Page 1024 - 1035 **DOI:** *https://doij.org/10.10000/IJLMH.1112114*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Cybersquatting and Trade Name Protection in Online Advertising: A Comparative Legal Study of EU, USA and India

MAHEK PONIA* AND DR. LAKSHMI PRIYA VINJAMURI**

ABSTRACT

The rapid growth of digital commerce has made domain names more valuable as important business identifiers. However, this also makes cybersquatting and trade name abuse more likely in online ads. This article compares the laws in the US, India, and the EU that protect trade names and stop cybersquatting. It looks at how cybersquatters use domain names and advertising methods, like misleading URLs and search engine marketing, to steal customers, hurt brand value, and make money illegally. This study analyzes significant legal frameworks, including the Uniform Domain Name Dispute Resolution Policy (UDRP), the Anti-Cybersquatting Consumer Protection Act (ACPA) in the United States, the trademark and unfair competition laws of the European Union, and the Trademark Act and Information Technology Act of India. The essay shows how the legal systems in different places are similar and different by looking at how courts have ruled in the past and how laws are enforced. It also looks at how well the current solutions deal with the new problems that online advertising causes. The article's conclusion proposes harmonized and technologically astute legislative measures to enhance trade name protection and effectively combat cybersquatting in the global digital economy.

Keywords: *Cybersquatting, domain names, online advertising, comparative law, UDRP, ACPA, trademark law, digital commerce, the EU, the US, and India.*

I. INTRODUCTION

The internet has changed the way people do business around the world, and domain names are now important tools for advertising and having an online presence. A domain name serves as a reflection of a brand's identity and goodwill in addition to being an address.

* Author is a Student at Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.
** Author is a Professor at Uttaranchal University, Dehradun, Uttarakhand, India.

 [ISSN 2581-5369]

Cybersquatting, in which people register domain names that resemble well-known trademarks in order to profit from their economic worth, has also resulted from this change. Trademark owners and domain name registrants engage in legal issues as a result. Recent developments in the field of digital and intellectual property have led to the emergence of a new issue known as "cybersquatting," a portmanteau that refers to the act of "squatting" or rather holding onto a domain name. Since many laws around the world judge criminal cases under the guise of "bad faith," there have been several discussions about whether the trademark rules now in place are sufficient to decide these cases. As a result, many nations are starting to or have already developed specific laws against cybersquatting, most notably the Anti cybersquatting Consumer Protection Act (ACPA) in the UnitedStates. Cybersquatting has also become more common in India since the historic Yahoo!, Inc. v. Akash Arora case; the 2023–2024 JioHotstar.com dispute is one recent example.

Because of the internet's global reach, cybersquatting poses special legal issues that call for both domestic and global answers. The ways that various governments handle these problems are examined critically in this essay.

II. THE NOTION OF CYBERSQUATTING

Cybersquatting is the registration, trafficking, or use of a domain name with the malicious intent to profit on the goodwill of another party's trademark.

A. Characteristics of Cybersquatting

- **Similarities that confound or are identical:** The domain name is either similar or identical to a trademark, brand name or name of a famous person which can confuse users. People may think the website is owned by the original owner. Example includes “amaz0n.com” instead of “amazon.com”.
- **Lack of a valid interest:** The registrant of the domain name has no legitimate interest or right to use that name or a lawful purpose for doing so. They are not licensed by the trademark holder, nor do they go by that name as a matter of general knowledge.
- **Bad faith (Wilful):** The domain is registered with evil intent, such as reselling it to the owner at a high price, misleading customers, damaging a competitor’s reputation or profiting from confusion.

B. Kinds of Cybersquatting

- **Type of squatting**[1]

This involves registering domain names with small spelling mistakes or typing errors of popular websites to attract users accidentally. Example: "gooogle.com" instead of "google.com".

Squatting based on identity: In this type, a person registers the name of a celebrity, company, or well-known individual as a domain name without permission to gain profit or attention.

Reverse cybersquatting: This occurs when a trademark owner falsely accuses a legitimate domain holder of cybersquatting in order to take control of the domain name unfairly.

III. THE SIGNIFICANCE OF TRADEMARK LAW IN CYBERSQUATTING

This section of the article serves as a review of the literature and includes: an overview of international and Indian standards for assessing trademark and domain name disputes; an analysis of the current application of Indian law to cybersquatting cases; a proposal for standardizing the classification of different types of cybersquatting; and an identification of the shortcomings in these legal remedies.

A. Global trademark regulations

In collaboration with the World Trade Organization, the World Intellectual Property Organization currently upholds global trademark standards and arbitration. As a result, several internationally recognized rules are used to decide international disputes. These include the TRIPS agreement, which specifies minimum conditions for trademark qualification, and the Madrid System for the International Registration of Marks.

Since they were first created in 1989, the [2]Madrid System and the TRIPS quotas have been changed and improved. This has led to an internationally accepted standard for arbitration. People have been very critical of these protocols, especially TRIPS, because their rules for enforcement are not clear. This makes it hard to put the suggested frameworks into action. WIPO and the International Corporation for Assigned Names and Numbers (ICANN) also work closely together on issues related to internet domain name registration and digital intellectual property rights. This makes it possible to decide cases of cybersquatting. The United States' Anti-Cybersquatting Consumer Protection Act (ACPA) and India's Indian Trademarks Act, 1999 are two examples of laws that each country uses to look at cybersquatting cases.

[1]Manisha Singh & Shubham Kumar, *Cybersquatting: Trademark Protection in Cyberspace*, 3 Indian J. Intell. Prop. L. 78 (2011).
[2] McCarthy on Trademarks and Unfair Competition, J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 25A:50 (5th ed. 2024).

B. Indian Standards of Trademarking

[3]The Trademark Act of 1999 is India's national law that governs trademark management. It has been changed to follow the basic rules of TRIPS, which means that Indian trademark law is now in line with TRIPS standards.This Act covers the process of registering a trademark in India, the rights that come with it, and a full understanding of what counts as an infringement and what rights you have against it (Jain et al., 2024). It also includes a number of important steps to stop trademark abuse, such as protecting well-known, already-registered trademarks from being diluted by companies that infringe on them, making it illegal to use certification marks to make sure that branded property meets standards like AGMARK and ISI, and registering marks that could trick, confuse, or hurt the public.

Trademark squatting is on the rise right now, which shows that the Indian laws against trademark infringement aren't working as well as they could. The first business or party to register a trademark is considered to be its owner under India's first-to-file arbitration system. This has resulted in the issue of trademark squatting, namely cybersquatting, which allows anyone to register trademarks in bad faith with the goal of selling these rights for huge sums of money. India presently relies on decisions and verdicts of cases in the sector under trademark laws rather than having explicit legislation against cybersquatting, in contrast to the United States of America, which has specific legislation known as the ACPA to combat this crime.

C. Combating cybersquatting with Indian Frameworks

[4]As previously stated, India has not yet passed any laws specifically addressing cybersquatting. However, courts have applied current trademark laws in contemporary situations, such as the previously stated "Indian Trademarks Act, 1999." In the Section 29 which addresses fraudulent trademark transformation and declares it to be a violation. These consist of any trademarks that might trick and mislead the people into thinking that a trade name is held by a well-known or established company when in fact it is not. The IT Act's Sections 43 and 66 address illegal access to and damage to computer systems and data.

Furthermore, the Hon'ble Court have established in [5]Yahoo Inc. v. Akash Arora & Anr that in addition to being an internet address, domain names can function as company identities, allowing the application of traditional trademarking standards in the context of cybersquatting.

[3] Trade Marks Act, No. 47 of 1999, India Code (1999).
[4] S. K. Verma, *Domain Name Disputes and Trademark Protection on the Internet*, 44 J. Indian L. Inst. 259 (2002).
[5] Yahoo! Inc. v. Akash Arora, 1999 PTC 201 (Del.).

 [ISSN 2581-5369]

D. Legal and Literature Deficits in Cybersquatting

India's approach to cybersquatting is still inconsistent and not well thought out, even after a number of important court decisions. This is mostly because there are no specific laws that deal with this problem. Unlike the Anti cybersquatting Consumer Protection Act [6](ACPA) in the United States, Indian law does not have a clear way to determine bad faith in domain name disputes. Because of this, courts often use the passing off doctrine and the Trade Marks Act (1999), which were made for traditional trademark disputes. This method relies on consumer confusion and goodwill, which are often hard to prove in cybersquatting cases. This makes relying on passing off even harder. Because there isn't clear statutory support, court decisions about domain names have mostly been based on interpretation, which has led to results that are inconsistent and hard to predict. Also, Indian law doesn't have strong remedies for cybersquatting, and measures like statutory damages or streamlined domain recovery procedures make enforcement and deterrence less effective. Thus, it is obvious that utilizing international anti-cybersquatting frameworks would assist Indian law in developing more efficient and open legislation.

E. Cybersquatting Case Type Classification

[7]Current terms cover a lot of different kinds of cybersquatting, but there isn't a single set of categories that covers all of them. Because there isn't a standard way to do things, it's hard to spot and deal with the many ways that cybersquatters use, such as stealing domains, phishing, typosquatting, and bad-faith registrations. Such disputes could be better understood, regulated, and resolved with the help of a widely approved classification system.In order to address this problem, the f unique framework that defines categorization labels, provides meanings for these categories, and offers actual case studies to support the proposed descriptions.

IV. THE USA'S METHOD FOR FIGHTING CYBERAQUATTING

In 1999, the Lanham (Trademark) Act was supplemented with the Anticybersquatting Consumer Protection Act (ACPA), is the main tool used in the US to combat cybersquatting. [8]Trademark owners can sue companies that register, use, or traffic in a domain name that looks like or weakens a registered brand or service mark thanks to this law. The ACPA defines

[6] Anti cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (1999).
[7] Chandra, R., & Bhatnagar, V. (2019). Cyber-squatting: A cyber crime more than an unethical act. International Journal of Social Computing and Cyber-Physica Systems2 146–150
[8] David Lindsay, *International Domain Name Law: ICANN and the UDRP*, 24 Eur. Intell. Prop. Rev. 102 (2002).

cybersquatting and lists the legal options that trademark owners have, such as money damages, injunctive relief, and, in some cases, legal costs.

A. Crucial Clauses and Legal Measures

The ACPA says that damages for each domain name in a civil lawsuit can be between $1,000 and $100,000. It lets people or groups that are involved in cybersquatting sue each other in civil court.

When the domain registrant can't be found, the [9]ACPA's rules for in rem proceedings against the domain name itself help to settle disputes.

Defenses and Fair Use:[10] The law also takes into account the "fair use" theory, which shields anyone who use domain names for justifiable activities like news reporting, criticism, or commentary without intending to unfairly profit from a trademark's well-established reputation.

The ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP), which provides an alternate, less onerous method of addressing disputes outside of the conventional court system, complements the efficacy of the ACPA.This dual strategy, which combines arbitration procedures with legal action, is an all-encompassing method to successfully prevent cybersquatting and protect persons and organizations from potential abuses in domain name registrations.

B. Important cases of cybersquatting in the USA

Let's look at some interesting case studies to learn more about how well cybersquatting law works:

1. [11]Facebook v. Face-book.com: In 2011, Facebook sued the person who owned the domain name Facebook.com because they were using it to send people to a different website. After the court ruled in favour of Facebook, it was given damages and told to transfer the domain name that was infringing. This shows how social media can be proactive.
2. [12]Apple vs. AppleStory.com: In 2009, a third party registered the domain name AppleStory.com, which could have been a threat to Apple Inc. Apple's successful case to transfer the domain name showed how important it is to protect trademarks and enforce cybersquatting laws.

[9] Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (1999).
[10] McCarthy on Trademarks and Unfair Competition, J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 25A:50 (5th ed. 2024).
[11] Facebook, Inc. v. OnlineNIC Inc., No. 5:19-cv-07071 (N.D. Cal. 2019).
[12] Apple Inc. v. Domain Admin, WIPO Case No. D2011-1390 (2011).

 [ISSN 2581-5369]

V. THE CYBERSQUATTING LAW FRAMEWORK OF THE EUROPEAN UNION

The European Union (EU) doesn't just rely on one rule for cybersquatting; instead, it uses a multi-layered, harmonized legal system. To protect trade names and settle domain name disputes, a mix of national legal systems, [13]EU-wide trademark rules, and special procedures for resolving disputes are used. This mixed structure is an example of the EU's main legal idea of finding a balance between consistency and the power of member states.

A. The Main Basis of EU Trademark Law

The EU Trade Mark Regulation (EUTMR), Regulation (EU) 2017/1001, is the basis for EU cybersquatting laws. This rule gives registered EU trademark owners special rights, such as the ability to stop other people from:

Using signs that are very similar or the same in business, taking advantage of a well-known brand's reputation, and making it more likely that customers will get confused.

[14]Domain names are not officially classified as trademarks, but they are considered commercial identifiers when used in online advertising. So, this could mean:

Taking advantage of a brand's or trademark's reputation without paying for it. The Court of Justice of the European Union (CJEU)[15] has made decisions that support this interpretation.

B. What the European Union Court of Justice (CJEU) does

The CJEU has had a big impact on cybersquatting law by applying traditional trademark rules to the digital world. [16]Arsenal Football Club plc v. Reed (2002) is an important case. The Court ruled in this case that using a trademark in business without permission, even outside of normal advertising channels, may be considered infringement if it gets in the way of the trademark's main purpose, which is to show where something came from.

This idea has been used in cybersquatting cases, where domain names are used to trick customers or send traffic to the wrong site. Louis Vuitton versus Google France SARL (2010). The Court made it clear that using trademarks in online settings, like domain names and ads, must not cause confusion or give one side an unfair advantage, even though it focused on keyword advertising. These decisions show that EU trademark protection covers the wrong use of trade names and trademarks online, even through domain names.

[13] David Bainbridge, *Intellectual Property* 702–15 (11th ed. 2022).
[14] Tanya Aplin & Jennifer Davis, *Intellectual Property Law: Text, Cases, and Materials* 918–30 (3d ed. 2021).
[15] Court of Justice of the European Union.
[16] Arsenal Football Club plc v. Reed, Case C-206/01, [2003] Ch. 454 (ECJ).

 [ISSN 2581-5369]

C. Laws in all Jurisdiction

Different countries, including the United States, the European Union, and India, have quite different laws governing cybersquatting and trade name protection in internet advertising. Although the commercial value of domain names is acknowledged by all three systems, their legal responses differ in terms of court interpretation, enforcement procedures, and statutory clarity.

- **In USA**

With[17] 1999's Anticybersquatting Consumer Protection Act (ACPA)[18], the United States takes a statutory and enforcement-focused strategy. Cybersquatting is clearly defined by the ACPA, which also offers remedies for bad faith domain name registration .The ACPA requires a plaintiff to prove:

Possession of a well-known or unique trademark, Profit-seeking in malice Using or registering a confusingly similar domain name.

The Act is one of the most complete frameworks in the world because it offers powerful remedies, such as statutory damages and in rem jurisdiction. To further improve protection in online advertising environments, the Lanham Act also regulates unfair competition and trademark infringement.

- **The European Union**

The European Union has a complex legal system that depends on:

The EU Trade Mark Regulation is Regulation (EU) 2017/1001. (EUTMR). Laws pertaining to unfair competition and trademarks Mechanisms for Alternative Dispute Resolution (ADR) for ".eu" domains The EU does not have a specific cybersquatting law, in contrast to the USA. Rather, consumer protection laws and trademark infringement concepts are used to handle domain name disputes[19].

The Court of Justice of the European Union (CJEU) has a big impact on the EU framework because it expands trademark protection in online situations like domain names and digital advertising.

- **In India**

There isn't a specific legal framework in India that addresses cybersquatting. Rather, protection

[17] J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition* § 25A:50 (5th ed. 2024).
[18] Anti cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (1999).
[19] David Lindsay, *International Domain Name Law: ICANN and the UDRP*, 24 Eur. Intell. Prop. Rev. 102 (2002).

 [ISSN 2581-5369]

stems from:

1. Information Technology Act of 2000[20]
2. Trade Marks Act of 1999[21]

Common law principles for passing off. Trade names have been accepted by Indian courts as company identifiers on par with trademarks. But rather than being codified, enforcement is still mostly decided by judges. India also adheres to the Trade Name Dispute Resolution Policy (INDRP) is founded on international norms but lacks the substance of statutory remedies.

VI. FINDINGS AND COMPARATIVE ANALYSIS

Significant variations in the efficacy of legal frameworks are revealed by the comparative analysis.

A. Explicitness and Codification

- **American States:** The Anticybersquatting Consumer Protection Act (ACPA) provides a clear and specific legal definition of cybersquatting. It explains what amounts to bad-faith registration and gives trademark owners strong legal remedies. This ensures greater certainty and uniformity in legal proceedings.
- **United Nations:** The United Nations does not have a specific international law directly regulating cybersquatting. However, international trademark protection is supported through harmonized intellectual property principles and agreements, helping countries cooperate in resolving disputes.
- **Asia:** Many Asian countries lack a dedicated statutory framework specifically dealing with cybersquatting. Because of this, courts often rely on trademark laws and judicial interpretation to decide cases, which can create ambiguity and inconsistency in decisions.[22]

Locating: In comparison, India's framework is less predictable and certain.

B. How to Handle Bad Faith

- **USA:** In the United States, bad faith in cybersquatting is clearly identified through statutory standards under the Anticybersquatting Consumer Protection Act. Courts examine factors such as intent to profit, misleading consumers, or selling the domain name to the trademark owner.

[20] Information Technology Act, No. 21 of 2000, India Code (2000).
[21] Trade Marks Act, No. 47 of 1999, India Code (1999).
[22] B.L. Wadhera, *Law Relating to Trademarks, Trade Names, Copyright and Geographical Indications* 421–34 (5th ed. 2016).

 [ISSN 2581-5369]

- **EU:** In the European Union, bad faith is mainly interpreted through unfair competition principles, trademark laws, and judicial precedents[23]. Courts analyze the conduct and intention of the domain holder based on case law.

- **India:** In India, there is no separate legislation specifically defining bad faith in cybersquatting. Indian courts determine bad faith based on judicial interpretation, trademark principles, and the facts of each individual case.

Locating: India's strategy is the most flexible, but it's not always the same; the US strategy is the most strict.

C. Effect on Online Advertisement

- **USA:** In the United States, strong legal protection against cybersquatting provides better security for online advertisements and branded websites[24]. Clear laws reduce misuse of domain names and protect businesses from consumer confusion.

- **EU:** The European Union follows a balanced approach that protects both businesses and consumers. Trademark laws and unfair competition principles help maintain trust in online advertising while ensuring fair market practices.[25]

- **India:** In India, the absence of a specific cybersquatting law creates legal loopholes. This increases the risk of misuse of domain names, which may negatively affect online advertisements, brand reputation, and consumer trust.[26]

Locating: The system in place in India doesn't do as good of a job of protecting digital advertising ecosystems.

VII. DOMAIN MANAGEMENT AND PROTECTING BRAND

When it comes to digital identity, protecting a brand's online presence is just as important as protecting data. Monitoring your brand online can help you avoid threats and see potential problems before they happen. Also, defensive registrations and blocking services are very important because they protect trademarks by stopping illegal people from registering domain names with more than 240 extensions. The Anticybersquatting plays an important role. The

[23] Milton Mueller, *Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy*, 17 Info. Soc'y 151 (2001).
[24] Jacqueline D. Lipton, Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution, 23 Harv. J.L. & Tech. 447 (2010).
[25] British Telecomms. Plc v. One in a Million Ltd., [1999] 1 W.L.R. 903 (CA).
[26] Shubham Sharma, Cybersquatting and Protection of Domain Names in India, 8 Indian J.L. & Tech. 55 (2019).

1999 Consumer Protection Act (ACPA)[27] makes cybersquatting illegal and lets trademark owners get money damages and transfer or end domain names that are infringing.

VIII. SERVICE FOR ADVANCED DOMAINS AND ENFORCEMENT ACTIONS

To better protect digital identities, businesses need to think about domain purchase services and full domain name portfolio management. These services keep businesses' valuable digital assets safe and act as their eyes, ears, and enforcers, letting them focus on their main business operations. Sending stop and desist letters and other enforcement actions are very effective at stopping cybersquatters and also help settle disputes peacefully.[28] Making all decisions in these acts public boosts customer trust and makes sure that they have a real brand experience.

IX. CONCLUSION

Through this in-depth look at cybersquatting, its effects on digital identity security, and the different ways to fight it in India, the USA, and the European Union, we have stressed how important it is to have strong legal frameworks and preventative measures. The report says that strategic registration, legal vigilance, and cutting-edge technical solutions are all important ways to protect trademarks and personal names from being misused. The comparative study stresses the effectiveness of laws like the ACPA in the US and points out the chances and problems that come with the Indian legal system in order to better fight the growing problem of cybersquatting.[29] It also says that there needs to be more cooperation between countries and more consistent legal standards.

As cybersecurity and privacy policies improve and more people use blockchain technology for self-sovereign identities, digital identity protection will get better and more focused on users. The work of international organizations and new global trends in digital identity verification suggest that there is a good chance of lowering the risks associated with cybersquatting. It also shows how important it is to stay alert, work together, and be flexible in both legal and technological responses in order to protect digital identities across borders.

X. SUGGESTIONS

1. **Public awareness and Education:** Businesses can protect themselves by teaching people about the risks of cybersquatting and how to keep their digital identities safe.

[27] Anti Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (1999).
[28] S. K. Verma, *Domain Name Disputes and Trademark Protection on the Internet*, 44 J. Indian L. Inst. 259 (2002).
[29] R. Polk Wagner & Catherine T. Struve, Realspace Sovereigns in Cyberspace: The Case of Domain Names, 19 Santa Clara Comput. & High Tech. L.J. 799 (2003).

 [ISSN 2581-5369]

You need to know about the different types of cybersquatting, such as cyberpiracy and brandjacking.

2. **Proactive Domain Management:** Companies should register brand variations as domain names and make use of monitoring services to quickly identify possible cybersquatting activity.
3. **Working together with other countries:** Countries should try to make legal rules on cybersquatting the same through international treaties in order to improve their ability to enforce laws across borders. Organizations like ICANN[30] and WIPO[31] help settle most international cybersquatting disputes.
4. **Using Advanced Technologies:** Using technologies like blockchain for self-sovereign identity management and biometric verification can make it much harder for people to cybersquat. These technologies can stop people from registering domain names for bad reasons.
5. **Higher Penalties for Offenders:** Stricter penalties for proven cases of cybersquatting can stop people from doing it, encourage people to follow trademark rules, and protect the integrity of brands. This would help businesses avoid damage to their finances, their reputation, and the law.

*****

[30] Internet Corp. for Assigned Names & Numbers (ICANN), Uniform Domain Name Dispute Resolution Policy (1999).
[31] World Intell. Prop. Org. (WIPO), The Management of Internet Names and Addresses: Intellectual Property Issues (1999).

 [ISSN 2581-5369]