was not the one who sold Rather, the seller was the one who violated the trademark. Although the e-commerce platform is not directly liable, they could be held secondarily liable if they have significantly failed to stop the spread of counterfeit goods. The CJEU had previously said that injunctions might be issued against e-commerce sites, provided that the injunctions were reasonable and effective in preventing the sale of counterfeit goods on the platforms.

In Amazon.com Inc. v. Heather R. Oberdorf[197], amazon was unable to identify the seller who attempted to sell fake goods. The US Court declared that Amazon was accountable for the product sale and that the platform was ineffective.

4.2.2 Secondary Liability

According to the theory of secondary liability, a third party may be accountable for the acts of the trademark squatter. On e-commerce platforms, secondary responsibility lawsuits appear to be more successful; the owner protects his brand by providing quick security on his products to prevent the sale of any additional counterfeit goods. One category of secondary liability is-

i. Vicarious Infringement; and
ii. Contributory Infringement.

In the first type, an infringement happens when a third party and the direct infringer establish a partnership or understanding that binds them together and gives them control over the items that are being infringed upon. On the other hand, the second category, the liability covers any indirect violation in which a third party commits a tort or violates the law without realizing it, Courts appear to have noticed a pattern with secondary liability over time. Courts have held search engines accountable for participating in unlawful sales through keyword advertisements, and online auctions have been held accountable for engaging in unethical counterfeiting and other illegal acts.

eBay Inc. v. Tiffany (NJ) Inc[198]. Tiffany discovered that thousands of silver Tiffany jewellery were being sold on eBay as fake goods in this particular case. Tiffany contacted eBay about this so that preventive

[196] L'Oreal v. eBay, C-324/09.
[197] Amazon.com Inc. v. Heather R. Oberdorf and Anr., 930 F.3d 136 (3d Cir. 2019).
[198] eBay Inc. v. Tiffany (NJ) Inc., 600 F.3d 93 (2nd Cir. 2010).

action could be taken against such illegal acts, but eBay was only said to be able to remove counterfeit items after they were reported. Tiffany filed a lawsuit against eBay, claiming that the online retailer was selling the goods directly to consumers, resulting in deceptive advertising, unfair competition, and trademark dilution. Tiffany's claims were all rejected by the Southern District Court of New York. The court then questioned Tiffany to find out if eBay had continued to supply or sell counterfeit goods, but Tiffany was unable to offer sufficient justification for this question.

When explaining why eBay could not be held contributorily accountable for selling counterfeit products, the Second Circuit (2010) went above and beyond. eBay looked quite corporate when Tiffany posted the products, which were promptly taken down by the platform. The site could not pursue legal action against Tiffany's counterfeit goods unless the issue had been disclosed in advance. eBay enforced strict anti-counterfeiting measures, such as removing fake listings from the site within 24 hours. More than 280,000 ads were deleted from eBay between 2003 and 2007. The Second Circuit did not hold eBay secondary or contributory liable because eBay was always advancing its technology, anti-fraud measures, Trust and Safety Department Staff that implemented counterfeit measures by selecting fraud engines, the Verified Rights Owners (VERO) program that gives brand owners an easier way to list out the illegal violations on the platform, and sufficient measures. eBay's clever strategy serves as a model for other e-commerce platforms, as it requires them to collaborate with trademark owners, devote time and funds to technological advancements, create software that speeds up the removal of listings, and hire staff who deal proactively with trademark squatters[199].

4.3 ADDRESSING TRADEMARK INFRINGEMENT ON E-COMMERCE PLATFORMS IN INDIA

E-commerce platforms are generally exempt from trademark infringement liability under Section-29 of the Trademark Act, 1999 unless they engage in specialized activities such producing advertisements, establishing trust, or displaying support for sellers. Third-party providers are exempt from liability under the safe harbour doctrine of Section-79 of the Information Technology Act of 2000, provided that they have no knowledge of any criminal activity. E-commerce platforms must function passively, producing simply information rather than starting or changing it, in order to be eligible for safe harbour[200].

A revised version of the Information Technology (Media Guidelines and Digital Media Policy) Act, 2021, which enforced different rules of conduct on intermediaries, was suggested by the Department of Electronics and Information Technology in 2022. Initially, intermediaries were required to keep an eye on users adhering to their rules and steer clear of hosting particular content. Second, they have to adhere to transparency, confidentiality, access, and due diligence. Third, it was expected of the mediators to protect citizens constitutional rights. Fourth, they have seventy-two hours to respond to complaints about content

[199] Id.
[200] Ana Pokrovskaya, *"Liability for Trademark Infringement on E-Commerce Marketplaces"* 2 Int'l JILI 87-101 (2023).

removal. Furthermore, a Grievance Appellate Committee was established to manage appeals; nonetheless, customers retained the option to pursue legal remedies[201].

The quantity of digital platforms that are revolutionizing conventional business practices both B2B and B2C has grown dramatically. In any event, the emergence of e-commerce has presented a number of challenges for nations, chief among them being the escalating issue of trademark infringement due to the selling of fake goods. Prior to the development of e-commerce platforms, sellers sold fake goods covertly in constrained locations. However, the use of trademark names and goods that are confusingly similar to well-known or already-existing trademarks has increased as a result of the quick expansion of these online platforms[202]. According to a 2018 Local Circles social media platform survey, about 38% of respondents reported receiving counterfeit goods with trademark infringement and the sale of counterfeit goods via e-commerce platforms[203], both of which are likely to rise in the years to come. About 12% of all fake goods sales on e-commerce platforms were made by Snapdeal, with Amazon coming in second at 11% and Flipkart at 6%[204]. The survey also revealed that handbags, shoes, clothes, and fragrances made up the bulk of the counterfeit goods sold.

One such incident included the well-known American shoe brand Sketchers, which confiscated over 15,000 pairs of Sketchers from warehouses in Delhi and Ahmedabad and held the e-commerce site Flipkart and four of its vendors accountable for selling counterfeit goods[205]. The best venue to list the infringer and its brand from the platform is the e-commerce platform, should any trademark infringement occur. Amazon, Flipkart, and Snapdeal three of the most well-known e-commerce sites in India have established policies aimed at stopping the sale of goods bearing counterfeit labels and trademarks that appear to violate IP holder's rights while maintaining the integrity of the brand. These platforms have made it possible for IP Holder to resolve their concerns by removing the vendor and its brand, as well as by supplying sufficient documentation and proof.

Section-79 of Information Technology Act, 2000[206], talks about protection for intermediaries like Amazon, Flipkart, and Snapdeal is provided by. According to this clause:

> *"An intermediary cannot be held accountable for any third-party data, information, or communication link that he hosts or makes available[207]".*

---

[201] Ministry of Electronics and Information Technology, https://mib.gov.in/sites/default/files/Digital%20Media%20Ethics%20Code%20Rules%20%20Notification%20%281%29.pdf (last accessed on 1 ,May 2024).

[202] Id.

[203] Local Circles, https://www.localcircles.com/a/press/page/counterfeit-fake-product-from-ecommerce-sites-amazon-flipkart-snapdeal (last accessed on 1 ,May 2024).

[204] Id.

[205] Sagar Malviya, *Skechers takes Flipkart, sellers to High Court over fakes,* ECONOMIC TODAY (Dec 25, 2017, 01:19 AM), https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/skechers-takes-flipkart-sellers-to-high-court-over-fakes/articleshow/62235842.cms?utm_source=contentofinterestandutm_medium=textandutm_campaign=cppst

[206] The Information Technology Act, 2000 S. 79:Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality"

[207] Id.

These platforms, which the Information Technology Act refers to as intermediaries, are protected from liability for any third-party infringement on the platform because they have complied with section-79 of the Act and Rule 3 of the Information Technology (Intermediaries Guidelines) Rule, 2011[208].

Rule 3 of the Information Technology (Intermediary Guidelines) Amendment Rules 2018 specifies the rules that internet platforms must abide by. The Indian Supreme Court modified the following regulations[209]:

i. The intermediary that serves more than half a million users in India must be acknowledged by the Indian government as a business that was established under the Companies Act, 1956 or the Companies Act, 2013, have a permanent registered address in India, and designate a Senior designated functionary who will coordinate around-the-clock with the relevant government authorities.
ii. The intermediary must, upon request, provide all necessary details within 72 hours to any government agency.
iii. The intermediary must remove and track the originator of data when requested and with the help of a government agency.

These modifications aim to strike a balance between protecting intermediaries from liability for third-party content while ensuring they cooperate with legal authorities in addressing unlawful activities on their platforms. As the digital ecosystem continues to evolve, such regulatory measures will play a crucial role in governing the operations of intermediaries and maintaining a safe and lawful online environment.

4.3.1 Role of Indian Judiciary

Regarding the liability of the intermediaries under the Trademark Act, 1999 and the Information Technology Act of 2000, the judiciary has been very influential in the nation.

Christain Louboutin vs Nakul Baja and Ors[210] In this case, Christian Louboutin, a well-known luxury French brand that is known for creating and selling shoes of the highest calibre, filed a lawsuit in Delhi High Court against Garveys, an e-commerce website, alleging that it was trying to sell fake goods under the well-known trademark name and that it was using obvious keywords like ‘Christian’ and ‘Louboutin’ to drive traffic to the website. Claiming that the products offered on the websites were genuine, the defendants in this instance had clearly violated the well-known trademark. They identified themselves as a

[208] Information Technology (Intermediaries Guidelines) Rule, 2011 Rule 3 (2) prohibits intermediaries from knowingly hosting or publishing information which amongst other things may be ‘grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, otherwise unlawful in any manner whatever.

[209] MeitY, https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf (last accessed on 1 May 2024)

[210] Christain Louboutin v. Nakul Baja and Ors, (COMM) 344/2018, I.As. 19124/2014, 20912/2014, 23749/2014 and 9106/2015.

'intermediary,' not a merchant. The plaintiff's claims of trademark infringement were upheld by Judge Prathiba M. Singh since it was revealed that the defendant platform had directly kept counterfeit goods and created invoices for them. However, as Darvey Platform was merely advertising and promoting the product no actual sales occurred, the court did not issue any orders against the defendant for damages.

My Space Vs Super Cassettes Industries Ltd[211] In this instance, Super Cassettes Industries Ltd. (SCIL) claimed in 2007 that MySpace had let users to disseminate SCIL copyrighted content without the company's prior consent. Previously, the plaintiff, SCIL, had received an interim injunction; however, the respondent was not satisfied with the ruling and decided to seek an appeal with the High Court, which was eventually granted. Section-79 of the Information Technology Act, 2000 grants immunity to the appellant (MySpace) because it acted as an intermediary. This Section should be read in conjunction with Section-81 of the IT Act, 2000[212], which stipulates that intermediaries are not liable if appropriate due diligence is conducted without knowledge of infringement. The Respondent's Advocate, however, contended that as the Appellant was already aware of the infringement on the platform, Section 51(a)(ii) of the Copyright Act, 1957 is not applicable. The Single Bench's 2012 ruling, which found MySpace accountable for infringement even though it was unaware of the violation, was overturned by the High Court Bench. The Division Bench's 2016 ruling overturned the injunction and required the Appellant to use stronger, more creative methods to protect copyrighted content on its platform.

The Information Technology Act of 2000's Section-79 strengthened the intermediaries' safe harbor immunity by requiring the Respondent to produce a catalogue listing all the links that were infringing, and to commit to removing the links and content within 36 hours of receiving the complaint.

In Kapil Wadhwa and Ors. v. Samsung Electronics Co. Ltd. and Anr[213]*,* Samsung had filed a lawsuit against the Respondent for engaging in the import of goods, particularly printers, from overseas markets under the Samsung brand and thereafter selling the printers in India for significantly less money. A Delhi High Court single bench decided in Samsung's favor in 2012. Nevertheless, the Appellants (Kapil and ors) filed an appeal against the aforementioned order. In this situation, two questions were answered.

i. Firstly, does India adhere to the principle of national exhaustion or international exhaustion?
ii. The second question is: Is it legal for India to import products in parallel?

Since the previous Single Bench had recognized India under the theory of national exhaustion, the Division Bench's initial goal in the first issue was to understand what is meant by the word 'market' in section 30(3) of the Trademark Act, 1999, whether it refers to a national or worldwide market. On the other hand, the Division Bench adopted a broader viewpoint by citing and depending on the purposes and rationale behind the Trademark Bill, 1999. As a result, they also examined India's correspondence with the Uruguay Rounds and the Standing Committee report concerning the Copyright (Amendment) Bill, 2010. The Court concluded

[211] My Space v. Super Cassettes Industries Ltd, C.M Appeal. 20174/2011, 13919 and 17996/2015
[212] Information Technology Act 2000, S.81
[213] Kapil Wadhwa and Ors. v. Samsung Electronics Co. Ltd. and Anr. MIPR 2012 (3) 0191

that India operates under the principle of international exhaustion, which permits a product legally obtained from a foreign market to be sold anywhere in the world[214].

Regarding the second matter, the Division Bench permitted the appellant to be stopped from importing goods in parallel in India. The Appellant was also allowed by the Bench to proceed with the sale of printers, subject to the requirement that a disclaimer regarding the devices' foreign importation be included. These are solely applicable to the appellant at its own risk, discharging Samsung (Respondent) from any warranty on the goods and services. This ruling increased the leads that legitimate buyers in the nation could explore under the theory of international exhaustion, without putting the foreign seller at risk.

Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. and Others[215], The Delhi High Court's Single Bench Judge in this case heard six cases concurrently and as a result barred the respondents (e-commerce sites Amazon, Flipkart, Healthkart, and Snapdeal) from endorsing or vending any of the plaintiffs' (Amway, Oriflame, and Modicare) products[216].

In 2019, the Division Bench of the High Court overturned the Single Bench's ruling and permitted the Appellants, which are e-commerce platforms, to begin selling the Respondents' items directly to customers, even in cases where consent was not obtained. The Respondents contended that the Appellants had begun selling the products on the platforms without first obtaining their consent, which appeared to be against the Direct Selling Guidelines, 2016, specifically clause 7(6), which specifies that e-commerce platforms must be given permission to allow direct sellers to sell products. The Division Bench had declared that the prior order would negatively affect e-commerce platforms since it limits customers' options for online product purchases. The Bench also dismissed respondents' arguments regarding the quality and fake goods offered on the platform because there was insufficient evidence to support them.

In this instance, the Bench addressed four difficulties by overturning the Single Bench's ruling in the following ways:

i. First, it decided that the Gazette notices are merely advisory in nature and do not pertain to a legal status.
ii. In the second, the Division Bench cited the case of Kapil Wadhwa and Ors. v. Samsung Electronics, which granted the right to the lawful purchasers to export the goods to overseas markets and sell them anywhere, neither of which is an infringement. The Bench further argued that there would be no post-sale restrictions on the buyer of lawfully purchased goods, and that the requirement under Clause 7(6) of the guidelines was rendered invalid in the current lawsuit because there was no contractual duty between the Entities and the e-commerce platforms.
iii. With regard to the third point, the Division Bench argued that intermediaries might offer value-added services in accordance with section 2(1)(w) of the IT Act, 2000 and that they could

[214] Id.
[215] Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. and Others FAO(OS) 133/2019 And CM Appeal 32954/2019.
[216] Amway India Enterprises Pvt. Ltd. v. 1Mg Technologies Pvt. Ltd. and Anr., CS(OS) 410/2018.

not be held accountable for any third-party information placed on the platform under section 79 of the IT Act, 2000.

iv. The Division Bench had defended, in the fourth issue, that there was no contract in existence that allowed for a breach of contract to occur and result in tortious liability. And providing more justification for the e-commerce platform's status as having a Safe Harbor Protection shield, which shields it from liability for the sale of goods that violate trademarks.

4.4 HOW HAS UNITED STATES DEALT WITH TRADEMARK INFRINGEMENT THROUGH E-COMMERCE WEBSITES

The United States Lanham Act of 1946 primarily mandates the legal requirements of trademark law, however it excludes contributory trademark risk from its purview. Due to this, when US courts have to decide whether there is contributory risk of trademark infringement, they typically rely on common law principles. Trademark infringement often occurs when an unauthorized use of a trademark has the potential to cause confusion, blunder, or mislead. One type of trademark infringement is duplicating, which entails feigning to be someone important in order to deceive or fool. In these situations, the doctrine of contributory trademark infringement extends the duty to those who contribute to the fraudulent cycle but are not primary infringers.[217]

The United States Lanham Act, 1946 primarily mandates the legal requirements of trademark law, however, it excludes domain-contributory trademark risk. Due to this, when US courts have to decide whether there is a contributory risk of trademark infringement, they typically rely on common law principles[218]. Simply said, trademark infringement often occurs when an unauthorized use of a trademark has the potential to cause confusion, agitation, or misdirection. One type of trademark infringement is duplicating, which entails pretending to be someone important in order to deceive or fool. In these situations, the doctrine of contributory trademark infringement extends the duty to those who contribute to the fraudulent cycle even though they are not primary violators.

It must be shown that an online commercial centre had actual or valuable knowledge of the infringement and that it intended to regulate the infringement in order to successfully prosecute a case for contributory risk against the centre. The concept of contributory trademark responsibility was first recognized by the Supreme Court in a non-web domain in the 1982 case of Inwood Laboratories, Inc. v. Ives Laboratories, Inc[219]. According to the court, a group is considered contributorily liable if it satisfies the following criteria: it intentionally encourages another party to violate a trademark; it continues to handle goods that it approves of or is motivated to purchase that violate a trademark.

---

[217] Naumovski, Goce, and Dimitri Chapkanov, *"Convergence of Trademark Law and E-Commerce: Overview of US, EU and China Regulations on Trademarks and Domain Names."* AJOL, 424-438 (2014)

[218] Id.

[219] Inwood Laboratories v. Ives Laboratories, 456 U.S. 844 (1982)

4.5 HANDLING TRADEMARK DISPUTES IN THE AGE OF E-COMMERCE

Any firm can benefit from trademarks since they are unique identifiers that help a company stand out from the competitors. In the era of online shopping, when consumers have an abundance of options, a unique trademark may establish recognition and foster brand loyalty.

However, trademark holders have additional challenges due to the nature of e-commerce itself. Because the internet has no geographical boundaries, those who violate it could be anywhere in the world, making it impossible to locate and prosecute them using traditional legal methods. Furthermore, the expansion of social media and online markets allows unauthorized merchants and counterfeiters to offer illegal goods. When a business or individual uses a trademark that is strikingly similar to the registered trademark of another party, trademark infringement concerns arise. In order to avoid customer misunderstanding and preserve the trademark owner's goodwill and image, these issues may need to be resolved. It will cover a variety of approaches to resolving issues involving trademark infringement, such as settlement talks with the parties involved, litigation, alternative dispute resolution procedures, domain name dispute resolution procedures, and infringement remedies and fines[220]. Another fundamental issue arising cause of trademark infringement is the domain name problem which is that registration is done on a 'first come, first serve basis,' which frequently leads to abusive registration that is, registration by someone who does not have a legitimate claim or interest in the relevant domain name. Furthermore, it is widely acknowledged that the original trademark owner retains ownership of domain names.

(i) Negotiation with Infringing Parties: Negotiation between the owner of the trademark and the alleged infringer is one of the main ways to settle a trademark infringement case. When compared to litigation, this course of action can result in a quicker and less expensive conclusion, making it beneficial for both parties. Multiple steps may be involved in negotiations, including licensing the mark, delivering a cease and desist letter, and signing a coexistence agreement. Gaining direct contact with the party committing the infringement can help determine the type and scope of the violation. Sometimes there is miscommunication and the disagreement can be settled without getting worse. To aid you through the negotiating process, it is usually advisable to speak with a trademark attorney.

(ii) Alternative Dispute Resolution Mechanisms: Parties may choose to use alternative dispute resolution (ADR) techniques like mediation or arbitration if negotiations are unsuccessful. Since ADR promotes cooperation between the parties in order to resolve disputes, it is frequently faster and more affordable than litigation. Through discussion and negotiation, a neutral third person assists the opposing parties reach a mutually agreeable resolution through mediation. Contrarily, in arbitration, a neutral third-party arbiter or panel hears testimony from both parties and renders a legally binding

[220] Shantanu Raman, *"Perils of E-commerce Transaction for Customers: A Review of the Availability of Counterfeit Goods on Marketplace Platforms,"* 10 JETIR 394 (2023).

ruling. When parties to a complex issue want expert advice to obtain a just conclusion, arbitration may be helpful.

The WIPO Arbitration and Mediation Centre (WIPO Centre) is an organisation that offers services for resolving disputes. The ICANN drafting committee sought technical guidance from the WIPO Centre to comply with the requirements of the UDRP Policy and Rules. WIPO has formulated Supplementary Rules for the Uniform Domain Name Dispute Resolution Policy with the aim of enhancing and fortifying it.[221]

By using the UDRP Administrative Procedure, any individual or organisation worldwide can submit a domain name complaint over a gTLD.If the relevant ccTLD registration authority adopts the UDRP Policy voluntarily, then the UDRP Administrative Procedure may also be employed in the event of a dispute concerning a domain name registered in a ccTLD. The overview of every ccTLD for which WIPO offers dispute resolution services includes this information.

(iii) Litigation for Trademark Infringement: Litigation can be required if none of the aforementioned strategies result in a satisfactory outcome. Generally speaking, a trademark infringement case is litigated through a formal lawsuit, court appearances, and maybe a jury or judge trial. The owner of the trademark must establish that the defendant's use of the mark is likely to lead to misunderstandings or confusion about the origin or association of the products or services. In the end, litigation might be the most efficient way to protect trademark rights and get a court order to halt the infringement, but it can also be time-consuming and costly.

(iv) Remedies and Penalties for Trademark Infringement: Various remedies and fines may be imposed upon the outcome of a trademark infringement issue, contingent upon the specific circumstances and the dispute resolution procedure employed. The parties may agree to a wide range of remedies in talks or alternative dispute resolution (ADR), including paying monetary damages, changing the allegedly infringing mark, or signing a licensing agreement.

In a legal dispute, the judge has the authority to declare goods that violate intellectual property unlawful, grant damages, or even impose an injunction to prevent the mark's continued use. Defendants found guilty of willful infringement may also occasionally be subject to statutory damages, legal fees, and other such sanctions. It's crucial to speak with an experienced trademark lawyer to help you understand the several sanctions and remedies that may apply in your specific situation.

iv.5.1 ICANN UDRP and The World Intellectual Property Organisation (WIPO):

193 states worldwide are members of the World Intellectual Property Organisation (WIPO), an organisation established by a treaty between states. The member states founded the Organisation to advance intellectual

[221] Colby B. Springer, *Master of the Domain (Name): A History of Domain Name Litigation and the Emergence of the Anticybersquatting Consumer Protection Act and Uniform Dispute Resolution Policy*, 17 Santa Clara High Tech. L.J. 315 (2001).

property protection, distribution, and use globally for social, cultural, and economic advancement. The organisation offers services to the people and businesses that make up its member states as well as to the persons themselves[222].

The Uniform Domain Name Dispute Resolution Policy, also known as the UDRP Policy, outlines the legal framework for resolving disputes between a domain name registrant and a third party (i.e., a party other than the registrar) involving the abusive registration and use of Internet domain names in the generic top-level domains, or gTLDs. The ICANN Board of Directors adopted the UDRP Policy on August 25 and 26, 1999, while meeting in Santiago, Chile. The recommendations in the WIPO Internet Domain Name Process Report, along with input from registrars and other pertinent stakeholders, served as the basic foundation for the policy[223].

In October 2006, a news statement from WIPO stated that the Arbitration and Mediation Centre, which is responsible for accrediting dispute resolution service providers, has rendered a decision in its 25,000th case, directing the domain name to be transferred to the trademark owner. Trademark holders now have additional rights to pre-emptively register and contest the registration of new generic top-level domains (gTLDs), in addition to the UDRP, according to procedures that WIPO and ICANN have put in place regarding the launch of new gTLDs. Trademark holders are granted the opportunity to pre-register their name before anybody else may. ICANN's policies for domain name registrations provide trademark holders unique rights that are not conferred by trademark law; however, WIPO suggested the policies be put in place to give trademark owners preference in cyberspace[224].

The contentious ICANN policy regarding the WHOIS database and its dissemination of personal data online one that WIPO advised. According to ICANN's WHOIS policy, everyone who has ever registered a domain name must provide their personal contact information, including their home address and phone number, to a free online database that is open to anyone for any reason. The WHOIS database is one of the main sources of information for consumer abuses such as identity theft, fraud, and other privacy violations because of ICANN's policy derived from WIPO[225].

In reaction to ICANN's establishment, WIPO published a report in 1998 stating that, notwithstanding privacy concerns, publicly accessible databases including the full and correct contact details of every domain name registrant must be made available. Regardless of whether there has been any infringement of intellectual property rights or any other kind of infringement, the WIPO study suggested that furnishing any false registration information should be cause for domain name forfeiture.

---

[222] WIPO, https://www.wipo.int/about-wipo/en/ (last accessed om 1 May, 2024)
[223] WIPO, https://www.wipo.int/amc/en/domains/guide/#:~:text=The%20WIPO%20Center%20was%20the,the%20UDRP%20Policy%20and%20Rules (last accessed on 1 May, 2024)
[224] Supra note 142 at 56
[225] Icann, https://www.icann.org/resources/pages/wdrp-2012-02-25-en#:~:text=At%20least%20annually%2C%20a%20registrar,data%2C%20and%20make%20any%20corrections (last accessed on 1 may 2024)

Despite a vote in April 2006 by the Generic Names Supporting Organisation (GNSO) Policy Council of ICANN stating that the WHOIS database serves a narrow and technical purpose, large intellectual property holders maintain that the database of personal information should remain accessible to all to safeguard intellectual property rights.

4.5.2 WTO-TRIPS:

The World Trade Organisation (WTO) is tasked with supervising the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), which is widely regarded as the most important instrument concerning intellectual property rights, even though WIPO oversees an additional 24 treaties. Unlike the WIPO treaties, the TRIPS Agreement includes robust mechanisms for ensuring compliance with its provisions, such as trade sanctions and lawsuits in the World Court[226].

The goal to establish a mutually supportive relationship between the WTO and the World Intellectual Property Organisation is expressed in the preamble of the WTO's TRIPS Agreement, which was signed in 1994. In 1996, the WTO and WIPO signed a cooperation agreement to help with the TRIPS Agreement's implementation. The 1996 WTO-WIPO cooperation agreement calls for collaboration in three primary areas: technical cooperation; enforcing national emblem protection procedures; and notifying, making accessible, and translating national intellectual property rights legislation. Two more technical cooperation agreements were introduced by the WTO and WIPO in 1998 and 2001 following the 1996 agreement to encourage developing countries to incorporate the TRIPS provisions into their national legislation[227]. It covers the following areas of IP:

i. Copyright and related rights
ii. Trademarks
iii. Geographical indications
iv. Industrial designs
v. Patents
vi. Layout-designs (topographies) of integrated circuits

The issues considered by the Council for TRIPS were reported to include:

> *"advantages and opportunities relating to access to technology and the administration of IPRs; the use of digital and telecommunications technologies in the management of IPRs to extend the benefits of IPRs to right holders in developing countries; what kind of exploitation of IPRs on the Internet constitutes an infringement; the relationship between the TRIPS Agreement and the WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty; developments concerning trademarks and well-known trademarks, including the work carried out by and underway in WIPO; implications of the WIPO Internet Domain Name*

[226] Supra 147 at 46
[227] PETER DRAHOS, A PHILOSOPHY OF INTELLECTUAL PROPERTY 45 (ANU, 2016).

Process in relation to trademarks, geographical indications and other distinctive signs; use of patents in the digital environment particularly in relation to software and business methods; potential anti-competitive uses of IPRs in the digital environment; challenges to the enforcement of IPRs; ways in which digital technology can be used to enhance enforcement of IPRs at the border while at the same time facilitating trade; and international cooperation under Article 69 of the TRIPS Agreement in respect of intellectual property infringements occurring in the digital environment.[228]"

4.5.3 National Arbitration Forum

The size of the internet creates special difficulties for trademark enforcement. Conventional legal action can be costly and time-consuming. The National Arbitration Forum (NAF) has become an important tool in this context for settling trademark disputes involving domain names. Leading supplier of alternative dispute resolution (ADR) with a focus on domain name conflicts is the NAF[229]. It provides trademark owners with a quick and affordable way to reclaim domain names that are confusingly similar to or exact replicas of their trademarks.

4.5.4.1 Constraints on the NAF:

The NAF procedure can only deal with domain name disputes; it cannot handle more general trademark infringement problems, such as the online sale of counterfeit goods. No Binding Decision i.e., The losing party may still file a lawsuit, and NAF rulings are not legally binding[230].

Reverse Domain Name Hijacking (RDNH): A legal claimant to a domain name may submit a UDRP complaint to wrest ownership of the name from the legitimate trademark owner. This is a danger known as reverse domain name hijacking.

The National Arbitration Forum is essential to the online protection of trademarks. A quick, easy, and economical method of resolving domain name disputes resulting from cybersquatting and, occasionally, trademark dilution is through the UDRP procedure. It's crucial to recognise the NAF's limitations, too, and to use it as one instrument in a larger arsenal for trademark protection. The NAF will probably modify its policies as the internet develops in order to meet new difficulties and maintain an equitable and well-rounded framework for online trademark enforcement.

The quickness of the ICANN dispute resolution process is an advantage. In response to a complaint, respondents have 20 days to respond. After all submissions are received, the panel has 45 days to make a decision. Typically, a WIPO domain name complaint is resolved in two months. Hearings are not held in person unless there are exceptional circumstances. A panel of one or three arbitrators, chosen from a list of specialists in intellectual property problems approved by ICANN, is an alternative available to the parties.

---

[228] WTO, https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm (last accessed om 1 May, 2024)

[229] Gunmala Suri, *Intellectual Property Rights Management: Emerging Cyberspace Issues in Knowledge Society: A Critical Analysis*, UBS PU, 256 (2019), https://csi-sigegov.org.in/critical_pdf/29_256-262.pdf.

[230] Jacqueline D. Lipton, *Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy*, 40 Wake Forest Law Review 1361 (2005).

Domain Names 55 The panel will thereafter make its judgement solely based on the pleadings. Everything that happens is done so electronically. Therefore, the process of remedy is substantially quicker than typical court litigation. Another benefit of the UDRP is that it is simple to enforce the awards because of agreements between ICANN, domain name registrars, and registrants that make the awards binding[231]. UDRP's drawback is that, even in situations where registrations were made in bad faith, you are not entitled to any financial compensation. Furthermore, injunctive relief is not offered. It is possible to gain both of these through legal litigation. Therefore, one can choose either of these two approaches for resolving disputes, assessing the benefits and drawbacks of each according to his needs.

4.6 Preventing and Combating Trademark Infringement in E-commerce

Worldwide, trademark infringement in e-commerce is becoming a bigger issue since fake goods may be detrimental to both customers and businesses[232]. Businesses in the online marketplace need to take proactive measures to avoid and combat trademark infringement in order to safeguard their intellectual property and keep a competitive advantage.

(i) Registering Trademarks Nationally and Internationally: Obtaining trademark registration in the appropriate jurisdictions is one of the first steps toward safeguarding a brand against unapproved use. Businesses who register their trademarks are granted the only right to use them in connection with the products and services for which they were intended. To guarantee complete protection, trademarks should be registered both domestically and in important foreign markets. Companies should think about registering their trademarks in the nations in which they want to produce or sell goods, as well as in areas with a high concentration of counterfeiting activity. Businesses can more successfully defend their rights against infringers and pursue legal action against them by registering trademarks in several jurisdictions. Additionally, companies must to consider the potential for trademark registration via the Madrid System, an international trademark system run by the World Intellectual Property Organization (WIPO). Rather than submitting separate applications for each nation, firms can use the Madrid System to register their trademarks in numerous countries with a single application, saving time and money.

(ii) Enforcing Trademark Rights on E-commerce Platforms: Because counterfeiters frequently use e-commerce platforms to sell fake goods under a brand's name, these platforms are a hotspot of trademark infringement. Businesses must continuously scan e-commerce sites for products that violate intellectual property rights and take appropriate legal action. The majority of significant e-commerce sites, including eBay, Amazon, and Alibaba, have policies in place for reporting and eliminating fake listings. Companies that find counterfeit goods should get familiar with these processes and file infringement lawsuits right away. Participating in brand protection initiatives

[231] Id.

[232] LISA KA 1Z JONES, *TRADEMARK.COM: TRADEMARK LAW IN CYBERSPACE, file:///C:/Users/DELL/Downloads/alr,+37-4_8_Katz_Jones.pdf (last accessed on 1 May 2024).*

provided by top e-commerce sites is also advised, since these initiatives frequently give extra resources and tools to help identify and eliminate products that violate intellectual property rights. Additionally, by facilitating information sharing between the platform and the brand, these initiatives enable more effective enforcement actions.

(iii) Involving Law Enforcement Agencies: In certain instances, e-commerce trademark infringement may justify the involvement of law enforcement agencies to combat illicit activities like online piracy and counterfeiting. Businesses should notify local, national, or even worldwide law enforcement organizations of any noteworthy or continuous violations. Businesses may combat counterfeit activities by partnering with law enforcement organizations to take advantage of additional resources and experience. Furthermore, criminal sanctions for trademark infringement might effectively discourage potential counterfeiters.

(iv) Educating Consumers About Counterfeit Risks: In order to prevent trademark infringement in e-commerce, it is best to inform customers about the dangers of purchasing fake goods. Businesses may enable consumers to make educated purchasing decisions and steer clear of counterfeit goods by educating them about the risks associated with counterfeit items. Among the strategies to inform customers are the development of instructional materials, the dissemination of advice on how to spot fake goods, and the promotion of the benefits of real goods. Additionally, in order to raise awareness of the dangers of counterfeit goods and encourage authenticity, brands can work with regulatory bodies, consumer advocacy groups, and influencers.

(v) Technological Solutions for Trademark Protection: Companies can also use technology solutions to stop and fight online trademark infringement. Digital watermarking, blockchain, and artificial intelligence (AI) are examples of cutting-edge technologies that can be extremely helpful in protecting brands and safeguarding trademarks. AI-driven solutions, for instance, are capable of effectively monitoring and analyzing enormous volumes of data to spot possible violations instantly. Immutable records of trademark registrations can be produced using blockchain technology, assisting in the demonstration of ownership and preventing unauthorized usage. By adding distinctive identifiers to product photos and digital material, companies can trace their assets and confirm their legitimacy through the use of digital watermarking techniques.

(vi) The Policy for Uniform Dispute Resolution (UDRP**):** The Uniform Domain Name Dispute Resolution Policy (UDRP Policy) establishes the legal structure for resolving conflicts between a domain name owner and a third party in generic top-level domains (gTLDs) such as .biz, .com, .info, .mobi, .name, .net, and .org, as well as in country code top level domains (ccTLDs) that have chosen to adopt the UDRP Policy[233]. The UDRP Policy was approved by the ICANN Board of Directors during its sessions in Santiago, Chile on August 25 and 26, 1999. The policy was mostly based on

[233] Registry, https://www.registry.in/domaindisputeresolution (last accessed on May 5, 2024).

recommendations described in the WIPO Internet Domain Name Process Report, together with feedback from registrars and other stakeholders.

All ccTLDs that have implemented the Policy and ICANN-accredited registrars permitted to register names in the gTLDs have committed to uphold and enforce it for those domains. To register a domain name in the relevant gTLDs and ccTLDs, individuals or organisations must agree to the terms and conditions of the UDRP Policy[234]. The ICANN Board approved the Uniform Domain Name Dispute Resolution Policy (UDRP Rules) on October 24, 1999.

The Policy will be upheld and enforced for those domains by all ccTLDs that have implemented it and by ICANN-accredited registrars allowed to register names in the gTLDs. Individuals or organizations must accept the terms and conditions of the UDRP Policy to register a domain name in the applicable gTLDs and ccTLDs. On October 24, 1999, the ICANN Board adopted the Uniform Domain Name Dispute Resolution Policy (UDRP Rules). These regulations outline the procedures and additional needs for every phase of the administrative dispute settlement procedure. Dispute resolution companies with ICANN accreditation are in charge of the procedure.[235].

4.7 CONCLUSION:

When it comes to effectively settling domain name disputes, the UDRP is essential. It offers a uniform procedure for safeguarding intellectual property rights. Even while it has worked well, fairness can be improved even further by implementing three-member panels and an appeals procedure. It will increase the UDRP's ability to effectively handle changing domain-specific difficulties.

There are two main and secondary effects to the domain name transfer cure. When it comes to disputes under the UDRP, the complainant receives the domain name as the primary outcome, while the respondent's online identity is deleted as the secondary outcome. The primary effect of the generalised Code's remedy becomes the secondary effect of the UDRP remedy under a generalised Code. Put differently, the principal outcome of the remedy provided by the generalised Code is the elimination of the respondent's online identity, at least with regard to any domain names that serve as Website addresses or universal resource locators (URLS) for the website where the intellectual property infringements took place[236].

Even if their response is unsuccessful, they can easily re-establish their online presence by utilising a different domain name. Therefore, if a respondent had such intentions, it might keep violating the complainant's intellectual property rights by simply creating a new website under a different domain name that contained the same offensive content. It follows that a generation of the UDRP along the lines mentioned above would not serve as much of a deterrent to those who are intent on violating intellectual

[234] Dev Agrawal, *UDRP (Domain Name) Arbitration: Enforceability and Relevance under Alternate Dispute Resolution Framework,* 5 JIPR. 135 (2022).
[235] The WIPO Arbitration and Mediation Center received accreditation for UDRP cases from ICANN on 29 November 1999
[236] Supra note 37 at 15

property rights and will stop at nothing to do so[237]. Domain names are seen as essential company assets in the modern digital environment. They are crucial in increasing customer loyalty, brand value, and popularity. The increasing prevalence of online business and commerce has coincided with a significant rise in the threat of cyber-attacks. Cyber squatters assault and target the identities of well-known companies in an effort to exploit or sell these phoney websites for undue profit. Strong action must be done to combat this global threat, especially in light of the surge in cyber-squatting cases in recent years. This misrepresentation not only violates the rights of real trademark holders but also confuses the public[238].

This approach seeks to resolve the disagreement rather than merely placing the domain name on hold until the parties settle it amicably or through litigation, which is a significant distinction between it and the prior dispute resolution policy that NSI had implemented. Domain names will no longer be placed on hold under this system. It will no longer be possible for trademark owners to quickly stop the holder of a domain name from engaging in any potentially unpleasant behaviour[239]. If they wish to stop the use of a name until the UDRP resolution is made, they will need to go to court. This provision, of course, ensures that domain name owner who run websites won't have their sites wrongfully taken down unless they have the legal capacity to enjoin such action. Unless a lawsuit is brought against the disputed name under the UDRP or in court, NSI had stated that it will drop the holds on the 1,300 domain names that were contested under its prior policy. To avoid an overflow of the new UDRP system, the names will be made public over the course of the following three months.

In summary, courts have found it difficult to reconcile the interests of platform operators, trademark owners, and customers in cases involving secondary responsibility and the part that online platforms play in encouraging trademark infringement. It will be feasible to avoid trademark infringement in the digital age by strengthening the current structure, encouraging stakeholder cooperation, enhancing regulatory clarity, and conducting due diligence. Future e-commerce growth will present both opportunities and challenges for trademark protection. More court rulings and legislative modifications are also anticipated to enhance the legal landscape and provide greater guidance and clarity for resolving trademark infringement cases in the digital ecosystem.

[237] H. Brian Holland, *The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. Marshall J. Computer and Info. L. 1 (2005).
[238] Gulafroz Jan, *Applicability of Trademark Laws to Cyberspace: An Analysis*, IJLMH, 463-498 (2021).
[239] Sourabh Ghosh, Domain Name Disputes and Evaluation of The ICANN's Uniform Domain Name Dispute Resolution Policy, 9 JIPR. 424 (2004).

CHAPTER 5: CONCLUSION AND SUGGESTIONS

5.1 CONCLUSION

> *"When you incorporate a company in a state, the state doesn't bother to see if there are other conflicts with trademarks that may be registered in other states it just checks with the secretary of state to see if the same name has been registered .... That in no way entitles you to use the name if in fact there is a conflict with a federally registered trademark."*[240]

According to the hypothesis question related to stringent legislative and policy measures required for the effective protection of trademarks in cyberspace, the dissertation has answered the question with the help of primary and secondary data and is based on the examination of national and international legislations, their judicial interpretations, and other non-judicial policies and frameworks including books, publications, and content available on web portals; furthermore, the study has gone beyond that and justified that the legal nature of trademark in cyberspace.

Both small and large businesses have benefited greatly from the introduction of the Internet. Before, nearly any business could not have reached such a broad client base without investing a significant amount of time, effort, and resources. But it's a new day, and trademark law needs to change to keep up with these technological developments. Early case law helped to build a corpus of common law that has aided companies looking to safeguard the goodwill generated by using their trademarks in commerce. On the other hand, the rapid growth of technology has outpaced the common law[241]. It has been sluggish to answer the plethora of queries, which will only increase in frequency as businesses continue to use the internet to conduct business with clients more quickly. As a result, there is no justification to believe that the trademark law is inadequate to address the advancements in the business world.

Courts in the United States and Europe are faced with the challenge of interpreting and applying national laws in the context of a digitally borderless realm due to trademark uses in electronic ads and referencing services in cyberspace. In addition, it has led to disputes over competence and jurisdiction, giving the owner of a trademark in the EU the freedom to select the court in which to challenge infringement. The importance of the trademark owner's goodwill is demonstrated by the differing methods

---

[240] Joshua Quittner, *Billions Registered" Right Now, There Are No Rules to Keep You from Owning a Bitchin " Corporate Name as your own Internet Address*", WIRED, (Oct. 1994), https://www.wired.com/1994/10/mcdonalds/.

[241] Supra 29 at 11.

that courts in the US and the EU have taken when dealing with instances of trademark infringement by internet intermediaries acting as primary or secondary infringers[242].

It demonstrates the extent to which their consumer protection policies are compassionate toward other middlemen while maintaining fair competition and fair use. Since there is a chance that consumers will be confused about the source, affiliation, sponsorship, or connection of a product due to the actions of advertisements and intermediaries motivated by financial gain, courts have consequently established a common foundation for determining infringement.

Trademark law must be adaptable enough to take into account new trends of trademark infringement given the likelihood of trademark infringement in the exciting new world of internet commerce. Second, almost every type of cyber fraud that was mentioned in the first paragraph can be addressed by sufficient criminal legislation. Under no circumstances is it necessary to add the wisdom of concluding that this is a legal error. This is not a problem. Presumably, the US government was forced to create legislation to address the 'case' of cyber hacking since trademark owners are prohibited from participating in the market. It is possible, nonetheless, that this action will limit people's freedom of expression[243]. Furthermore, given India's more developed state of 'stare decisis,' where appropriate acknowledgment is granted, there is no need to emulate the actions taken by the United States in this regard. In other words, if courts will handle novel forms of trademark infringement and apply the same standards to the existing rules of trademark law, there is no need to be suspicious of them.

Infringements on intellectual property rights are increasingly occurring in cyberspace. A number of actions taken by the operators of cyberspace websites led to the infringement of other website operators' rights, including intellectual property rights. It is now essential that people understand how their webpages and websites are being used illegally[244].

International treaties and conventions have established a number of rules to prevent online IPR infringement, which is promoting the expansion of e-businesses and e-commerce. Nevertheless, there are no prohibitions in the Information Technology Act regarding cybercrimes pertaining to intellectual property rights, cyberstalking, cyberdefamation, etc. Furthermore, there is no mention of online trademarks in the Indian Trademark Act of 1999.

Trademark law has been a territorial phenomenon, ever since the Paris Convention and the Berne Convention for the Protection of Literary and Artistic Property, the first intellectual property convention of the late nineteenth century, were given national consideration[245].

A signature state needed to guarantee the same level of protection to the citizens of other signatory states as it did to its own inhabitants. Geographical factors play a crucial role in providing context, which in turn establishes the limitations of trademark rights. Given the core purpose of trademark law, it made logical

[242] Supra 223 at 67.
[243] Sally M. Abel, *Trademark Issues in Cyberspace: The Brave New Frontier*, 5 Mich. Telecomm. and Tech. L. Rev. 91 (1999).
[244] THOMSON WEST, INTERNET LAW AND PRACTICE (18th ed. 2002).
[245] WIPO, https://www.wipo.int/treaties/en/ip/berne/ (last accessed on 1 May 2024)

for trademark rights to be spatially specified. Trademark law was created to protect customers from misunderstanding and to preserve producer goodwill, both of which were achieved by acknowledging local producers' rights.

Territoriality is the term used to describe actions done to protect goodwill within a given geographic area, on the other hand, the desire for cross-border trade incentives and more efficient international rights enforcement has increased due to global markets and digital communication. Trademarks act as badges of origin, letting customers know where their goods or services are coming from. As a result, trademark rights forbid other parties from making money off of the goodwill associated with a brand and hurting the owner's sales[246].

It is crucial for trademark owners to keep educated and take proactive measures to protect their trademarks in the digital age as businesses grow more global and technology develops. Ensuring long-term success in the marketplace can be facilitated by firms establishing and preserving their brand identity, goodwill, and reputation through effective trademark protection. Trademark law in cyberspace has evolved over time to take into account new business practices and technological advancements. One of the more recent developments in this industry is domain name disputes, which happen when someone else registers a domain name that is confusing to customers and looks similar to a trademark[247]. As a result, the trademark owner can see a decline in sales.

5.2 SUGGESTIONS

Trademark law has historically been formulated to minimize the expenses associated with consumer searches and to maintain the fundamental doctrinal framework of attenuated, perception-based rights. Having a built-in First Amendment compass, traditional trademark law is wholly consistent with the theory of the First Amendment, which does not protect commercial fraud,[248] as opposed to trademark dilution law. Courts have formed opinions about trademark protection and use based on two criteria: distinctiveness and confusion. One cannot overstate the significance of protecting consumers, and even in domain name disputes, the average consumer standard should continue to be the main focus of the investigation.

The Uniform Domain Name Dispute-Resolution Policy (UDRP) is a widely used tool by trademark owners to contest domain name registrations and protect their rights. An additional noteworthy development in brand management is the growing utilization of social media. Social media platforms are now an essential tool for companies looking to build consumer relationships and brand awareness. But there has also been a rise in trademark infringement on social media as a result of this. Owners of trademarks must keep a close eye on social media sites for any possible trademark infringement and take proper legal action to safeguard their brands. Undoubtedly, in the age of the internet, the UDRP has demonstrated itself to be an efficient and reasonably priced means of resolving domain name disputes and addressing online conflicts that impact

[246] Rewe-Zentral v. Ohim Lite Case T-79/00 (2002)
[247] ASHWANI KUMAR BANSAL, THE LAW OF TRADEMARKS (3rd ed. 2014).
[248] Mattel, Inc. v. MCA Records, Inc., 296 F.3d 894, 905 (9th Cir. 2002)

landmark owners[249]. However, there is still much work to be done to improve its functioning at the territorial level. Global experience has demonstrated that numerous other nations have even attempted to close the legal loophole by enacting unique legislation to address the issue, such as the US's Trademark Cyber Piracy Prevention Act 1999. Similar to other countries, India likewise requires a law on the subject, as the passing law concept does not offer a comprehensive resolution to the problem at hand.

There are problems with this policy on its own. First of all, since it's not a law, the countries cannot be required to use this particular conflict resolution method. The parties to the arbitration may bring a new lawsuit in any other court that has jurisdiction, and the rulings rendered by the arbitral bodies under the UDRP are also not conclusive, meaning they do not set a precedent. As a result, the main objective of the UDRP, which was to provide time-bound dispute resolution, has been achieved.

A careful examination of the court's numerous rulings indicates that there isn't a suitable system in place to keep an eye on the growing problem of cybersquatting. To prevent infringers from registering their marks and obtaining an unfair advantage over the reputations of others, the current trade mark regime provides a correct method for registering a trade mark, together with proper monitoring and verification. On the other hand, anybody can register a domain name. According to the study, a suitable process needs to be started for domain name registration as well, to ensure that no one registers a domain name for an already-registered brand on the black market with bad intentions.

To secure the domain names, this researcher believes that a new system needs to be implemented at the national level. Tight guidelines must be established to monitor those who are either unauthorized users or do not have the legal authority to use the domain name due to the presence of a prior trademark. Furthermore, the author claims that, similar to trademarks, domain names also require previous search to be done. One effective strategy to address the problems with trademark protection in cyberspace is to form an impartial adjudicatory organization that deals with issues related to domain names and cybersquatting.

As a result of globalization and the expansion of cross-border trade, trademark owners now confront difficulties in defending their brands across nations with disparate trademark regulations. This means that in order to protect their trademark rights in each jurisdiction, trademark owners must be aware of the legal requirements in each nation. Lastly, non-traditional trademarks -like colors, fragrances, and sounds are starting to play a bigger role in branding. These unconventional trademarks are frequently used to establish distinctive brand identities and set a business apart from its rivals' offerings.[250] The need to protect these unconventional trademarks is growing as technology develops. To sum up, it is critical for trademark owners to keep up with new developments in internet trademark law and to take preventative measures to safeguard their brands in the digital era. Businesses may accomplish this by building and preserving their goodwill, reputation, and brand identity all of which are essential for long-term success in the marketplace.

---

[249] Supra note 22 at 7

[250] Llewelyn, David and Reddy, Prashant, Metatags Using Third Party Trade Marks on the Internet, https://ssrn.com/abstract=3683824 (January 31, 2020).

Under the Indian trade mark legislation, there should be a provision for an additional and simpler method of registration for each State. This will save a lot of time and ease the burden of number of procedural hurdles for the owner seeking a territorial registration alone. The Indian law should shorten the five-year period of non-use of a trade mark as a basis for revocation to three years[251]. This would prevent someone from using a registered name to prevent another squatter from using it, as they are aware of how time-consuming and drawn out the litigation process can be. Some potential loopholes in trademark protection in cyberspace:

i. Political and Economic Motivations: The statement suggests that the imposition of intellectual property rights (IPR), including trademarks, by richer countries may not necessarily be driven by the desire for positive economic benefits, but rather by political and economic power dynamics. This implies that there could be instances where trademark protection in cyberspace is used as a tool for asserting dominance or control, rather than solely for the protection of legitimate intellectual property.

ii. Impact on Poorer Countries: The analysis indicates that the TRIPS agreement, which includes provisions on intellectual property rights, may not be in the best interests of poorer countries. This raises the possibility that in the context of cyberspace, trademark regulations could disproportionately favor richer nations or entities with greater resources to enforce their trademarks, potentially leaving loopholes or gaps in protection for trademarks held by entities in poorer countries.

iii. Evaluation of Economic Evidence: The statement mentions an objective evaluation of economic evidence regarding the influence of intellectual property rights on factors such as export performance, foreign investment, and economic growth. This suggests that there may be complexities in assessing the actual impact of trademark protection on economic outcomes, which could indicate areas where loopholes or weaknesses in trademark enforcement might exist.

iv. Case Studies in Intense Conflict Areas: The statement highlights case studies from sectors like pharmaceuticals and agricultural biotechnology where conflicts over intellectual property are particularly intense. These case studies could provide insights into specific challenges or vulnerabilities in trademark protection within these sectors, which could extend to cyberspace as well, especially considering the increasing digitalization of these industries.

By considering these points, one can approach the analysis of trademark protection in cyberspace with a critical perspective, looking for potential areas where political, economic, and social dynamics may create loopholes or weaknesses in enforcement mechanisms. This might include examining how power dynamics between different countries or entities influence the development and enforcement of trademark regulations, as well as identifying specific industries or sectors where conflicts over intellectual property are especially pronounced and may reveal vulnerabilities in trademark protection strategies.

[251] Mr. Atul Satwa Jaybhaye, *Cyber Law and Ipr Issues: The Indian Perspective,* BLR 166, 185 (2016).

Another recommendation is to include provisions regulating cybercrimes, particularly cybersquatting, in information and technology law as well as trade mark law[252]. This will safeguard the rights of legitimate claimants both at the territorial and extraterritorial levels. To protect trademarks in cyberspace, brand owners should:

i. Register their marks in relevant jurisdictions
ii. Monitor online for infringement and cybersquatting
iii. Enforce rights through domain dispute resolution procedures
iv. Adapt enforcement strategies to the online environment
v. Stay informed on evolving legal and technological developments

Navigating the complex and rapidly changing world of trademarks in cyberspace requires vigilance, adaptability, and legal expertise. By staying proactive and working with qualified professionals, brand owners can protect their valuable intellectual property rights in the digital age.

BIBLIOGRAPHY

BOOKS

1. MICHAEL BENEDIKT, CYBERSPACE (The MIT Press 1992).
2 ASHWANI KUMAR BANSAL, THE LAW OF TRADEMARKS (3rd ed. 2014).
3 THOMSON WEST, INTERNET LAW AND PRACTICE (18th ed. 2002).

[252] MICHAEL BENEDIKT, CYBERSPACE (The MIT Press 1992).

4 D ROWLAND AND E MACDONALD, INFORMATION TECHNOLOGY, (Cavendish Publishing 2005).
5 DONALD G. RICHARDS, INTELLECTUAL PROPERTY RIGHTS AND GLOBAL CAPITALISM: THE POLITICAL ECONOMY OF THE TRIPS AGREEMENT (Routledge, 2004).
6 DIANE POREMSKY, GOOGLE AND OTHER SEARCH ENGINES 60 (Peachpit Press 2004).

JOURNAL

1. Kenneth Sutherlin Dueker, *Trademark Law Lost in Cyberspace: Trademark Protection for Internet Addresses*, 9 Harv. J. L. and Tech. 483 (1996).
2. Mr. Atul Satwa Jaybhaye, Cyber Law and IPR Issues: The Indian Perspective, BLR 166, 185 (2016).
3. David Yan, *Virtual Reality: Can We Ride Trademark Law to Surf Cyberspace,* 10 Fordham Intel. Prop. Media and Ent. L.J. 773 (2000).
4. Justin Hughes, The Internet and The Persistence of Law, 44 B.C.L. Rev. 359 (2003).
5. Prof. Michael Geist, Is There a There There? Toward Greater Certainty for Internet Jurisdiction, 16 Berkeley Tech. L.J. 1345 (2001).
6. Gulafroz Jan, Applicability of Trademark Laws to Cyberspace: An Analysis, IJLMH, 463-498 (2021).
7. H. Brian Holland, The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty, 24 J. Marshall J. Computer and Info. L. 1 (2005).
8. Aaron L. Melville, *New Cybersquatting Law Brings Mixed Reactions from Trademark Owners*, 6 B.U. J. Sci. and Tech. L. 13 (2000).
9. Huey-Ing Liu, *Mobile domain name system: an alternative for mobile IP*, 2 ICCS 830, 834-838 (2002).
10. Sourabh Ghosh, Domain Name Disputes and Evaluation of The ICANN's Uniform Domain Name Dispute Resolution Policy, 9 JIPR. 424 (2004).
11. Dev Agrawal, UDRP (Domain Name) Arbitration: Enforceability and Relevance under Alternate Dispute Resolution Framework, 5 JIPR. 135 (2022).
12. Thomas R. Lee, In Rem Jurisdiction in Cyberspace, Wash. L. Rev. 97 (2000).
13. A Froomkin, The collision of trademarks, domain names, and due process in cyberspace, 40(2), CACM 91-97 (2001).
14. Richard L. Baum and Robert C. Combow, First Use Test in Internet Domain Name Disputes, NATL. LJ 30, (1996).
15. Pope, Michael and Warkentin, Merrill and Mutchler, Leigh and Luo, Robert, The Domain Name System: Past, Present, and Future, 30 Communications of the AIS, 251 (2012).
16. Jacqueline D. Lipton, Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy, 40 Wake Forest Law Review 1361 (2005).
17. Muragendra B. T, Copyright and Trademark in Cyberspace, 3 IJSER 1,4 (2012)

18. Heidi S. Padawer, *Google This: Search Engine Results Weave a Web for Trademark Infringement Actions on the Internet*, 81 WASH. U. L. Q. 1099 (2003).
19. Aaron L. Melville, New Cybersquatting Law Brings Mixed Reactions from Trademark Owners, 6 B.U. J. Sci. and Tech. L. 13 (2000).
20. Meenakshi Duggal, and Gaganpreet Kaur Ahluwalia. "Assessing the Growth of E-commerce in India: A Study of Flipkart's Performance, Viability, and Future Prospects." 11(2) TOJDEL, 135-148 (2023).
21. Ana Pokrovskaya, "Liability for Trademark Infringement on E-Commerce Marketplaces" 2 Int'l JILI 87-101 (2023).
22. Naumovski, Goce, and Dimitri Chapkanov, "Convergence of Trademark Law and E-Commerce: Overview of US, EU and China Regulations on Trademarks and Domain Names." AJOL, 424-438 (2014)

WEBSITES

1. Fortinet, https://www.fortinet.com/resources/cyberglossary/what-is-ip-address, (last accessed on Feb. 20, 2024).
2. Fortinet, https://www.fortinet.com/resources/cyberglossary/cybersquatting (last accessed on May 1, 2024).
3. Whitney C. Gibson, *New '.sucks' domain name gives rise to extortion claims, future online reputation attacks,* LEXOLOGY, (May 22, 2015), https://www.lexology.com/library/detail.aspx?g=78893456-c62c-4f0a-b9ae-73b32ffda09c.
4. Llewelyn, David and Reddy, Prashant, Metatags Using Third Party Trade Marks on the Internet, https://ssrn.com/abstract=3683824 (Last accessed on May 1, 2024).
5. WIPO, https://www.wipo.int/trademarks/en/ (last accessed on Apr. 9, 2024).
6. Registry, https://www.registry.in/domaindisputeresolution (last accessed on April 19, 2024).
7. Mondaq, https://www.mondaq.com/india/trademark/525188/legality-of-metag-ing-linking--framing (last accessed on April 9, 2024).
8. BANANAIP, https://www.bananaip.com/ip-news-center/history-and-evolution-of-trademark (last accessed on April. 20, 2024)
9. ICANN, https://www.icann.org/resources/pages/policy-2012-02-25-en (last accessed on May 1, 2024).
10. Nikita Tambe and Aashika Jain, *What Is a Top-Level Domain (TLD),* FORBES, (Mar. 20, 2024, 5:52 pm), https://www.forbes.com/advisor/in/business/software/top-level-domain/ .
11. LISA KA 1Z JONES, *Trademark.Com: Trademark Law in Cyberspace, file:///C:/Users/DELL/Downloads/alr,+37-4_8_Katz_Jones.pdf (last accessed on 1 May 2024).*
12. Pranjalig, *Cyber-Squatting and Trademark Issues,* SCRIBD (Nov. 5, 2017), https://www.scribd.com/document/363557362/cyber-squatting-and-trademark-issues

13. Gunmala Suri, *Intellectual Property Rights Management: Emerging Cyberspace Issues in Knowledge Society: A Critical Analysis*, UBS PU, 256 (2019), https://csi-sigegov.org.in/critical_pdf/29_256-262.pdf.
14. Oberlo at https://www.oberlo.com/statistics/google-ad-revenue (last accessed on 22 April 2024)
15. Supra note 89 at 29
16. Anamika, *Google can't claim safe harbour if use of trademarks in Ads Programme violates trademark: Delhi HC,* ETtech (Aug 12, 2023, 11:32:00 AM), https://economictimes.indiatimes.com/tech/technology/google-cant-claim-safe-harbour-if-use-of-trademarks-in-ads-programme-violates-trade-mark-delhi-hc/articleshow/102653776.cms?from=mdr.
17. WIPO, at http://www. wipo.int/exportsites/www/copyright/en ecommerce/pdf/survey. Pdf. (last accessed on 22 April 2024).
18. Joseph Tiffany and Robert B. Burlingame, *Trademarks on The Internet - Fair Play or Fair Game?* PILLSBURY LAW (Apr. 22, 2024) https://www.pillsburylaw.com/images/content/2/4/v2/2492/11F15.pdf.
19. Manisha Singh and Puja Tiwari, *Tackling Illicit Trade: Smuggling and Counterfeiting, MONDAQ* (5 DECEMBER 2023), https://www.mondaq.com/india/trademark/1397688/tackling-illicit-trade-smuggling-and-counterfeiting
20. SCC Times, https://www.scconline.com/blog/post/2023/05/25/implementation-of-ip-vis-vis-it-law-and-e-commerce-in-india/ (last accessed on 1 May 2024).
21. WIPO, https://www.wipo.int/amc/en/domains/panel.html (last accessed on 1 May 2024).
22. WIPO, https://www.wipo.int/edocs/pubdocs/en/wipo-pub-1081-1-en-introduction-to-the-international-intellectual-property-legal-framework.pdf (last accessed on April 23, 2024)
23. LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/lanham_act, (last accessed on April 20, 2024)
24. Live Law, https://www.livelaw.in/law-firms/articles/concept-of-jurisdiction-173713 (last accessed on 29 April 2024).
25. Live Law, https://www.livelaw.in/columns/cyber-defamation-libel-slander-section-79-it-act-internet-cyberspace-social-media-205264 (last accessed on 1 May 2024).
26. Law Docs, https://lawdocs.in/blog/understanding-jurisdictional-issues-in-cyberspace, (last accessed on 30 April 2024).
27. Conseil De L'Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention (last accessed on 30 April 2024).
28. National Internet Exchange of India, https://nixi.in/ (last accessed on April 20, 2024)

29. INDIAN KANOON, https://indiankanoon.org/doc/1005493/, (last accessed on April 20, 2024).
30. INTELLECTUAL ASSET MANAGEMENT, https://www.iam-media.com/article/securing-domain-name-protection-in-india, (last accessed on April 20, 2024).
31. WIPO, https://www.wipo.int/treaties/en/registration/madrid_protocol/ (Last accessed on April. 20, 2024).
32. WIPO, https://www.wipo.int/treaties/en/ip/tlt/ (Last accessed on April. 20, 2024)
33. MeitY, https://www.meity.gov.in/writereaddata/files/public_comments_draft_intermediary_guidelines_rules_2018.pdf (last accessed on 1 May 2024)
34. CNBC, https://www.cnbc.com/2020/01/24/dhs-report-targets-online-counterfeit-sales-on-amazon-e-commerce.html (last accessed on 1 may 2024)
35. UNITED STATES TRADE REPRESENTATIVE, https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf (last accessed on 1 May 2024)
36. Icann, https://www.icann.org/resources/pages/wdrp-2012-02-25-en#:~:text=At%20least%20annually%2C%20a%20registrar,data%2C%20and%20make%20any%20corrections
37. WIPO, https://www.wipo.int/about-wipo/en/ (last accessed on 1 May 2024)
38. WIPO,https://www.wipo.int/amc/en/domains/guide/#:~:text=The%20WIPO%20Center%20was%20the,the%20UDRP%20Policy%20and%20Rules (last accessed on 1 May 2024)
39. WTO, https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm (last accessed on 1 May, 2024)
40. Joshua Quittner, *Billions Registered" Right Now, There Are No Rules to Keep You from Owning a Bitchin " Corporate Name as your own Internet Address*", WIRED, (Oct. 1994), https://www.wired.com/1994/10/mcdonalds/.
41. WIPO, https://www.wipo.int/treaties/en/ip/berne/ (last accessed on 1 May 2024)