International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 8, Issue 10
October, 2025
Pages: 19-39

A Comparative Analysis of Cybersquatting Policies in India, the US, and Canada

Aadi Chakraborty

The British School, New Delhi, India

aadi.chakraborty@gmail.com

http://dx.doi.org/10.47814/ijssrr.v8i10.2996

Abstract

Cybersquatting—a cybercrime involving the registration of internet domain names in bad faith—has become an increasingly complex legal challenge worldwide with the rise of internet usage. However, lacking dedicated legislation or standardized bad faith criteria, Indian courts struggle to deliver consistent rulings and rely on existing trademark policies and doctrines—most notably the principle of passing off. This creates uncertainty for brand owners and enables domain name abuse, particularly in cases involving non-registered marks or cross-border disputes. To examine and propose solutions to this issue, this paper addresses the research question: "How do countries approach cybersquatting, and what lessons can India draw from foreign legislation?" It argues that India must draw on structured foreign anti-cybersquatting frameworks, such as those of the United States and Canada, to develop clear statutory definitions of key principles—namely bad faith—and monetary and non-monetary remedies. While legal scholars broadly agree on the need to modernize cybersquatting frameworks globally, detailed, country-specific reforms for India remain scarce. This paper offers a comparative legal analysis between the U.S., Canada, and India, focusing on three key points: understandings of bad faith, provision of remedies, and assessment of parody cybersquatting cases. Following this analysis, the paper identifies five key gaps and corresponding reforms in India's legal approach to cybersquatting: enacting a specific anti-cybersquatting statute to reduce inconsistencies in rulings and address cases involving non-registered marks where trademark law is inadequate; introducing statutory damages to ensure compensation even when losses are hard to quantify; allowing in rem actions against domain names where registrants are unidentifiable or beyond the court's reach; providing a clear definition of bad faith with flexible assessment criteria to guide consistent rulings; and adopting a model law approach to promote international uniformity and offer a long-term solution to cross-border cybersquatting disputes.

Keywords: *Cybersquatting; Trademark Law; Intellectual Property Law; Domain Name Disputes*

1 Introduction

Trademarks have existed since the dawn of human civilization, with cases of ancient Egyptians using similar 'personal marks' to establish their intellectual property (VerSteeg, 2018)[i]. Similarly, denominations of trademark law have evolved over centuries, since trademarks act as the predominant manner of ensuring one's property remains secure. The Egyptian concept of personal marks persisted through Greek and Roman civilizations (Rogers, E.S., 1910)[ii], evolving into guild marks during medieval Europe to guarantee product quality and trade regulation. The Industrial Revolution necessitated standardized protections for trademarks due to mass production and global trade. This led to policies such as 'The Trade Marks Act, 1999[1], and the Madrid Protocol, 1989 (WIPO, 2007)[iii], which are examples of current Indian and international standards upon which arbitrations are conducted respectively.

Modern changes in the field of digital and intellectual property have led rise to a new issue, labelled as 'cybersquatting', a portmanteau connoting the act of 'squatting' of or rather holding on to, a domain name[2]. Cyber-squatting or domain squatting is the act of registering a domain with the primary objective of gaining profit or any other intention of bad faith (Chandra et al., 2019)[iv]. With many legislations around the world judging cases of crime under the pretense of 'bad faith', many debates have emerged regarding whether existing laws surrounding trademarking are adequate to judge these cases. Thus, many countries are beginning to, or have already, built specified policies against cybersquatting - notably the United States' Anticybersquatting Consumer Protection Act (ACPA). Since the landmark case of Yahoo!, Inc. v. Akash Arora, cybersquatting has been growing increasingly prevalent in India as well, with recent examples including the 2023–2024 JioHotstar.com dispute.

Therefore, this study seeks to address the research question: "How do countries approach cybersquatting, and what lessons can India draw from foreign legislation?". To answer this question, this paper aims to: review existing literature and frameworks to examine the relationship between trademark law and cybersquatting; classify the key forms of cybersquatting; analyze the legal frameworks currently used in India, the United States, and Canada; and propose suggestions to strengthen India's legislative response to cybersquatting.

2 Trademark Law and Its Implications for Cybersquatting Cases

This section of the paper serves as a literature review and includes: an overview of international and Indian standards for assessing trademarks and domain name disputes; an analysis of how current Indian legislation is applied to cybersquatting cases; a proposal for the normalized classifications of different types of cybersquatting; and the identification of the shortcomings of these legal responses.

2.1 International standards of trademarking

The World Intellectual Property Organization[3] in collaboration with the World Trade Organization, currently upholds international standards and arbitration concerning trademarking. Thus, international cases are judged based on several internationally agreed regulations. These include the TRIPS agreement[4] which describes minimum standards of qualification for trademarks, and the Madrid System for the International Registration of Marks.

[1] The Trademarks Act, 1999: "An Act to amend and consolidate the law relating to trade marks, to provide for registration and better protection of trade marks for goods and services and for the prevention of the use of fraudulent marks."

[2] WIPO is internationally recognized as the leading provider for cybersquatting-related disputes

[3] WIPO, 1967, Article 3 - WIPO was established in 1967 by the WIPO Convention, which states that WIPO's objective was "to promote the protection of intellectual property throughout the world…"

[4] TRIPS stands for "Agreement on trade-related aspects of intellectual property rights"

The Madrid System and the TRIPS quotas have been appended and built upon since their inception in 1989, and have created an internationally agreed-upon arbitration standard. On the other hand, these protocols, especially TRIPS, have been criticized widely for vague enforcement standards, causing several challenges in implementing the proposed frameworks. This has led to several individual companies and governments adding standards that exceed the minimum requirements set by the TRIPS protocol, with these policies collectively known as TRIPS-plus, or TRIPS+ (Trainer, 2008)[v].

The WIPO also works closely with the International Corporation for Assigned Names and Numbers (ICANN) on cases that pertain to the registration of internet domain names and digital intellectual property rights - which allows cases concerning cybersquatting to be judged. However, some jurisdictions also provide their own legal frameworks to assess cybersquatting cases—most notably the USA through the Anticybersquatting Consumer Protection Act (ACPA), and, to a limited extent, India through the Indian Trademarks Act, 1999.

2.2 Indian Standards of Trademarking

Indian trademarking law complies with the TRIPS standards, with their governing national legislation for the administration of trademarks in India - "The Trademark Act, 1999" - having been amended to adhere to their minimum regulations.

This legislation covers the registration process of trademarking in India, rights conferred through registration, and a detailed understanding of infringement and remedies in the case of infringement (Jain et al., 2024)[5] [vi]. It also covers several key provisions to prevent the misuse of trademarks, such as the protection of existing, well-known trademarks from dilution by infringing firms; the prohibition of the registration of marks that may confuse, deceive, or hurt the public; the enforcement of certification marks to ensure that trademarked property meets specific standards such as AGMARK and ISI[6].

Though trademarking policies have proved effective in several cases[7] the modern influx of trademark squatting has exposed a gap in the Indian legislation against trademark infringements. India has adopted a first-to-file system of arbitration, which judges the first organization or party to register the trademark to be the trademark owner. This has incurred the issue of trademark squatting, and in particular, cybersquatting, which allows parties to register trademarks in bad faith[8], intending to sell these trademark rights for exorbitant sums of money. Unlike the United States of America, which contains specified legislation to combat this crime, known as the ACPA, India, to this day, does not have any specific legislation against cybersquatting, instead relying on renditions and judgements of cases in the field under trademark laws.

[5] Academics have noted that while the Act incorporates TRIPS-compliant provisions and modern protections, lengthy registration processes (18-24 months on average) and high costs create barriers, particularly for small and medium-sized enterprises (SMEs). These delays expose trademarks to vulnerabilities like cybersquatting during the registration phase

[6] Section 2(1) of the Trademark Act, 1999: The ISI mark certifies the 'Indian Standard Institution' mark, certifying the quality, safety and performance of a variety of products. The Agmark, or Agricultural mark, certifies the quality of agricultural products like species and fruits in India. Several other marks exist alongside these, as specified within the Trademark Act, 1999

[7] **An example of this lies in the case of "Yahoo v. Akash Arora ('Yahoo India')", 1999IIAD(DELHI)229, Dr. M.K. Sharma, J.**

[8] The Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125 (d) (2002)

2.3 Using Indian Frameworks to counter cybersquatting

As mentioned earlier, India has not adopted cybersquatting-specific legislation to date. Nevertheless, courts have used existing legal frameworks in the field of trademarking in modern cases - including the aforementioned 'Indian Trademarks Act, of 1999'.

Section 29 of the Trademark Act pertains to the deceptive transformation of existing trademarks and states that this is an act of infringement. These include any trademarks that could deceive or confuse the public into believing that a domain name belongs to a renowned/existing organization even when it does not. Sections 43 and 66 of the IT Act deal with the unauthorized access and damage of computer systems and data. Though these primarily concern cybercrime such as hacking and identity theft, they can also be used in the context of cybersquatting (Naik Naik & Co. , 2023)[vii].

Moreover, courts have ascertained, in Yahoo Inc. v. Akash Arora & Anr[9], that domain names may also act as company identifiers rather than simply an internet address, thus allowing the use of general trademarking principles in the field of cybersquatting.

2.4 Gaps in Cybersquatting Literature and Legislation

Despite numerous landmark rulings, India's approach to cybersquatting remains fragmented and inconsistent, largely due to the absence of specific statutory provisions addressing this issue. Unlike jurisdictions such as the United States with the Anticybersquatting Consumer Protection Act (ACPA), Indian law lacks a standardized bad faith identification framework for assessing domain name disputes. Hence, courts often rely on the Trade Marks Act (1999) and the doctrine of passing off[10], which were originally designed for traditional trademark disputes. The reliance on passing off creates further challenges, as this doctrine focuses on consumer confusion and goodwill—elements often difficult to prove in cybersquatting cases.

As a result, on account of a lack of explicit legislative backing, judicial decisions on domain names have depended heavily on interpretation, resulting in inconsistent and unpredictable outcomes. Moreover, Indian law lacks robust remedies tailored to cybersquatting, such as statutory damages or streamlined domain recovery mechanisms, weakening enforcement and deterrence. Therefore, it is evident that Indian law would benefit from drawing on foreign anti-cybersquatting frameworks to develop clearer, more effective legislation.

2.5 Classification of Cybersquatting Case Types

Although existing terminologies address various forms of cybersquatting, no comprehensive framework systematically classifies all these cases under a unified set of labels. This lack of standardization creates inconsistencies in identifying and addressing the diverse strategies employed by cybersquatters, ranging from typosquatting and bad-faith registrations to domain hijacking and phishing schemes. A universally accepted classification system could aid in better understanding, regulating, and resolving such disputes.

Therefore, the following table proposes a compact, original framework (see Table No. 1) to solve this issue, defining classification labels, definitions of these labels, and real-life case studies to support proposed descriptors.

[9] **Yahoo!, Inc. vs Akash Arora & Anr. on 19 February 1999, 78(1999)DLT285**

[10] "Passing off" is a law tort used to protect the goodwill of trader's unregistered trademark from being passed off as belonging to another party

Table 1 - Proposed classification of cybersquatting case types

Classification	Proposed Definition and Dimension	Case Studies
Trademark-erosion based cybersquatting	● This classification covers cases where existing trademarks have been infringed upon through domain names. ● Trademark laws can be used to combat such infringements, particularly when domain names are used in bad faith to profit from the trademark.	● **Sportsman's Market Inc. v. Sporty's Farm L.L.C.**: Domain names cannot infringe upon trademarks previously registered by firms. The use of domain names in bad faith is considered trademark infringement. ● **Northern Light Technology Inc. v. Northern Lights Club**: Domain names used to gain profit without legitimate use can be considered bad faith, triggering trademark infringement under the ACPA.
Speculative and extortive cybersquatting	● This refers to cases where cybersquatters hold domain names and demand exorbitant prices for them, under the pretense that a company or organization will need to buy them ● Legal challenges arise when the domain is transferred internationally	● **JioHotstar.com (2024)**: The case involved legal action against cybersquatting on domain names containing non-trademarked identities, with challenges due to India's lack of cybersquatting legislation. If Jio enforced UDRP, the cybersquatters may have had faced charges for bad-faith registration ● **ClintonKaine.com + HarrisWalz.com**: Jeremy Peter Green registered domain names with political figures' names, purchasing them speculatively and aiming to sell them for profit
Parody cybersquatting	● Parody cybersquatting involves using domain names similar to existing websites or organizations to mock or criticize them ● This may be protected under the First Amendment in the U.S., but not under international laws against cybersquatting	● **PETA.org vs. PETA.com (2001)**: A parody website mocked the original PETA website. The UDRP panel ruled the parody was legitimate free speech, though PETA lost ● **Walocaust.com**: A parody of Walmart criticizing its business practices. Walmart pursued legal action, but the courts recognized the parody as protected free speech under the First Amendment
Anonymous cybersquatting	● This classification involves cases where the identity of the cybersquatters is concealed, making it difficult to take legal action ● In some cases, in-rem actions, which take action against the domain name itself rather than a perpetrator, may be necessary to transfer the domain	● **Jacobsen v. Katzer (2007)**: The defendant registered "decoderpro.com" using the plaintiff's software project. The identity was concealed, but WIPO ruled in favour of the plaintiff and transferred the domain
Situational cybersquatting	● Situational cybersquatting involves using natural disasters, famous events, or incidents as domain names to capitalize on public interest and attract unsuspecting individuals.	● **Hurricane Katrina**: Over 4,000 cases were registered using similar domain names exploiting the disaster. Many were fraudulent. ● **The London 2012 Olympics**: Individuals registered domain names containing "London 2012" and related terms to profit from the event's popularity. LOCOG took action under UDRP, transferring infringing domains like 'mylondon2012.com'.
Legislative Disputes in Cybersquatting	● This refers to situations where different governing bodies have different interpretations of a case, especially when the ACPA and international arbitrators like WIPO clash in their rulings. ● Though this is not directly a classification of cybersquatting, it is quite an important demonstration of how national and international legislation may collide and disagree in certain cases.	● **PETA.org vs. PETA.com (2001)**: As discussed earlier, the U.S. courts and WIPO had different interpretations of whether the parody website constituted bad faith. This led to the US's ACPA framework winning the judgement of the case, overturning the ruling of the WIPO, portraying how national legislation may, in some cases, actually outweigh the rule of international legislation.

3 Methodology

3.1 Research Objectives

This research seeks to:

1. Critically evaluate the adequacy of India's legal framework in addressing cybersquatting
2. Compare and contrast Indian legal approaches with the structured frameworks of the ACPA in the U.S. and Canada's trademark laws
3. Suggest revisions and additions to Indian law to combat cases of cybersquatting beyond the scope of trademark law

3.2 Research Question

The research question for this paper is: "How do countries approach cybersquatting, and what lessons can India draw from foreign legislation?"

This research question aims to explore how cybersquatting—an issue where individuals register domain names resembling established trademarks or brand names to exploit their value—has been addressed in the legal frameworks of India, the United States of America, and Canada. The focus is on identifying which specific aspects of cybersquatting are emphasized or prioritized within Indian legislation, and how broader international standards and practices can improve these. By comparing Indian laws with those in Canada and North America, the study seeks to highlight differences in regulatory approaches, enforcement mechanisms, and the underlying legal philosophies that influence how cybersquatting is managed in each jurisdiction.

A comparative study of Indian, Canadian, and American legislation will provide a broader context for understanding the global and regional dynamics of cybersquatting regulation. The US and Canada have established robust systems for dealing with cybersquatting through both legal recourse and specialized dispute resolution mechanisms. By contrasting these with India's approach, the research will assess whether there is a need for further legislative reforms in India, especially in terms of aligning Indian law with the best global practices and ensuring a more effective legal response to the misuse of domain names.

3.3 Relevant Legal Frameworks Across Jurisdictions

The legal frameworks referenced in this study span three jurisdictions. In India, cybersquatting disputes are addressed primarily under the Trade Marks Act, 1999. In the United States, two key statutes govern such matters: the Anticybersquatting Consumer Protection Act (ACPA), 1999 and the Lanham Act, 1946. In Canada, the relevant legislation includes the Trademarks Act, 1985 and the CIRA[11] Domain Name Dispute Resolution Policy (CDRP[12]), 2011. These frameworks collectively form the basis for the comparative analysis in this paper.

3.4 Case Data Set

This research draws from a variety of secondary sources, including judicial precedents, statutory analyses, and academic commentaries. Central to this analysis are landmark cases demonstrating the

[11] "CIRA" is a common acronym for the Canadian Internet Registration Authority
[12] Although the CDRP only governs ".ca" domain names, its policies and frameworks provide guidance for the assessment of cybersquatting cases involving other domain types in Canada as well.

evolution of cybersquatting jurisprudence in India, the U.S., and Canada. These cases provide valuable insights into the varying approaches taken by different jurisdictions.

The following cases have been selected from each jurisdiction to highlight the strengths and weaknesses of their respective legal frameworks. While the majority of cases involve domain name disputes—examined under both specific cybersquatting laws and general trademark legislation—some trademark infringement cases have also been included. These are crucial for understanding how courts assess core factors such as bad faith and intent to mislead, which are central to both trademark and cybersquatting cases.

Table 2 - Sample Set of Selected Cases

Serial Number	Jurisdiction	Case Name	Case Reference Code	Verdict & Reasoning
1	India	Yahoo!, Inc. vs Akash Arora & Anr.	1999IIAD(DELHI)222	The court ruled in favor of Yahoo, emphasizing the need to protect trademarks in cyberspace.
2	India	Tata Sons Limited vs Mr. Manu Kishori & Ors.	2001IIIAD(DELHI)545	The court ruled in favor of Tata Sons, underscoring the importance of preventing bad-faith registrations.
3	India	Tata Sons Ltd. v. Greenpeace International	178 (2011) DLT 705	The court dismissed Tata Sons Ltd. and ruled in favor of Greenpeace international, leading to the ruling that parody and satire without consumer confusion do not constitute trademark infringement
4	India	Satyam Infoway Ltd. v. Siffynet Solutions Pvt. Ltd.	AIR 2004 SUPREME COURT 3540	The Supreme Court ruled that domain names are trademarks, and their misuse constitutes trademark infringement.
5	India	Rediff Communication Ltd. v. Cyberbooth & Anr.	AIR 2000 BOMBAY 27	The Bombay High Court emphasized that domain names are an integral part of business identity.
6	India	Dr. Reddy's Laboratories Ltd. v. Manu Kosuri & Anr.	2001IVAD(DELHI)583	The Delhi High Court ruled in favor of Dr. Reddy's Laboratories, citing cybersquatting as an unfair trade practice.
7	India	Indian Hotels Company Ltd v. Jiva Institute of Vedic Science and Culture	CS(OS) No.1960/2006	The court ruled against the use of the iconic Taj Mahal trademark for profit without authorization.
8	India	Infosys Technologies Ltd. v. Park Infosys	2007(34)PTC178(DEL)	The court emphasized protecting the goodwill associated with a business's name.
9	India	Times Of Money Limited vs Remithome Corporation & Another	I.A. No.3037/2011 in CS (OS) No.456/2011	The court was forced to dismiss the case on grounds of jurisdiction and thus exposed that instances of cybersquatting must be tried through valid jurisdictions.
10	India	Manish Vij And Ors. vs Indra Chugh	97(2002)DLT1	The plaintiff was unable to establish bad faith on part of the defendants. Therefore, the plaintiff's application for interim relief was rejected. The court notably mentioned that, in the context of Indian law, "the term "bad faith" does not simply mean bad judgment, but it implies the conscious doing of a wrong with a dishonest purpose. It contemplates a dishonest state of mind".
11	USA	People for Ethical Treatment of Animals v. Doughney	263 F.3d 359 (4th Cir. 2001)	The court held that using 'peta.org' for a parody site violated the ACPA.
12	USA	Panavision International, L.P. v. Toeppen	141 F.3d 1316 (9th Cir. 1998)	The Ninth Circuit ruled that registering domain names of famous trademarks to extort money constituted trademark dilution.
13	USA	Lamparello v. Falwell	420 F.3d 309 (4th Cir. 2005)	The court ruled in favor of free speech, stating that non-commercial, critical commentary was not cybersquatting.
14	USA	Virtual Works, Inc. v. Volkswagen of America, Inc.	238 F.3d 264 (4th Cir. 2001)	The court ruled that registering 'vw.net' in bad faith to sell to Volkswagen was cybersquatting.
15	USA	Sporty's Farm L.L.C. v. Sportsman's Market, Inc.	202 F.3d 489 (2nd Cir. 2000)	The court found that registering a domain name to disrupt a competitor's business was cybersquatting.

16	USA	Ford Motor Co. v. Greatdomains.com	177 F. Supp. 2d 635 (E.D. Mich. 2001)	Ford successfully sued to stop the sale of domain names that infringed on their trademarks.
17	USA	Shields v. Zuccarini	254 F.3d 476 (3rd Cir. 2001)	The court ruled that registering similar domain names to Shields' trademark was cybersquatting under the ACPA.
18	USA	Caesars World, Inc. v. Caesars-Palace.com	112 F. Supp. 2d 502 (E.D. Va. 2000)	The court held that using a domain name similar to a well-known trademark to attract web traffic constituted cybersquatting.
19	USA	Hasbro, Inc. v. Clue Computing, Inc.	66 F. Supp. 2d 117 (D. Mass. 1999)	The court ruled that Hasbro's case over 'clue.com' required a nuanced view of intent and trademark strength.
20	USA	Harrods Ltd. v. Sixty Internet Domain Names	302 F.3d 214 (E.D. Va. 2002)	The court ordered the transfer of domain names incorporating 'Harrods,' finding them registered in bad faith.
21	USA	Verizon California Inc. v. OnlineNIC, Inc.	2009 WL 2706393	The plaintiffs were awarded $33.15 million, or $50,000 for each of 663 domain names that were identical or confusingly similar to Verizon's marks, in total.
22	Canada	Microsoftv. MikeRoweSoft (2004)	N/A (settled outside court)	A Canadian teenager, Mike Rowe, registered "MikeRoweSoft.com" for his web-design business. Microsoft challenged the domain on account of its phonetic similarity. The parties ultimately settled: Rowe transferred the domain to Microsoft in exchange for an Xbox and Microsoft services.
23	Canada	Canadian Tire Corporation, Limited v. Mick McFadden	WIPO D2001-0383	Canadian Tire filed a WIPO lawsuit against a private registrant of "Crappytire.com", alleging trademark infringement. The panel dismissed the challenge, noting that "Crappy Tire" as an expression was not a protected mark of Canadian Tire, so no transfer was ordered
24	Canada	PicMonkey LLC v. Whois Privacy Services Inc.	CIRA CDRP Dispute No. 00337	PicMonkey LLC initially lost its .ca domain claim and the initial CDRP panel ruled against PicMonkey LLC, concluding that the company had not established trademark rights in Canada for the PICMONKEY mark prior to the registration of the domain name. Consequently, it had failed to demonstrate that the domain name was confusing with its trademark at the relevant time. Upon re-filing with completed evidence, PicMonkey successfully reclaimed picmonkey.ca
25	Canada	Fiducie de soutien à La Presse v. Mike Morgan	CDRP-24635	"Fiducie de soutien à La Presse" filed a complaint under CIRA's Domain Name Dispute Resolution Policy and successfully secured the transfer of laprese.ca from Mike Morgan, finding the domain confusingly similar to their trademark and registered in bad faith.

3.5 Methodological Framework

By systematically comparing Indian, U.S., and Canada's approaches to cybersquatting, the research identifies strengths, weaknesses, and transferable principles from each jurisdiction. This analysis highlights how structured frameworks, such as the ACPA's bad faith test, could inform Indian legislative reforms.

Judicial precedents are examined to uncover patterns in reasoning and decision-making. For instance, Indian courts often rely on passing off, whereas U.S. courts employ the ACPA's detailed bad-faith criteria. This analysis provides insights into the advantages and limitations of each approach.

Recurring themes such as "bad faith intent" and "consumer confusion"[13] are explored in depth to evaluate the effectiveness of existing legal principles. The thematic analysis also considers the balance between protecting intellectual property and safeguarding free speech rights.

[13] Consumer confusion occurs when the similarity between a trademark and another mark or domain name leads consumers to mistakenly believe there is a connection between them.

4 Findings and Comparative Analysis

This section of the paper assesses the anti-cybersquatting legislation of each of the countries mentioned earlier - India, the United States of America, and Canada - based on the following criteria: Understanding of Bad Faith; Legal remedies, Case Outcomes, and Rationale; and Free Speech and Parody Cases. At the end of each section, a discussion will compare the laws across jurisdictions and highlight any gaps or inconsistencies. These discussions include hypothetical situations and contextual interpretations of existing policies. This section concludes by using the cases, analysis, judgments, and findings from the previous three sections to suggest possible revisions to Indian legislation to better address cybersquatting, considering how these changes could have affected the assessment, ruling, and outcome of the 2024 JioHotstar domain-squatting case.

4.1 Understanding of Bad Faith

4.1.1 United States Legislation (Anticybersquatting Consumer Protection Act, 1999)[14]

This section mentions 9 clear angles[15] from which a court may determine bad faith in the context of cybersquatting, including malicious intent through commercial sale; intent to divert users from an existing domain; and trademark dilution[16]. This section also mentions how these angles must be viewed with the Trademark Act of 1946, Subsection (c)(1) of section 43[17]. The ability of courts to determine whether or not the case can use the concept of bad faith depends on the court's understanding of whether the person holding the domain had reasonable grounds to believe that the use of the domain was lawful upon registration.[18]

In Panavision Int'l, L.P. v. Toeppen, the defendant registered "panavision.com" and attempted to sell it to the plaintiff for $13,000[19]. The court found that this conduct demonstrated his intent to profit by selling the domain name to the complainant[20]. Notably, the court noted that the domain names could potentially confuse and frustrate Panavision's customers, thereby tarnishing the company's reputation and reducing its visibility to prospective clients. Similarly, in People for the Ethical Treatment of Animals v. Doughney[21], the Fourth Circuit found bad faith based on: the misleading similarity of the domain name and the "peta" mark; and Doughney's intent to prevent PETA from using its mark online, especially as he had encouraged them to "settle" by purchasing the domain—implying a profit motive.

[14] The Anticybersquatting Consumer Protection Act is not a separate piece of legislation, but rather an amendment and subset of the existing Trademark Act of 1946 (15 U.S.C. 1051 et seq.). Therefore, sections of this act may refer to the act as a whole, which will be discussed in the footnotes when necessary.
[15] It is important to note that the ACPA's mentioned facets to consider in the assessment of bad-faith are non-exhaustive. This means courts may use other justifications beyond the 9 steps which have been mentioned.
[16] See Section 3002(a)(1)(B)(i) for all 9 angles
[17] "Injunctive Relief - Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury."
[18] Section 3002. a. B. (II) - Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.
[19] Additionally, Toeppen stated that upon receiving full payment, he would refrain from acquiring any other Internet addresses that Panavision Corporation claimed as its property.
[20] After Panavision refused to pay, Toeppen proceeded to register "panaflex.com," which he used solely to display the word "Hello". It can also be considered that Toeppen's continued registration of domain names—without any legitimate interest such as criticism, and purely to prevent Panavision from acquiring them with the intent to gain profit from selling the domain names—was central to its reasoning
[21] Doughney registered "peta.org" and used it as a parody site titled "People Eating Tasty Animals."

In contrast, Lamparello v. Falwell, the Fourth Circuit held there was no bad faith in registration under the ACPA, as Lamparello was not attempting to mislead consumers or profit commercially[22].

Therefore, the ACPA provides clear, yet flexible, mediums to assess bad faith in cases of cybersquatting, placing significant weight on whether the registrant had reasonable grounds to believe that the use of the domain was lawful upon the registration of the disputed domain.

4.1.2 Canadian Legislation (Canadian Trademarks Act and the CIRA Domain Name Dispute Resolution Policy)

Similar to the ACPA, the CDRP mentions a non-exhaustive guideline through which courts may determine whether a domain name has been registered in bad faith [23]. The 4 mentioned guidelines to assess are: the intent to sell, rent, license, or transfer in some form, the registration of the domain name to the complainant (similar to a "ransom"); the intent to prevent the owner of the mark from registering their mark as a domain name; the intent to disrupt the complainant's business; and the intent to attract attention by creating confusion within the public for the sake of commercial gain, or to endorse a product/service.

The Federal Court of Canada has clarified the use of bad faith practically in the case of Beijing Judian Restaurant Co. Ltd. ("BJR") v. Wei Meng [24]. The Court used existing verdicts in regions such as the United States of America and Europe, concluding that registering a trademark with the sole intent of interfering with an existing third-party trademark without legitimate commercial purpose can be considered bad faith - a principle extending to domain names and cybersquatting cases. Thus, the Court identified three key facets to reach the ultimate verdict: pattern of conduct, awareness of BJR's reputation, and lack of legitimate use.

Therefore, the CDRP provides a framework similar to that of the ACPA, offering clear yet non-exhaustive factors for determining bad faith, such as whether the registrant had a legitimate interest in the domain name.

4.1.3 Indian Legislation (The Indian Trademarks Act, 1999)

Similar to Canadian trademark legislation, the Indian Trade Marks Act, of 1999 does not explicitly define methods of determining bad faith. However, the concept is well-recognized in Indian jurisprudence and functions as a mechanism to regulate the registration of exploitative trademarks. Section 11[25] of the Act concerns the "Relative grounds for refusal of registration", while Section 142[26] prohibits "groundless threats of legal proceedings", which considers the bad faith in the registration of a trademark infringement suit. Additionally, common law principles, such as passing off, play a crucial role in addressing domain name squatting and deceptive business practices. Moreover, Indian Courts have established domain names as more than internet addresses, but unique identifiers linked to a firm or individual's reputation, and covered under the Indian Trade Marks Act.

This principle was firmly established in Rediff Communication Ltd. v. Cyberbooth & Anr. (1999), where the Bombay High Court ruled that domain names are integral to a business's identity and that unauthorised use of deceptively similar names can lead to consumer confusion and dilution of brand

[22] Lamparello operated "fallwell.com," a criticism site targeting televangelist Jerry Falwell's views on homosexuality.
[23] CDRP Page 4, Section 3.5: "Registration in Bad Faith"
[24] Beijing Judian Restaurant Co. Ltd. v. Wei Meng, 2022 FC 743: Beijing Judian Restaurant Co. Ltd. (BJR), a well-known Chinese restaurant chain, expanded to Canada in 2018. In 2019, Wei Meng registered BJR's "JU DIAN & Design" trademark in Canada for "beer" and "restaurant services." Meng then demanded $1.5 million from BJR for the trademark and later advertised it for sale. Evidence showed he had also registered other well-known Chinese restaurant trademarks without legitimate intent.
[25] Indian Trademarks Act, 1999, p. 11-13 - Clause 11. (Relative grounds for refusal of registration) subsection 1 and 10
[26] Indian Trademarks Act, 1999, p. 47-48, Section 142

goodwill. The court observed that domain name misuse, particularly in bad faith[27], could constitute passing off, reinforcing the notion that an online business with an established reputation can seek legal remedies against domain name squatters. The Court also referenced the case of Yahoo! Inc. v. Akash Arora & Anr. (1999)[28].

Moreover, in Satyam Infoway Ltd. v. Siffynet Solutions Pvt. Ltd. (2004), the Supreme Court of India emphasised that deceptively similar domain names could mislead consumers and damage the rightful owner's goodwill, further strengthening the application of passing off principles in cyberspace. Courts referred to the cases above as well in passing their final verdict.

Therefore, India lacks a formal framework to assess bad faith, often relying on existing common law principles, trademark laws, rulings from previous cases, and general understandings of bad faith. However, this approach can become inadequate when dealing with cases that do not involve a registered trademark.

4.1.4 Collective Discussion of Bad Faith Understanding

Therefore, across the United States, Canada, and India, there is a shared basic understanding of what constitutes bad faith. In all three jurisdictions, bad faith is generally seen as an intentional act designed either to undermine an existing mark or to profit from a mark that rightfully belongs to someone else. However, where these countries really diverge is in how clearly they define this principle, and how effectively they apply it through their legal systems.

In the United States and Canada, the concept of bad faith is defined and assessed through detailed frameworks. The Anticybersquatting Consumer Protection Act (ACPA) in the U.S. and the CIRA Domain Name Dispute Resolution Policy (CDRP) in Canada provide courts and panels with clear guidance on how to assess bad faith. Both frameworks suggest key factors such as: whether the registrant intended to profit, whether the registrant knew or had reason to believe their actions infringed on an existing mark when registering the domain, whether the domain name in question would be likely to mislead the public, and whether the use of the domain name risks damaging the reputation of the rightful owner. Notably, neither law treats parody or criticism as bad faith, as long as the action does not interfere with the aforementioned principles. The CDRP also defines “legitimate interest”, giving decision-makers another tool to weigh the registrant’s true intent behind the use of the domain as a part of their rulings.

These laws give courts enough flexibility to take context into account—such as whether the domain is being used for fair comment or parody—while still setting clear limits on what crosses into unlawful cybersquatting. Therefore, outcomes from cases using these frameworks are predictable and consistent across most cybersquatting cases.

India, on the other hand, does not have a similar, dedicated legal framework. While Indian courts do recognize bad faith as a legal principle (see Manish Vij v. Indira Chugh (2002)), it has left to be defined and applied on a case-by-case basis, without the benefit of clear legislative guidance. This has led to inconsistent rulings, placed an unjust burden on plaintiffs to prove bad faith without any specific framework to do so, and left room for exploitation.

Given these challenges, it is clear that India would benefit from introducing a formal framework for assessing bad faith in cybersquatting cases. Such a framework should allow courts to consider factors like whether the domain name is misleading, whether there was commercial intent, knowledge of the

[27] A general understanding of bad faith does exist amongst Indian courts—as seen in Manish Vij v. Indira Chugh, where bad faith was defined as “the conscious doing of a wrong with a dishonest purpose” - but is not defined explicitly within Indian law

[28] In Yahoo! Inc. v. Akash Arora & Anr. (1999), the Delhi High Court rejected the argument that domain names are mere digital addresses, holding that they function as source identifiers similar to trademarks.

complainant's mark, patterns of abusive registration, and the risk of harm to the complainant's reputation or goodwill. By adopting an approach that offers both flexibility and clarity—along the lines of the ACPA or CDRP—India could make its legal response significantly fairer, creating more consistent decisions in these disputes.

4.2 Legal Remedies, Case Outcomes, and Rationale

4.2.1 United States Legislation (Anticybersquatting Consumer Protection Act, 1999)

The ACPA allows the plaintiff to choose how they wish to elect to be compensated in the case of proven bad faith or reckless disregard[29].

To begin, the ACPA permits a plaintiff in a cybersquatting case to elect statutory damages in lieu of damages based on actual incurred harm. These damages range from a minimum of $1,000 to a maximum of $100,000 per infringing domain name, with the exact amount left to the court's discretion based on the severity and nature of the violation.

Alternatively, under the Lanham Act[30], a plaintiff may choose to pursue actual damages and profits instead of statutory damages. This allows the claimant to seek compensation for specific financial harm, rather than be limited to the statutory cap, particularly in cases where the economic losses exceed the predefined threshold. The court may also, in its discretion, award costs and attorneys fees to the prevailing party[31].

Unless connected to other crimes, the ACPA does not mention any chance of imprisonment on account of cybersquatting, only citing the transfer of domains and monetary compensation based on the aforementioned criteria. The court may also grant injunctive relief to the domain name registrant, including the reactivation of the domain name or the transfer of the domain name to the domain name registrant[32]. The ACPA also outlines that in the case of 'bad faith of complaint', where the complainant misleads a registrar, registry, or other registration authority into taking action[33], the person making the misrepresentation is held liable for any and all damages incurred by the domain name registrants as the result of such action[34].

In the case of Shields v. Zuccarini (2001)[35], the plaintiff, Joseph Shields, was awarded statutory damages[36] based on the court's finding that Zuccarini's - the domain registrant - actions were willful and malicious, thereby constituting bad faith.

Moreover, in Verizon California Inc. v. OnlineNIC, Inc., the court found that OnlineNIC had acted willfully, and that the registered domain names were misleading and substantially similar to Verizon's

[29] Section 35 and 43 of the Trademark Act of 1946 (15 U.S.C. 1117)
[30] The Lanham Act is the principal federal statute governing trademark law in the United States, providing owners of federally registered trademarks the right to pursue civil remedies for various trademark-related offenses, including cybersquatting.
[31] ACPA Section 3002(B)(2)
[32] Lanham Act; Section 1114: Remedies; Infringement; Innocent Infringement by Printers and Publishers
[33] The acts which constitute an 'action' by the said authorities are defined in ACPA Section 3004. "Limitation on Liability" 2.D(ii)
[34] ACPA Section 3004. "Limitation on Liability" 2.D(iv)
[35] John Zuccarini registered multiple typographical variations of joecartoon.com in November 1999, a popular web comic site held by Joseph Shields since June 12th, 1997, in order to misdirect users for advertising revenue. Visitors were effectively "mousetrapped" on the websites — a term used in the digital domain to describe a tactic where users are prevented from exiting a site unless they navigate through multiple advertisements. Zuccarini earned between ten and twenty-five cents per click from these ads.
[36] The statutory damages awarded were $10,000 per domain name, as determined at the discretion of the United States Court of Appeals for the Third Circuit.

trademarks. While OnlineNIC's failure to comply with court orders did influence the final outcome[37], the ruling was primarily justified by violations of the ACPA on account of the similarities aforementioned. Similarly, in Virtual Works, Inc. v. Volkswagen of America, the court held that the domain vw.net had been registered in bad faith with intent to profit by selling the domain to Volkswagen. The ACPA was applied to transfer the domain and mitigate potential consumer confusion as a result of the misleading domain name.

Notably, in People for the Ethical Treatment of Animals (PETA) v. Doughney, although Doughney was ordered to transfer the domain name to the plaintiff, PETA was ineligible for the compensation of attorney's fees on account of the Doughney's - the domain registrant - initial belief that creating a parody site was protected under the first amendment.

Therefore, the ACPA and the Lanham Act permit complainants, upon successfully proving a case of cybersquatting, to elect compensation either through statutory damages—at the discretion of the court, within a range of $1,000 to $100,000 per domain name—or through the recovery of actual damages incurred.

4.2.2 Canadian Legislation (Canadian Trademarks Act, 1985 and Related Rulings)

The CDRP places the onus on the complainant to prove that: the registrant's ".ca" domain is confusingly similar to a mark already, and currently, owned by the complainant at the time of registration; the registrant has registered the domain name in bad faith; and that the registrant has no legitimate interest[38] in the domain name. Unlike the ACPA, the CDRP does not mention any monetary rewards or remedies - including statutory damages - even if the complainant proves the registrant to have registered the domain name in bad faith. Instead, the CDRP gives the Panel - the authority appointed to decide the proceeding - the ability to decide whether the registration should be deleted, or transferred to the complainant [39].

On the other hand, unlike the lack of a monetary limit on the remedy bestowed upon the registrant seen in the ACPA, the CDRP details that if a registrant proves that the complaint placed against them was unjust and intended to cancel/obtain a transfer of any domain name registration, the panel has the authority to order the complainant to pay the registrant - through the provider - an amount up to $5000 as a remedy to the costs incurred by the registrant in preparing for the proceeding. This policy aims to prevent and punish false accusations against domain registrants.

In Fiducie de soutien à La Presse v. Mike Morgan, the panel ruled in favour of the complainant, ordering the transfer of "laprese.ca". This decision was on account of the domain having been found to be confusingly similar to the 'La Presse' trademark and registered in bad faith, supported by the registrant having no legitimate interest in the domain name[40].

On the other hand, in PicMonkey LLC v. Whois Privacy Services Inc., the plaintiff initially failed to prove that they had the trademark rights to 'PICMONKEY' in Canada prior to the registration of the disputed domain name by the registrant. Though this ruling was overturned when the plaintiff submitted

[37] The plaintiffs were granted $33.15 million in damages—equivalent to $50,000 for each of the 663 domain names found to be identical or confusingly similar to Verizon's registered marks.
[38]CDRP Page 4 Section 3.4: "Legitimate Interests"
[39] CDRP Section 4.2: "Decision and Amendment to a Decision"
[40] Using a confusingly similar domain name to host commercialized links from which profit is gained is typically not considered legitimate interest under Paragraph 4.1(c) of the CDRP

another claim under the CDRP along with additional evidence [41] demonstrates the importance of establishing and holding trademark rights at the time of the registrant's domain registration. This case highlights the fact that there is no principle of 'res judicata'[42] during CDRP proceedings, and that the same complainant may file several complaints, between the same parties, regarding the same domain name.

Therefore, the CDRP, though allowing for the transfer or deletion of disputed domain names at the discretion of the panel when a case of cybersquatting is proven, does not directly provide monetary damages for losses incurred by the complainant because of the cybersquatting. However, complainants may choose to use the Canadian Trademarks Act to file for damages instead, though this may be complex in cases that do not involve the infringement of registered trademarks.

4.2.3 Indian Legislation (Trade Marks Act, 1999 and Judicial Interpretation)

Due to a lack of legislation specifically relating to cybersquatting, India does not have any specified punishments or repercussions in the event of the crime. However, Indian courts often use the Trademarks Act, 1999, alongside the concept of passing off, to determine remedies granted to plaintiffs instead.

As per Section 135(1) of the Trademarks Act, in the event of a case of passing off or infringement, courts may grant relief in the form of injunction, monetary compensation, or an account of profits. In addition, courts may also order the delivery-up of all infringing labels and marks to be erased.

However, the court cannot grant monetary compensation - excluding nominal compensation - or an account of profits if the defendant satisfies the following conditions: that they ceased using the trademark upon realization of the infringement, and that they had no reasonable ground to believe the trademark was registered (in the case of infringement complaints) or in use (in the case of passing off complaints)[43].

In addition, it is important to note that Indian courts do not impose statutory damages like the ACPA. Remedies are case-specific and dependent on proof of actual harm, potential harm, or the registrant's profits from the infringed domain.

In Yahoo! Inc. v. Akash Arora (1999), the Delhi High Court granted injunctive relief to Yahoo! Inc. and ordered the defendant to permanently cease the use of the domain "yahooindia.com"[44]. This case led to a landmark ruling in Indian cybersquatting jurisprudence, holding that domain names, like trademarks, are identifiers of source and reputation, thereby allowing traditional IP protections to extend into cyberspace. The court primarily considered Akash Arora's use of the domain name yahooindia.com

[41] This additional evidence proved that PicMonkey LLC had used the trademark 'PICMONKEY' prior to the registration of the disputed domain name, and that the registrant had acted in bad faith when registering the domain on account of a lack of legitimate interest.

[42] The principle of "Res Judicata" prevents a matter that has been ruled upon by a competent court from being disputed again between the same two parties under the same circumstances. Though one may argue that the lack of principle of 'res judicata' may allow more just decisions to be made, it may also open doors to possible misuses. Therefore, this may lead to - in the event of an inability to prove Bad Faith of Complaint - a complainant filing several cases in order to overburden the registrant with significant legal expenses. However, Canadian courts recognize and combat such issues under 'vexatious litigation'.

[43] Indian Trademarks Act, 1999; Section 135(2); Page 45

[44] The defendant, Akash Arora, registered his company under the name "Yahoo India" with the intent to offer digital services similar to those of Yahoo! Inc. In response, Yahoo! Inc. filed an application for an interim injunction to prevent the defendant from using the mark "Yahoo" in any form within his domain name. Yahoo! Inc. also filed a lawsuit against Akash Arora, claiming that the use of the domain name "yahooindia.com" was confusingly similar to its own trademark and could potentially mislead consumers.

to provide services similar to those of Yahoo! Inc., and the similarity and likelihood of confusion that would arise from the use of a domain name nearly identical to Yahoo's famous and registered mark.

The case of Satyam Infoway Ltd. v. Siffynet Solutions (2004)[45] proved to be one of the most interesting in the field of Indian cybersquatting cases, as it led to three different rulings and justifications—by the civil court, the High Court, and the Supreme Court. To begin, the civil court ruled in favour of Satyam Infoway, arguing that the plaintiff was the prior user of the word "sify" and had gained immense popularity through the sale of internet services under that name. The civil court further justified its decision by stating that the similarity in domain names would likely create confusion among the public. The defendant, Siffynet Solutions, then appealed to the High Court. The High Court considered where the 'balance of convenience' lay[46] and held that the differing nature of services offered by Siffynet Solutions and Satyam Infoway Ltd. would lead to little or no likelihood of confusion among customers. The Supreme Court set aside this decision by the High Court and once again ruled in favour of the plaintiff, thus stating the Sifynet Solutions should be forbidden from the use of the mark 'sify'. Notably, the final ruling was justified by declaring that domain names should be subject to the same regulatory framework as trademarks (i.e., the Trademarks Act, 1999) and should be protected under the law of passing off. Although the lack of structured cybersquatting legislation led to varying interpretations and decisions between the three courts, the final ruling upheld the principle that trademarks and domain names are to be treated as equivalent in the context of cybersquatting.

Therefore, Indian courts have ruled that domain names are covered under the same framework as trademarks, thus allowing complainants in domain name disputes to seek the same remedies as those available for trademark infringement or dilution under the Indian Trade Marks Act, 1999, including but not limited to injunctions and accounts of profits.

4.2.4 Collective discussion of Legal Remedies and Case Outcomes

The ACPA's direct provision of monetary remedies, independent of the U.S. Trademark Act, allows cybersquatting cases to be addressed separately from the restrictions of trademark law. This ensures that victims of cybersquatting, even where no registered mark exists, can seek compensation for harm caused by the registration and use of the disputed domain name. Additionally, both the ACPA and CDRP have established clear remedies to compensate victims of complaints made in bad faith. This serves as an important deterrent against false or baseless allegations and helps brands recover damages incurred in defending such claims.

However, the CDRP's scope is limited to .ca domain names, meaning cases involving other domain types must proceed under the UDRP, often resulting in slower and more complex proceedings. Moreover, the CDRP's lack of direct monetary remedies (see section 4.2.2, para. 1) also forces complainants to rely on the Canadian Trademarks Act, which creates challenges in cases involving non-registered marks.

Indian law faces similar difficulties as the CDRP; the absence of a specific cybersquatting statute forces complainants to fight cases under the Trade Marks Act, 1999 (see section 2.5). Furthermore, treating domain names solely under this Act (see section 4.2.3, para. 6) and the Information Technology Act, 2000, is partially inadequate, as these frameworks are not designed to address cybersquatting involving non-registered marks—a frequent occurrence in domain disputes. While the Trade Marks Act

[45] In Satyam Infoway Ltd v. Siffynet Solutions Pvt. Ltd (2004), the plaintiff, having used the coined term "Sify" since 1999 as part of multiple domain names, filed a suit against the defendant, who registered similar domain names like "siffynet.net" in 2001. Satyam issued legal notices demanding cessation and transfer, which were refused.

[46] The term 'balance of convenience' refers to the court's judgement on how the court's ruling would inconvenience the affected parties. Therefore, the High Court noted that Sifynet Solutions had already made significant investments in building a customer base of approximately 50,000 members and would therefore face substantial hardship and irreparable harm if the ruling were in favour of Satyam Infoway.

does provide injunctions and monetary remedies, the lack of suitable legislative scope as aforementioned often makes these remedies difficult to obtain for complainants. Though the INDRP ('.IN' Domain Name Dispute Resolution Policy) has streamlined the assessment of disputes involving '.in' domains, it creates a similar limitation to the CDRP, as it lacks the scope to address disputes involving other domain types.

Introducing a dedicated cybersquatting policy, similar to the ACPA, would help India close this gap, strengthen enforcement, and better protect both commercial interests—such as reputation and profit—and public interests by deterring cybersquatters through clear monetary and non-monetary repercussions.

4.3 Free Speech and Parody Cases

4.3.1 United States: A Constitutional Emphasis on Expression

In the U.S., the Anticybersquatting Consumer Protection Act (ACPA) prohibits the registration of domain names that are identical or confusingly similar to existing trademarks when done in bad faith. However, courts make a crucial distinction between commercial exploitation and non-commercial expressive use. This leads to the right to free speech being used as a justification if and only if bad faith, malicious intent, or possible customer confusion is not proven.

In People for the Ethical Treatment of Animals v. Doughney, the court ordered the defendant, Michael Doughney, to surrender the domain name[47]. Although Doughney claimed that his use of the domain peta.org was a parody protected under the First Amendment and free speech, the court rejected this defense[48]. Since the court believed that the domain name 'peta.org' could have caused consumer confusion, the court concluded that the domain name infringed upon the plaintiff's trademark rights[49]. Similarly, in Planned Parenthood Federation of America, Inc. v. Bucci (1997), the United States District Court for the Southern District of New York ruled in favor of the plaintiff, Planned Parenthood[50]. The court disagreed with Bucci's argument that this website was protected as free speech under the First Amendment to the U.S. Constitution[51], ruling that the plaintiff was not seeking to censor Bucci's speech, but rather to prevent his misleading use of its trademark.

[47] In 1995, Michael Doughney registered the domain name *peta.org* for a website titled "People Eating Tasty Animals." In 1996, PETA requested that Doughney voluntarily relinquish the domain, citing its ownership of the registered trademark "PETA." In response, Doughney argued that his website constituted a parody and was protected as an act of free speech under the First Amendment, thereby asserting that his use of the domain did not amount to trademark dilution or infringement.

[48] The court primarily relied on Cliffs Notes, Inc. v. Bantam Doubleday Dell Publishing Group, Inc. to determine whether Doughney's use of the domain name was a parody. The two key requirements of the use of the domain name as a parody were: to clearly convey that Doughney's website was not the official PETA site; and that peta.org was simply a parody rather than controlled by the PETA organisation itself. The court held that the domain name itself—peta.org—gave the impression that it was owned or operated by the actual organization - the domain name was identical to the 'PETA' mark -, and thus did not qualify as a parody.

[49] Doughney was subsequently ordered to relinquish the domain peta.org.

[50] Richard Bucci, an anti-abortion activist, registered the domain name "www.plannedparenthood.com" prior to the organisation itself having the chance to do so. Bucci subsequently used the domain name to display his own website, containing anti-abortion content and other similar content.

[51] The core issues considered by the court in this case were: Bucci's violation of the Lanham Act by using the website to advertise Lawrence Roberge's book 'The Cost of Abortion'; his provision of a service through the promotion of anti-abortion content; and the likelihood of confusion among users seeking Planned Parenthood's services, judged to create interference with the legitimate operations of the existing organization. As a result of these actions, Bucci was ordered to transfer the "plannedparenthood.com" domain to Planned Parenthood.

On the other hand, in Lamparello v. Falwell (2005), the Fourth Circuit ruled in favor of Lamparello, who had registered fallwell.com to criticize the views of Reverend Jerry Falwell[52]. The court emphasized that the website did not sell goods or services, nor did it attempt to mislead consumers[53] into thinking it was affiliated with Falwell. Since the domain was used solely for commentary and criticism[54], it was protected under the First Amendment and did not qualify as cybersquatting[55].

Therefore, the ACPA provides that as long as one's free speech does not encroach on what is forbidden under it—such as consumer exploitation or commercial intent—it is not restricted and thus remains protected under the First Amendment to the U.S. Constitution.

4.3.2 Canada – A Cautious Middle Ground on Parody and Free Speech

In Canada, freedom of expression is a fundamental right under Section 2(b) of the Canadian Charter of Rights and Freedoms. In the context of cybersquatting, freedom of expression is considered legal under the CDRP—and, where applicable, ICANN's UDRP—when the expression is non-commercial and not likely to be misleading.

Under the CDRP, Section 3.4(d) defines the non-commercial use of a domain name, such as for criticism (gripe sites), as a 'legitimate interest' and therefore legal. However, the clause requires that the action be carried out in good faith, meaning it must still pass through the CDRP process and be subject to the panel's assessment of whether the registrant acted in bad faith.

For instance, in Canadian Tire v. Mick McFadden, crappytire.com—a derogatory twist on a famous mark—was retained by McFadden because the panel found it to be non-infringing satire, not causing confusion or commercial harm.

Therefore, the CDRP upholds Canada's constitutional right to free speech under reasonable restrictions. Hence, the principle of free expression alone does not override actions or factors prohibited under the CDRP, such as the registration of a parody site with commercial intent or the registration of domain names likely to mislead the public.

4.3.3 India: Weaker Parody Protections, Trademark Prevails

India's legal system does not explicitly recognize parody or satirical commentary under the fair use principle of the Trademarks Act, 1999. While Article 19(1)(a) of the Indian Constitution guarantees freedom of speech, this right is subject to reasonable restrictions, including those related to defamation and decency.

---

[52] In 1999, Christopher Lamparello created "fallwell.com" to criticize Christian evangelical preacher Jerry Falwell's anti-homosexual views. Falwell, believing there was a confusing similarity between the domain name and his own name, sought legal action to block Lamparello's use of the mark "fallwell" and thus surrender ownership of the domain to Falwell.

[53] The Court utilized the 4th Circuit's seven-part test to assess whether the domain name had any likelihood of causing confusion amongst people: "(a) the strength or distinctiveness of the mark; (b) the similarity of the two marks; (c) the similarity of the goods/services the marks identify; (d) the similarity of the facilities the two parties use in their businesses; (e) the similarity of the advertising used by the two parties; (f) the defendant's intent; (g) actual confusion."

[54] The court ruled that the use of a mark in a domain name for a gripe site - a website dedicated to criticize or complain about a specific subject - criticizing the mark holder does not constitute cybersquatting. Rather, the Appeals Court ruled that nobody reading Lamparello's criticism would believe it was sponsored by Reverend Falwell himself, and thus constituted no claim of possible confusion.

[55] To be considered cybersquatting, it would have to be proven that Lamparello had bad faith intent to profit from the use of the "fallwell.com" domain, and that the domain name is likely to confuse the public. The Appeals court assessed the cases by considering: Lamparello's lack of intent to profit on his use of the domain name on account of: a lack of income from the site; the lack of an attempt to sell the domain name; and the fact that Lamparello had not purchased a large sum of domain names to display his critiques on Falwell.

However, Indian courts have ruled, in select cases, that satire and parody alone do not constitute trademark infringement. Courts often use the following criteria to judge exceptions: there must be no likelihood of public confusion resulting from the domain name and parody; no intent to profit or sell the domain to the trademark holder for profit in the future; no possibility of defaming the affected brand or mark; and no malicious intent in the content of the satire or parody.

Notably, in Tata Sons Ltd. v. Greenpeace International, the court dismissed Tata's claims of trademark infringement, stating that Greenpeace was invoking the right to freedom of expression by alerting the public to an environmental issue allegedly caused by Tata. The court found no intent to gain profit, no likelihood of public confusion, and it was clear that the domain was not officially endorsed by Tata.

Therefore, similar to Canada, India upholds and enforces the right to free speech under reasonable limits through the Indian Trade Marks Act, 1999. Hence, the registration of parody sites in bad faith—like other domain names—is considered illegal, while the registration of parody sites in good faith, often determined by the absence of intent to profit or cause public confusion, is not considered an act of trademark infringement.

4.3.4 Collective Discussion of Parody Cybersquatting

In the United States, freedom of speech under the First Amendment offers absolute protection for parody, satire, and criticism, but this right does not shield domain registrations made in bad faith, or domain names which risk consumer confusion (see section 4.3.1, para. 2). Therefore, the Anticybersquatting Consumer Protection Act (ACPA) ensures that registrants cannot invoke free speech as a defense when their intent is to mislead consumers or profit from confusion, while continuing to uphold the constitutional right to freedom of expression if the aforementioned are not proven.

Similarly, Canada protects free expression within the bounds of "reasonable limits" under the Canadian Charter of Rights and Freedoms. The CIRA Domain Name Dispute Resolution Policy (CDRP) recognizes non-commercial parody or criticism as a legitimate interest, provided it is not pursued in bad faith (see section 4.2.2).

The rationale behind the CDRP in the assessment of parody cybersquatting cases can be explored through the possible developments of the case of MikeRoweSoft v. Microsoft[56]. While Mike Rowe's domain could be viewed as legitimate non-commercial use since the domain name primarily consisted of his legal name, his later attempt to sell the domain for profit, alongside his intent to use the site to support Rowe's own web design business, could alternatively be seen as bad faith cybersquatting. This illustrates how structured frameworks like the CDRP allow decision-makers to weigh full context and intent behind registrations and reach balanced rulings that are both fair and predictable.

In contrast, India lacks clear statutory guidelines to differentiate legitimate satire from bad faith cybersquatting. Courts are left to resolve such disputes through case-by-case discretion, often leading to inconsistent outcomes. Though parody cybersquatting is not particularly problematic at the moment—as courts simply judge the context of the case to determine whether the parody itself is made in good faith using rulings from previous cases and general understanding of bad faith (see Sections 4.1.3 and 4.1.4)—this legislative gap could become increasingly problematic with the rising prevalence of 'meme' culture and internet satire. Given India's distinct constitutional values, it may not be feasible to adopt the ACPA or CDRP as a whole. Instead, India could benefit from introducing case-context-specific criteria—such as

[56] Though settled out of court, MikeRoweSoft v. Microsoft offers a useful hypothetical lens to explore the different perspectives a court might consider when assessing parody cybersquatting cases.

intent to profit, likelihood of confusion, and the genuine nature of the parody—to judge such cases without compromising free expression.

5 Proposed Reformations to Indian Law and Concluding Remarks

While the United States, Canada, and India approach cybersquatting with similar principles—focusing on intent, confusion, and harm—they differ significantly in their legal frameworks. The U.S., through the ACPA and Lanham Act, and Canada, via the CDRP and Canadian Trademarks Act, offer structured procedures, remedies, and clear definitions of key concepts such as bad faith. These frameworks enable courts to consistently adjudicate domain name disputes, including those not involving registered trademarks.

India, however, lacks a dedicated cybersquatting law and instead relies on the Trademarks Act, 1999 and the doctrine of passing off. This absence creates significant challenges for courts and litigants alike. Without a structured and normalized understanding of key concepts such as bad faith, commercial intent, or the distinction between parody and infringement, the resolution of domain name disputes becomes inconsistent and highly circumstantial.

For instance, without a clear standard to determine what constitutes bad faith or at what threshold profit-based intent arises, courts may struggle in assessing disputes where monetary gain is absent, but reputational harm or anti-competitive motives are alleged.

To begin, the existing issues within Indian law in dealing with cybersquatting cases can be explored through the 2023–2024 JioHotstar.com incident. A student registered the domain name 'jiohotstar.com' speculatively - an action labelled to be speculative cybersquatting (see table 1) - in anticipation of a merger between Jio and Disney+Hotstar. Although the student used the domain to seek funds for education—a seemingly noble cause—this could be clearly seen to have constituted bad faith due to the implied intent to profit. The domain was later transferred, by the student, to two UAE-based siblings who intended to repurpose it as an educational platform. Their foreign residency created jurisdictional challenges, and their lack of intent of commercial use made it even more difficult for Jio to justify reclaiming the domain. This case displays the challenge of proving bad faith, particularly in cases of speculative cybersquatting where the domain name did not directly infringe any existing trademark at the time of registration.

Therefore, it can be seen that one of the most significant gaps in India's current cybersquatting law is its lack of protection in disputes that do not involve registered trademarks. Presently, statutory remedies are largely confined to the misuse of registered marks, leaving complainants with little recourse when domain names, nicknames, monikers, or online reputations that lack formal registration are exploited. This limits enforcement in cases involving harmful or deceptive domain use that falls outside traditional definitions of infringement. Another gap arises from the limited scope of the INDRP, which applies only to disputes involving ".in" or ".bharat" domain names. Cases involving international domains like ".com" fall under the UDRP, which offers no monetary remedies and can complicate enforcement. To address this, India would benefit from establishing a dedicated anti-cybersquatting statute, similar in principle as that of the ACPA. Such a policy would allow courts to handle cybersquatting cases independent of the restrictions of trademark law.

Moreover, the absence of a standardized definition or framework for assessing bad faith in domain disputes. Although Indian courts have generally understood bad faith to mean the conscious doing of a wrong with dishonest intent (see Manish Vij v. Indira Chugh (2002)), this principle is applied inconsistently because there is no formal legislative guidance. This lack of clarity places an uneven burden on plaintiffs to prove intent, particularly in complex cases where there is no given method as to

how this can be done. Acts driven by spite, competitive obstruction, or reputational harm often fall into legal grey areas that current statutes struggle to resolve uniformly. To resolve this, India should introduce structured penalties, and establish the administration of statutory damages, modeled on frameworks like the ACPA. This would deter cybersquatting more effectively and provide compensation even when plaintiffs or courts cannot quantify financial loss, such in cases of brand defamation. Moreover, the establishment of comprehensive bad faith assessment criteria, through concepts such as legitimate interest and commercial intent (see section 4.1.4, para. 5), could guide courts in making consistent rulings when dealing with cases of intent of registration and bad faith.

Furthermore, jurisdictional limitations within the Indian Trade Marks Act, 1999, also create enforcement challenges, as the Act does not apply extraterritorially. Following the recommendations of scholars (Plotkin, 2015) [viii], India could adopt a model law approach as a long-term solution to this issue. This would promote uniformity across foreign jurisdictions as other countries adopt the proposed model law, which can be adapted over time in response to evolving legal interpretations. This may aid in the adjudication of cross-border cybersquatting cases through the establishment of a standardized anti-cybersquatting framework.

In addition, cases of anonymous cybersquatting (see table 1) are often hard to assess as well within the restrictions of the Indian Trade Marks Act. A solution could lie in enabling 'in rem' actions against domain names themselves—similar to provisions in U.S. law. This would allow cases to proceed even when the registrant's identity or location is unknown, optimising the process of reclaiming disputed domains (Plotkin, 2015) [viii].

Nevertheless, the socio-legal contexts of the U.S. and Canada differ significantly from India, potentially limiting the direct applicability of their frameworks and policies. Moreover, since this study focuses on select landmark cases across 3 jurisdictions, this paper may not fully encapsulate the complete spectrum of cybersquatting disputes. This could be improved in future studies through the analysis of a larger case set across a larger range of jurisdictions.

Future research could build on evolving legal interpretations from cybersquatting disputes—both within and beyond these three jurisdictions—to expand the case sample and offer further recommendations for improving Indian law. This ensures that, as the digital landscape continues to evolve, Indian law remains aligned, responsive, and just.

References

I. VerSteeg, R. (2018). Ancient Egyptian roots of trademarks. *The Antitrust Bulletin, 63*(3), 283–304. https://doi.org/10.1177/0003603X18780556

II. Rogers, E. S. (1910). Some historical matter concerning trade-marks. *Michigan Law Review, 9*(1), 29–43. https://repository.law.umich.edu/mlr/vol9/iss1/4

III. World Intellectual Property Organization. (2007). *Protocol relating to the Madrid Agreement concerning the international registration of marks.* https://www.wipo.int/wipolex/en/text/283484

IV. Chandra, R., & Bhatnagar, V. (2019). Cyber-squatting: A cyber crime more than an unethical act. *International Journal of Social Computing and Cyber-Physical Systems, 2*(2), 146–150. https://doi.org/10.1504/IJSCCPS.2019.100197

V. Trainer, T. P. (2008). Intellectual property enforcement: A reality gap (Insufficient assistance, ineffective implementation). *The John Marshall Review of Intellectual Property Law*, *8*(1), 47–79.

VI. Jain, A., & Gupta, E. (2024). Analyzing the efficacy of trademark enforcement against infringement of trademarks in India. *Indian Journal of Integrated Research in Law*, *4*(2).

VII. Naik Naik & Co. (2023, November 9). An analysis of the concept of cybersquatting & legal issues pertaining to trademarks in India. Retrieved from [URL]

VIII. Plotkin, J. (2015). The model for path forward: A proposal for model law dealing with cyber-squatting and other abusive domain name practices. *Denning Law Journal*, *27*, 204–240.

Copyrights