Page 1125 - 1137 **DOI:** *https://doij.org/10.10000/IJLMH.119203*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Domain Name Disputes in the Digital Age: A Study of Cybersquatting Laws in the USA and India

RITESH WARIKALLAMATH[1]

ABSTRACT

Trademarks serve as a crucial tool in preventing consumer confusion and protecting businesses from competitors who may seek to profit through deceptive means. Trademark law grants owners exclusive rights to register and protect their marks while offering limited protection to unregistered trademarks. The primary objective of trademark law is to prevent unfair competition by ensuring comprehensive protection for trademarks at a national level. By restricting the unauthorized use of source-identifying marks, trademark law reduces consumer search costs and promotes fair marketplace competition. Without such protection, consumers could be misled, making trademarks an essential mechanism for maintaining market integrity.

With the rise of digital marketing and e-commerce, trademark-related disputes have evolved, leading to the emergence of cybersquatting—a practice where individuals register domain names of well-known brands with the intent to sell them at high prices to competitors or the brand owners themselves. The most commonly targeted element in cybersquatting cases is the Second-Level Domain Name. Various forms of cybersquatting, such as typo-squatting, identity theft, and name-jacking, have further complicated legal enforcement.

In India, cybersquatting is not explicitly addressed under the Information Technology Act, 2000 or its 2008 amendment. Instead, disputes are resolved under the Trade Marks Act, 1999 when domain names acquire brand recognition. In contrast, the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA), 1999, specifically prohibits cybersquatting, providing a civil remedy against abusive domain name registrations that infringe on distinctive trademarks.

Keywords*: Cybersquatting, Trademark, Domain Name.*

I. INTRODUCTION

The Anti cybersquatting Consumer Protection Act (ACPA) which is a separate legislation that deals with cybersquatting as a form of infringement clearly defines cybersquatting as using a domain by registering, trafficking which is identical or is likely to confuse the consumer or a

[1] Author is a LL.M. Student at Antonin Scalia law school, United States.

 [ISSN 2581-5369]

service mark of another that is a well-known mark at the time of registration, with bad intent to gain profit from the goodwill of another's trademark which results:

a. Consumer fraud and societal confusion end up being the real sources of product and service sponsorship.;

b. reduces the impact of internet commerce, which is crucial for maintaining the balance between trade and the US economy.;

c. denies real trademark owners profit and goodwill from consumers; and

d. burdens a legal trademark owner in safeguarding their own priceless trademarks that they have registered in good faith with unwarranted, regrettable, and significant burdens[2].

e. Under the World Intellectual Property Organization, The three elements of cybersquatting are that the domain is identical or confusingly similar to a trade or service mark in which the complainant has a right, the domain name holder has no right or legitimate interest in the domain name, and the domain name was registered and is being used in bad faith to increase goodwill and earnings[3]. With respect to the Indian context, there is no separate legislation regarding cybersquatting but it is considered Trademark infringement even though there is no proper definition of Cybersquatting defined under the Trademarks Act, 1999 but the Hon'ble courts have defined cybersquatting in several cases like this case[4] the hon'ble court defined cybersquatting as "where the individuals are registering the trademark with fraudulent intent to sell the domain name to the rightful owner of the name in return of certain amount and profit".

f. A domain name is a combination of names on multiple levels[5], there are mainly 3 levels in domain names for example www.Kings.com where

   i. www: Sub- Domain name

   ii. Kings: Second -level Domain name

   iii. Com: Top-level Domain name.

The top-level Domains are again classified into 2 types one being the country code top-level domain and the other one being the generic Top-level domain. Country code Top Level Domain

[2] Sukrut Deo & Sapna Deo, *Cybersquatting: Threat to Domain Name*, 8 Int'l J. Innovative Tech. & Exploring Eng'g 1, 1–3 (2019).
[3] *Id.*
[4] Manish Vij v. Indra Chugh, A.I.R. 2002 Del. 243.
[5] Stefan Kuipers, *The Relationship Between Domain Names and Trademarks/Trade Names* (Lund Univ. 2015).

is specified to a given country[6] like India has .in whereas generic Top-level domain is not subjected to any territorial limit[7]. Usually, the target of cyber squatters is mainly the second-level Domain name, in the given example the word Kings would be subjected to infringement which is related to the Trademark of a company or is the Trademark.

II. FORMS OF CYBERSQUATTING

As mentioned above, with evolving technology, there are multiple ways in which individuals can engage in cybersquatting. Some of these include:

a. **Typosquatting**: This form of cybersquatting has been quite eminent in today's world there are various ways through which Typo squatting can be done, some of them being 'URL hijacking', 'a sting site', and 'a fake URL'. Most of the time the typo squatters wait for the mistakes to be committed by the internet users while linking a web address into an internet browser and then exploit visuals and similar trademarks that can confuse the consumers. A fake website may be created which is similar to a well-known trademark so that the internet users get confused, they do it with similar logos and coloring as well. As a result, they utilize these websites to make people buy their products, increasing traffic[8]. Some common examples of typosquatting include: i) the removal of the "dot" in a given domain name for example wwwkind.com. ii) a wrong spelling of the intended site: india.com. iii) a differently created domain name that is deceptively the same as a well-known domain name like indias.com. iv) A different top-level domain: india.org. Some of the main reasons why Typo squatters do it are to sell it back to a legitimate owner and gain profits by advertising from the legitimate domain.

One of the best examples of typosquatting was when the defendant Registered the domain name gateway.com way before the plaintiff attempted to register the name. Gateway 2000 filed the case against Gateway.com, Inc. The court held in favor of Gateway.com, Inc. because that was a legitimate reason for owning the given domain name and had registered such six years before and during that period Gateway 2000 was not even a well-known trademark. The fact that the defendant wasn't arbitrarily attempting to gain value by using a well-known mark was one of the factors that led to the decision[9].

[6] Internet Assigned Numbers Authority, *Delegating or Transferring a Country-Code Top-Level Domain (ccTLD)*, https://www.iana.org/help/cctld-delegation

[7] Daniel Fisher, *Cybersquatters Rush to Claim Brands in the New gTLD Territories*, Forbes (Feb. 27, 2014, 9:29 PM), https://www.forbes.com/sites/danielfisher/2014/02/27/cybersquatters-rush-to-claim-brands-in-the-new-gtld-territories/.

[8] Jude A. Thomas, *Fifteen Years of Fame: The Declining Relevance of Domain Names in the Enduring Conflict Between Trademark and Free Speech Rights*, 11 J. Marshall Rev. Intell. Prop. L. 1 (2011)

[9] Gateway 2000, Inc. v. Gateway.com, Inc., 1997 U.S. Dist. LEXIS 2144 (W.D.N.C. Feb. 6, 1997)

 [ISSN 2581-5369]

In the most recent case, where the complainant was a company that provided entertainment products and services in the USA, they registered the REDBOX as their trademark in the USA and also registered redbox.com in the year 2000. later in the year 2019 another domain called eedbox.com was registered which also provided the same service as that of the complainant, hence the complaint was filed at WIPO Arbitration and Mediation Centre. The contentions of the complainant were that the respondent just replaced the word "r" with "e" and registered the domain name further it also provides the same service which is confusingly similar, they also brought to awareness of the fact that the respondents had 6 other cases of typo squatting which showed they had no legitimate interest and such registration was done in bad faith. The panel held in favor of the complainants stating that the respondents did not have any legitimate interest and such registration was not bonafide and held that this was a clear case of Typo squatting[10].

b. **Reverse Cybersquatting:-**reverse cybersquatting, in this the rightful or genuine trademark owners try to secure a domain name by threatening them with the claim of cybersquatting[11]. This often is done by the domain name owners who transfer the ownership of those domain names in order to avoid any legal actions against them. This type of Cybersquatting is usually done by larger organizations or companies by means of coercion trying to make smaller companies or organizations surrender their domain names. The uniform domain name dispute resolution policy defines it as the filing of a complaint in bad faith, resulting in the abuse of the UDRP administrative process[12].

Reverse domain name "hijacking" is a counter practice of domain squatting, where a particular company with a rightful Trademark claiming cybersquatting is trying to claim a domain name of another company[13]. But with the increasing number of cybersquatting, we realized that the actual owners would want to settle the matter rather than try to litigate such, the reason for this is such lawsuits may also end up with legitimate owners losing their domain name, these will lead to losing the purpose of filing the lawsuit[14], hence the UNDRP after considering the situation bought in a way wherein they could remove the discouragement of filing a law through rules according to which a complainant while filing at UNDRP needs to furnish certification certifying that the present complaint being filed with information is true and accurate to the best of the knowledge of the complainant, that the complaint has not been filed with a wrong cause

[10] Redbox Automated Retail, LLC d/b/a Redbox v. Milen Radumilo, Case No. D2019-1600 (WIPO Oct. 15, 2019).
[11] Sallen v. Corinthians Licenciamentos Ltda., 2002 U.S. Dist. LEXIS 19976 (D. Mass. Dec. 19, 2000), rev'd, 273 F.3d 14, 17 (1st Cir. 2001).
[12] Uniform Domain Name Dispute Resolution Policy Rules, para. 15(e) (2015).
[13] Dr. Daniel Dimov & Rasa Juzenaite, *Latest Trends in Cybersquatting*, Data Theft & Financial Fraud (Jan. 25, 2023, 8:27 PM), https://resources.infosecinstitute.com/latesttrends-in-cybersquatting/#gref.
[14] Schmidheiny v. Weber, 164 F. Supp. 2d 484, 487 (E.D. Pa. 2001).

 [ISSN 2581-5369]

or to harass, further the current complaint being applicable under the law and it must be in good faith[15], if the panel finds out that the complaint was in bad faith for example in case of reverse cybersquatting if the complaint was filed in order to extort the domain name or to harass the domain holder then the panel can declare the complaint was filed with bad faith and constitute an abuse of the administrative proceeding[16].

c. **Meta Tagging:-**Web pages are written in markup languages, usually HTML (Hyper Text Markup Language). when an internet user does an internet search based on the search HTML uses several tags and markups to display data based on the search and Tags the HTML sends signals across to the web operators to ensure the internet user gets the correct output which he/she wants. While most tags have visual and aesthetic functions, a tag category named meta-tags allows the internet to produce the data search based on the tags, these Tags are connected with the description of the said website through which the search engines are able to pull out the relevant website based on the description of the given website to the end user for example if a person presses the word hospital in the internet search based on these the Met tags they can produce search results with respect to hospital if the given website in its description has anything regarding the hospital, this is how met tags work.

There is an option to modify the HTML source code in a way that will favor the search engine optimization, The cyber squatter may manipulate and insert Trademark or met tags in there description which is very similar to that of the competitors so that when a consumer searches based on it then their website might end up popping up which will harm the goodwill of the competitor. In the USA the 1st case that arrived was with respect to a law firm that deals with domain-related disputes and sued the defendants under the Lanham Act who used met tags containing the terms ‘oppedahl’ and ‘larson’, which were the registered Trademark of the firm they did this to divert the Traffic to themselves so that they gain more clients. The court after analyzing the given situation held that they used the term without the authorization of the complainant due to which it resulted in unfair use under the Lanham Act[17]. The scenario in India is a bit different from that of the USA as we do not define what is met tags under the Trademarks Act but the Bombay high court while dealing with a domain name dispute where the Plaintiff had a registered domain which was shaadi.com which had become a quite well-known trademark in India so again to divert the traffic to themselves the Defendants were using

[15] Uniform Domain Name Dispute Resolution Policy Rules, para. 3(b)(xiii) (2015).
[16] Uniform Domain Name Dispute Resolution Policy Rules, para. 15(e) (2015).
[17] Oppedahl & Larson v. Advanced Concepts, Civ. No. 97-Z-1592 (D. Colo. July 23, 1997).

the domain name ShadiHiShadi.com so that the when an internet user searches for the plaintiff's related service then that would lead to the search being diverted to them, hence the single judge bench held it in favor of the plaintiff and also for the first time defined Met tags as "special lines of code embedded in web pages. All HTML, used in coding web pages, uses tags. They do not affect the page display. Instead, they provide additional information: the author of the web page, the frequency of updation, a general description of the contents, Copyright notices, and so on. They provide structured data about the web page in question[18].

III. CYBERSQUATTING LAWS IN INDIA AND UNITED STATES

A. India

In contrast to many developed nations, India lacks a domain name protection law, and cases of cybersquatting are handled under the Trade Mark Act, 1999. Notwithstanding the fact that Indian courts distinguish between trademarks and domain names; wherein the Hon'ble Supreme Court in has observed that the "The two work differently, which is where the difference resides. A trademark is safeguarded by the laws of the nation in which it may be registered. A trademark may therefore be registered more than once in different countries throughout the world. On the other hand, a domain name could be accessible regardless of the customers' actual locations because an internet connection is available worldwide. Due to the likelihood of universal connectivity, a domain name would need to be globally exclusive, and state laws might not be enough to successfully secure a domain name"[19].

There is no specific legislation in place regarding such hence they apply the Trade Marks Act's provisions to these cases. In addition, the Court in the Case noted :

"There is no legislation specifically mentioning domain name dispute resolution as far as India is concerned. However, even if the Trade Marks Act of 1999 does not operate outside India due to which the domain names might not get that much protection, This does not imply that domain names should not be legally protected to the utmost extent possible under the passing-off laws"[20].

Many cyber crimes are addressed by the Information Technology Act, 2000 of India and The Information Technology (Amendment) Act 2008, which also created a dedicated cybercrime cell. The Act, strangely, ignores the issue of domain name disputes and cybersquatting. Due to use and brand repute, domain names used in cybersquatting may be considered trademarks and

[18] People Interactive (I) Pvt. Ltd. v. Gaurav Jerry & Ors., NMS (L) No. 1504 of 2014 in Suit (L) No. 622 of 2014.
[19] Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd., A.I.R. 2004 S.C. 3540.
[20] Id at 26

 [ISSN 2581-5369]

as such come under the Trade Marks Act, 1999. Not all domain names, nevertheless, are registered trademarks.

Individuals with domain names registered as trademarks can seek relief under the Indian Trade Marks Act, 1999 which specifies additional civil remedies for situations of registered trademark infringement or passing off, such as an injunction, damages, or an account of earnings, as well as the delivery up of infringing products or damage to infringing goods. Additionally, it enforces punishment for using false trademarks or trade descriptions and punishment for selling goods or services bearing a false trademark or description, both of which are punishable by imprisonment for a term of not less than six months and not more than three years and by fines of not less than Rs. 50,000 and not more than Rs. 2 lakhs[21].

Further Uniform Domain Name Dispute Resolution Policy (UDRP) procedure established by the ICANN is primarily used to settle disputes regarding registrations made in bad faith. WIPO was created as a means of protecting and using intellectual property around the world and is the top ICANN authorized domain name dispute resolution service provider under the UDRP. India is one of the 171 countries that belong to the WIPO. An individual has the right to file a complaint with one of the administrative dispute resolution service providers recognized by ICANN under the UDRP[22].

Under the supervision of the National Internet Exchange of India (NIXI), India has also developed its own registry called INRegistry, where disputes relating to domain names are settled. Dispute Resolution Procedures (INDRP). The Policy was created in accordance with generally recognized best practices and the pertinent regulations of the Information Technology Act 2000. Conflicts are resolved under InRegistry. Regulations for IN Domain Name Dispute Resolution (INDRP) and INDRP rules and procedure. These regulations outline the process, costs, communications, and how to make a complaint.

Despite the fact that domain names are not specifically established by Indian law or regulated by any particular legislation, the Trade Marks Act of 1999 has been utilized in certain situations by Indian courts by considering to grant a remedy for cybersquatting by considering it as infringement or passing off like in the first case that was brought before the Indian courts engaged an effort to try to use the domain name "yahoindia.com" for Internet-related services instead of the original domain name, "yahoo.com." The court stated that typically the extent of mark similarity is vitally important and significant in an action for passing off because in such

[21] Trademark Act, 1999, § 104, No. 47, Acts of Parliament, 1949 (India).
[22] Uniform Domain Name Dispute Resolution Policy Rules, r. 4(a) (2015).

 [ISSN 2581-5369]

a case there is every chance and likelihood of confusion and deception being generated. Given that both domain names are nearly identical or similar in character, it is obvious that there is every chance that an Internet user could be misled into thinking that they are connected by a single source even if they are actually owned by two separate organizations[23].

Hon'ble High Court of Delhi Court held that "It is established law that when a defendant operates under a name that is sufficiently similar to the name under which the plaintiff is doing business and that name has developed a reputation, the general public may be led to believe that the defendant is the plaintiff or that the defendant's operation is a branch or department of the plaintiff, The existence of the plaintiff's goods with which the defendant attempts to confuse his own domain name is never a requirement for the defendant to be liable for a passing-off action. In situations when the plaintiffs do not really deal with the infringing goods, passing off may happen. There is a serious and significant risk of confusion and deception when the plaintiffs and defendants are competing in the same or similar fields of endeavor. The domain name has the same function as the brand and is not just an address or an Internet directory, so the plaintiff is subjected to the same protection as the trademark. The domain name serves as more than just an Internet address because it lets users know what kind of website they are visiting. In an Internet service, a specific Internet site could be accessed by anyone proposing to visit it regardless of where they are in the world. When it comes to services offered via a domain name on the Internet, strong oversight is required to ensure that anyone from anywhere in the globe can easily access and reach them. The complainant's trademarks and domain name "DR. REDDY'S" and "drreddyslab.com" are nearly similar. The degree of similarity between the markings is typically crucial and relevant in a passing-off action since there is a high potential that confusion and deceit would result in such a situation. Given the names of the two domains, It is pretty obvious that there is a chance that an Internet user could be mislead or perplexed into believing that the plaintiff controls both domain names when in fact they are registered to two different businesses[24].

B. United States of America

In 1999, Congress passed the Anti cybersquatting Consumer Protection Act ("ACPA") in order to protect consumers and businesses, further to also promote e-commerce businesses, further the requirement of separate legislation for cybersquatting was required to provide clarity with respect to Trademark law prohibiting Cybersquatting or abusive registration of a distinctive

[23] Yahoo! Inc. v. Akash Arora & Anr., 1999 II A.D. (Delhi).
[24] Dr. Reddy's Laboratories Ltd. v. Manu Kosuri & Anr., 2001 (58) D.R.J. 241.

trademark and internet domain in order to gain profit and goodwill and the reputation[25]. The ACPA establishes a civil remedy for the registration of a domain name that is identical to or "confusingly similar" to a distinctive or well-known mark with the intention of profiting from it[26].

Congress approved the ACPA after concluding that cybersquatting causes consumer fraud and public confusion, hinders e-commerce, robs legitimate trademark owners of earnings and goodwill, and lays costs on trademark owners[27], in1999. There was no definite barrier to cybersquatting before the ACPA. Although the Federal Trademark Dilution Act was effective in battling cyber squatters, Congress felt that additional legislation was required[28]. As a result, in November 1999, the ACPA was passed into law, making it unlawful to register, use, or otherwise transact in a domain name belonging to another if it is confusingly similar to or a renowned or distinctive brand. The law lists nine considerations for examining for assessing ill-faith intent. An injunction, damages transfer, forfeiture, or cancellation of the domain name are available. The plaintiff may elect statutory damages of $1,000- $100,000.

An in rem lawsuit is available in the district where the domain name registrar is located if the trademark owner cannot establish personal jurisdiction over the defendant or if, after using reasonable care, they are unable to locate the defendant. Domain name registrars who suspend, cancel, or transfer domain names in response to a court order or as part of the implementation of a legitimate anti-cybersquatting policy are given limited immunity from liability[29].

For US trademark owners whose brands are registered as domain names by alleged cyber squatters, both local and foreign, the ACPA provides a range of legal remedies. It claims to have prescriptive and adjudicative authority over international registrants. Looking first at the ACPA's provisions with respect to adjudicative jurisdiction, Part II focuses on 15 U.S.C. § 1125(d)(2). This provision lays down about authorizing the Trademark owner to cancel or transfer a domain name by going on with “in rem” against the domain name itself a trademark owner to seek cancellation or transfer of a domain name by proceeding "in rem" against the domain name itself in such cases the U.S courts cannot impose personal jurisdiction over the defendant. The text and history of the provision show that the congress had the intention to authorize in rem proceedings in cases where a foreign registrant has no contact with the U.S.

[25] J. Ryan Gilfoil, *A Judicial Safe Harbor Under the Anti-Cybersquatting Consumer Protection Act*, 1 Berkeley Tech. L.J., Annual Rev. of L. & Tech. 185, 185–208 (2005).
[26] 15 U.S.C. § 1125 (d) (2002).
[27] 15 U.S.C. § 1125 (d) (2002).
[28] Supra Note 24, at 33.
[29] 15 U.S.C. § 1125(d) (2002).

would make the court's assertion of personal jurisdiction on the registrant unconstitutional because of the due process clause. that Congress intended to authorize in rem proceedings in cases where a foreign registrant's lack of contacts with the United States would render a U.S. court's assertion of personal jurisdiction over the registrant unconstitutional under the Due Process Clause[30].

To succeed in an ACPA claim, the plaintiff must prove the important three elements: 1) the plaintiff's mark is distinctive or unique or famous; 2) the defendant's domain name which has been registered is identical or confusingly similar to the plaintiff's mark; and 3) The defendant had a bad faith intention to profit when they registered, traded, or utilized the domain name.

The Court of Appeals for the Second Circuit applied and interpreted the ACPA in the case in February 2000, making it the first appellate court to do so. Inc Sportsman's first used the "sporty" emblem in the 1960s, and in 1985, the U.S. Patent and Trademark Office officially registered "Sporty's" as a trademark. "Sportys.com" is a domain name that Omega registered; The co-owner of Omega was conscious of the "Sporty's" brand. Sporty's Farm, an entirely owned subsidiary, purchased the domain name from Omega. Sporty's Farm sued to keep using Sportys.com when Sportsman's talked about registering the domain name in 1996. Under the Federal Trademark Dilution Act, Sportsman's counterclaimed for trademark infringement and dilution ("FTDA"). The district court ordered Sporty's Farm to give up all ownership rights to Sportys.com after finding that Sporty's Farm had violated the FTDA. The court of appeals ruled that the law to be applied is the law in effect at the time of the appeal and applied the ACPA, which was passed while the appeal was ongoing. The court had to first decide if "Sporty's" is a famous or distinctive brand before applying the ACPA. According to the court, it is both. After then, the court had to determine if the domain name "Sportys.com" is the same as or confusingly similar to the "Sporty's" mark.

According to the court, they are confusingly similar. The next step was for the court to decide if there was a bad faith purpose to profit. According to the court, "the record below contains more than enough proof of 'bad faith intent to benefit,'" As a result, Sporty's Farm broke the ACPA, and the district court's injunction was appropriate. In this way, the first appellate ruling affirmed a court order prohibiting a company from registering a third party's trademark as a domain name[31].

[30] Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 Vand. L. Rev. 309, 311 (2002).
[31] Sporty's Farm L.L.C. v. Sportsman's Market, 202 F.3d 489 (2d Cir. 2000).

 [ISSN 2581-5369]

IV. CONCLUSION AND SUGGESTION

As a result of cybersquatting's increased prevalence in the modern world, it has been referred to as a kind of modern extortion and is now taken seriously by the judicial system. In an effort to settle conflicts in this area, the United States passed the ACPA in 1999. Nevertheless, India does not have any legislation that specifically addresses cyber-squatting. All cyber-squatting proceedings in India are decided based on trademark law, which is unavoidably ineffective.

The focus shouldn't be on looking at every disagreement from a trademark perspective because not always going to court would be best because it wastes a ton of time and money. Thus, India urgently needs new legislation that would address cyber-squatting in particular. Although the Information Technology Act and other legislation do not contain any specific laws addressing cyber-squatting, the courts have used trademark law to resolve these domain name disputes. Courts frequently need to consult English and American statutes and rulings for guidance. Hence, a law like the ACPA, as it exists in the US, is necessary for the modern world. Additionally, it is important to make decisions made by the WIPO Arbitration and Mediation Center and ICANN regarding domain name disputes enforceable on Indian courts. Doing so will assist relieve the strain on the already overworked Indian court system. Finally, the likelihood of future conflicts may be significantly decreased if the registrar conducted certain background checks before assigning the domain name, hence reducing the likelihood of a dispute. Another option is to publish the pending domain names in a journal, similar to how trademarks are published in the trademark journal. Such methods of combating cyber- squatting would significantly reduce and eliminate domain name conflicts[32]. In the context of the internet, where parties from all over the world can communicate with one another with the click of a mouse, online litigation is frequently inconvenient, impractical, expensive, and time-consuming. Giving online dispute resolution options could help resolve complaints and boost consumer trust in online shopping. ADR (Alternative Dispute Resolution) is crucial in this situation. The WIPO established the ICANN Policy, a mechanism of online domain name dispute resolution, to settle conflicts with domain names. This method is not only quicker, but also more economical. ICANN approved the Unified Domain Name Dispute Resolution Policy on October 24th, 1999. This regulation outlines an efficient administrative procedure for resolving disagreements over improper and malicious domain name registration. A domain name may be canceled, suspended, or transferred by the Registrar As of today, the plaintiff must

[32] IPLEADERS, *Cybersquatting in India*, https://blog.ipleaders.in/cybersquatting-in-india/ (last visited Mar. 20, 2025).

submit a complaint to a provider of approved dispute resolution services.

The Anti Cybersquatting Consumer Protection Act of the United States is a significant example that expressly relates to cyberspace, even if it is still founded on conventional legal principles of trademark law. Additionally, and probably more significantly, it alludes to the domestic law's jurisdictional parameters, which are determined by actual territorial boundaries. This regulation ignores the international character of cyberspace and reads as if there are only US internet users. Since there are no geographical restrictions on access to the internet, a domain name may be reachable regardless of the users' whereabouts, according to the ACPA in the Satyam case in India. A domain name may not be sufficiently protected by national legislation. International regulation of the domain name system was necessary to close the gap (DNS). This international law was put into effect by the World Intellectual Property Organization (WIPO) and the Internet Corporation for Assigned Names and Numbers (ICANN). India ratified international law, hence the procedure should be respected if Indian law is unable to bring the issue to light on the national level[33].

Even though there is a separate legislation with respect to Cybersquatting in the United States it also has its lacuna which has been addressed The authors of the ACPA anticipated that the remedies outlined in the act would be ineffective if the plaintiff was unable to identify the registrant. In order to avoid being identified and served with legal documents by the mark owner, many cyber squatters register domain names under aliases or otherwise provide false information in their registration applications, according to the House Committee report. This presents a significant problem for trademark owners fighting cybersquatting[34].

Federal courts have always disfavoured lawsuits against anonymous defendants, and in order to properly serve the defendant with legal documents, the plaintiff must often identify and locate the defendant. The issue of anonymous defendants is illustrated by a case brought before the ACPA Due to the domain names seescandy.com and seecandys.com being registered by "someone other than the plaintiff," the assignee of many trademarks connected to See's Candy Stores, Inc., filed a lawsuit in federal court. The plaintiff was unable "to gather the information necessary to serve the lawsuit" on the registrant because the registrant had submitted inaccurate or incomplete information while registering the domain names. But, it weighed this need against "the legitimate and valuable right to participate in internet forums anonymously." The district

[33] MONDAQ, *Cybersquatting: Regulatory Mechanisms*, https://www.mondaq.com/india/trademark/1143202/cybersquatting--regulatory-mechanisms (last visited Mar. 5, 2023).

[34] Catherine T. Struve & R. Polk Wagner, *Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act*, 3 Berkeley Tech. L.J., Annual Rev. of L. & Tech. 989, 989–1041 (2002)

 [ISSN 2581-5369]

court acknowledged the plaintiff's need to determine the registrant's identity[35].

The in rem section of the ACPA eliminates the requirement to identify an evasive registrant, thus resolving the issue of anonymous defendants. If a mark owner cannot locate a domain name registrant and has an ACPA claim against the registrant, the owner may sue the domain name itself by sending notice to the postal and email addresses the registrant gave to the dealer. The due process requirements for notice of litigation are satisfied by the Act's requirements that the plaintiff send the notice to the addresses provided by the registrant and by the additional need that the plaintiff post notice of the case. Consequently, the in rem provision bears the potential of "offering] real protection to trademark owners while balancing the values of privacy and anonymity on the Internet" in cases where the registrant cannot be identified[36].

The ACPA's drafters aimed to address the issue of anonymous registrants as well as instances in which "a non-U.S. resident cyber squatters on a domain name that infringes upon a U.S Trademark.". In order to do this, the ACPA stipulates that the in rem action is also possible. The issue with this clause is that there are no instances of overseas cybersquatting for which § 1125(d)(2)(A)(ii)(I) is both applicable and constitutional, as we show below. In Part II, we go through this. C.L., there must be a basis for jurisdiction and constitutionality in the exercise of such jurisdiction for a court to have geographical jurisdiction in a specific case. According to a study of the relevant rules, there will always be a basis for in personam jurisdiction over ACPA claims against overseas registrants if the exercise of such jurisdiction is legal, Hence, Part II.C concludes that the exercise of in rem jurisdiction in any ACPA case where the exercise of in personam jurisdiction would contravene due process will also be illegal[37].

*****

[35] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577–78 (N.D. Cal. 1999).
[36] Catherine T. Struve & R. Polk Wagner, Realspace Sovereigns in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act, 17 Berkeley Tech. L.J. 989 (2002)
[37] Shaffer v. Heitner, 433 U.S. 186 (1977).

 [ISSN 2581-5369]