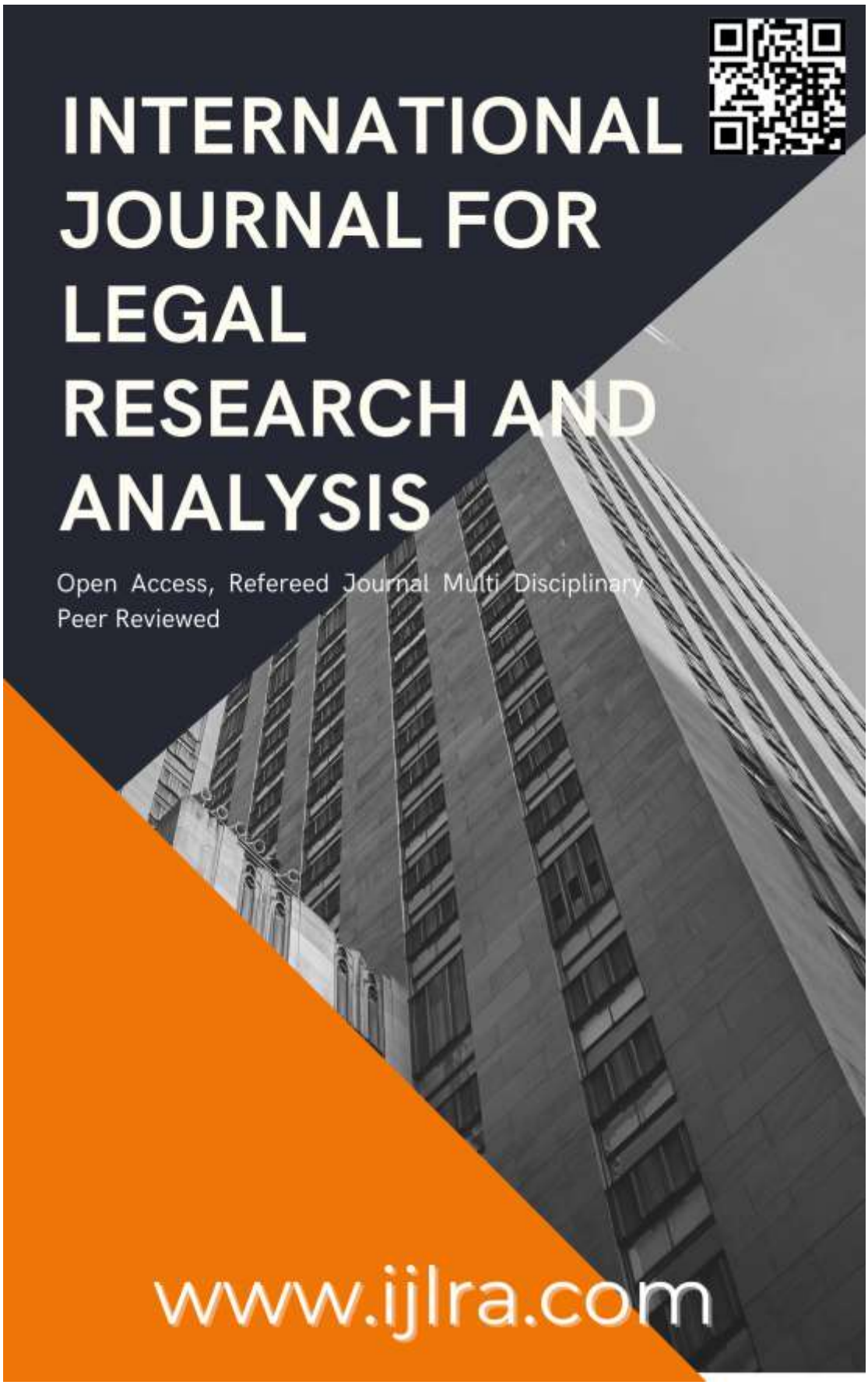

VOLUME 3 • ISSUE 8 • NOVEMBER 2026

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the International Journal for Legal Research & Analysis (IJLRA).

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ABOUT US

The International Journal for Legal Research & Analysis (IJLRA) (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the International Journal for Legal Research & Analysis aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The International Journal for Legal Research and Analysis (IJLRA) is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.

Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats.

The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published.

By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights.

The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

RESEARCH ARTICLE

Cybersquatting And Domain Name Disputes In India's E-Commerce Sector: A Study Of The INDRP/UDRP Framework In Comparison With The Us And Nigerian Statutory Models

Medisetti Jeevana Pragna

SASTRA Deemed University, School of Law

medisettijeevana@gmail.com

Abstract

In India's growing e-commerce market, a domain name is no longer just a website address it has become a valuable business asset that carries a brand's identity and trust. This has led to a rise in cybersquatting, where a person registers a domain name that copies or closely resembles a wellknown brand, either to sell it back for profit or to create a fake website used for phishing and online fraud. India does not have a separate law dealing with cybersquatting, so protection depends on the Trade Marks Act, 1999, along with two dispute resolution systems: the INDRP for ".in" domain names and the UDRP for international domain names. This paper studies how well these systems actually work in protecting both brands and customers in India's online market. It also compares India's position with two countries that handle cybersquatting differently: the United States, which has a dedicated civil law, the Anticybersquatting Consumer Protection Act, 1999, and Nigeria, which treats cybersquatting as a criminal offence under its Cybercrimes Act, 2015. The comparison looks at what these laws offer such as clear rules for proving bad intent, fixed compensation amounts, and the power to take direct legal action against the domain itself that India's present framework does not clearly provide. The study uses the doctrinal method, examining the Trade Marks Act, 1999, the INDRP and UDRP rules, and the relevant provisions of the US and Nigerian laws, to understand how each system defines and deals with cybersquatting. The paper will examine whether India's current civil approach is sufficient to address a problem that is increasingly used for fraud, or whether a separate law is needed.

Keywords

Cybersquatting, Domain Names, E-Commerce, Phishing, INDRP, UDRP.

Introduction

Background and Significance of the Research Area

A domain name began its life as a technical convenience, a readable stand-in for a numerical internet address. In e-commerce it has become much more than that. For a shopper who cannot see the seller, touch the goods or check a shop signboard, the web address is often the only assurance that the website in front of her belongs to the brand she has in mind. This is why the abusive registration of domain names, once seen as a mere nuisance of the early internet, has grown into a live commercial and consumer-protection problem. Cybersquatting is commonly understood as the registration or use of a domain name that corresponds to another person's trademark, in bad faith, in order to profit from the goodwill attached to that mark.[1] In practice it takes several forms: hoarding names to sell them to the mark owner at an inflated price, typosquatting on slight misspellings of a popular brand, and, increasingly, registering look-alike domains to run phishing pages

[1]15 U.S.C. § 1125(d)(1)(A); ICANN, Uniform Domain Name Dispute Resolution Policy (approved 24 October 1999) para 4(b).

or sell counterfeits.[2] The scale of the problem can be seen from the figures of the World Intellectual Property Organization (WIPO). WIPO reported that it administered more than 6,200 domain name cases in 2025, its highest caseload on record, and it has resolved over 80,000 cases since the "Uniform Domain Name Dispute Resolution Policy" (UDRP) came into being.[3] The sectors most often affected include banking and finance and retail, which are the very sectors that make up Indian e-commerce.[4] India makes an interesting case study, mainly because it has no statute that specifically deals with cybersquatting. A brand owner whose name has been hijacked online must instead choose between an action for infringement or passing off under the "Trade Marks Act, 1999", an arbitration under the ".IN Domain Name Dispute Resolution Policy" (INDRP) if the domain ends in .in, or a complaint under the UDRP if the domain sits in a generic top-level domain such as .com. The Supreme Court accepted this patchwork in "Satyam Infoway Ltd v Sifynet Solutions Pvt Ltd", where it held that a domain name can attract passing off protection even though no Indian law addressed domain names directly.[5] Two decades on, the position has not really changed in structure, even though the Indian e-commerce sector has grown enormously in the meantime. The choice of the United States and Nigeria as comparators is deliberate. The United States enacted a dedicated civil statute, the "Anticybersquatting Consumer Protection Act 1999" (ACPA), which sits inside its trademark law. Nigeria took a different road and made cybersquatting a criminal offence under "section 25" of the "Cybercrimes (Prohibition, Prevention, etc.) Act, 2015", while its country-code registry runs a dispute policy modelled on the UDRP. India, which has neither a civil statute nor a criminal provision, sits at a distinct point on this spectrum. Placing the three side by side lets this study ask what India could sensibly borrow, and what it would do well to avoid. The aim throughout is practical: to see whether the law, as it stands, gives an online business a dependable remedy when its name is taken.

Literature Review

Scholarship on domain name disputes is extensive, though it tends to gather around a handful of concerns. Five peer-reviewed works have been engaged here because each speaks to a different layer of the problem: the Indian common-law foundation, the design and legitimacy of the UDRP, its central bad-faith concept, the limits of the cybersquatting model, and the Nigerian statutory position. Each is discussed separately below, followed by a short synthesis.

Mukherjee, "Passing Off in Internet Domain Names - A Legal Analysis" (2004)

Mukherjee's article in the Journal of Intellectual Property Rights is an early Indian treatment of the subject.[6] It examines passing off as the tort through which domain name disputes were being handled in India, and compares the Indian position with that of other jurisdictions and international bodies, at a time when the "Trade Marks Act, 1999" had only just been notified. For this paper its value is mainly historical. It shows

[2]See eg *Shields v Zuccarini* 254 F 3d 476 (3d Cir 2001) (registration of misspelled variants of a well-known name held actionable under the ACPA).

[3]WIPO Arbitration and Mediation Center, '2025 Marks Record-Breaking Year for WIPO Domain Name Disputes' (14 January 2026) <https://www.wipo.int/amc/en/domains/news/2026/news_0001.html> accessed 28 September 2026.

[4]WIPO, 'Record Number of Domain Name Cases filed with WIPO in 2023' <https://www.wipo.int/amc/en/domains/caseload.html> accessed 28 September 2026 (listing banking and finance, biotechnology and pharmaceuticals, fashion, and retail as the top sectors in 2023).

[5]Satyam Infoway Ltd v Sifynet Solutions Pvt Ltd (2004) 6 SCC 145.

[6]Sunando Mukherjee, 'Passing Off in Internet Domain Names—A Legal Analysis' (2004) 9 Journal of Intellectual Property Rights 136.

that the reliance on passing off was a stop-gap solution adopted by courts and not a considered legislative choice, and that the ACPA had already been noted as a contrasting model at that early stage. Its limitation, given its date, is that it cannot address the INDRP, which came somewhat later, or the present scale of Indian e-commerce.

Helfer and Dinwoodie, "Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy" (2001)

Helfer and Dinwoodie offer the most influential analysis of the UDRP as a design problem.[7] They treat the UDRP as a non-national, privately administered system, and examine how its rules were drafted, how they depart from national trademark law, and what this means for the legitimacy of a regime that binds registrants through contract rather than through legislation. This matters directly for India, because the INDRP is, in essence, a national adaptation of the same contractual-arbitral idea. If the UDRP raises legitimacy questions of this kind, the INDRP inherits them, and the article's framework is used in this paper to examine that inheritance in Chapter II.

Gey, "Bad Faith under ICANN's Uniform Domain Name Dispute Resolution Policy" (2001)

Gey narrows the focus to a single concept, bad faith, and how it operates under the UDRP.[8] The concept matters because the whole framework depends on it: a registration that is merely similar to a mark is not enough, and the complainant must show abusive intent. This paper uses that strand of the literature to frame its comparison, since the three jurisdictions studied here define the culpable mental state in three different ways, as discussed in Chapter II. The article's limitation is that, being confined to the UDRP, it does not itself extend to the INDRP, the ACPA or the Nigerian provision, which this paper brings into the comparison.

Lipton, "Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy" (2005)

Lipton takes a critical step back from the trademark-owner's perspective that dominates most of the literature.[9] Her argument is that the UDRP, together with the ACPA, has been successful against classic cybersquatting, meaning the registration of names to extort a price from trademark owners, but that little thought has been given to other kinds of domain name disputes which the trademark-centred model serves poorly, such as gripe sites and fan sites. For an Indian study, this works as a caution against importing the ACPA wholesale. A law drawn only from the trademark owner's point of view risks catching criticism sites, fan sites and honest namesakes, and any Indian reform needs to build in safeguards for such legitimate, non-abusive registrants rather than assuming that every similar domain name is cybersquatting.

Gabriel-Whyte and Ajie, "The Cybercrimes (Prohibition, Prevention, etc) Act 2015: Legislative Ineptitude or Lack of Tact in Internet Matters?" (2025)

[7]Laurence R Helfer and Graeme B Dinwoodie, 'Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy' (2001) 43 William & Mary Law Review 141.

[8]Peter Gey, 'Bad Faith under ICANN's Uniform Domain Name Dispute Resolution Policy' (2001) 23(11) European Intellectual Property Review 507.

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

On the Nigerian side, Gabriel-Whyte and Ajie ask, in the very title of their article, whether the "Cybercrimes Act 2015" reflects legislative ineptitude or a lack of tact in internet matters.[10] Their discussion of the Act's offences includes "section 25", which they describe as prohibiting the intentional taking or use of a name, trademark or domain name belonging to another without authority, punishable by imprisonment or a fine. Read together with the earlier appraisal by Onadeko and Afolayan, this literature treats cybersquatting as one offence among many in an omnibus cybercrime statute rather than as a subject of dedicated trademark policy.[11] Its limitation for this paper is that, being focused on the Nigerian Act as a whole, it does not compare "section 25" against the Indian or American positions, which is precisely the gap this paper addresses.

Synthesis

Two observations emerge from this review. First, in the literature accessed for this paper, scholarship either studies the UDRP as a global system (Helfer and Dinwoodie, Gey, Lipton) or studies one national law in isolation (Mukherjee on India, Gabriel-Whyte and Ajie on Nigeria). Second, the Indian writing tends to state that India lacks a dedicated statute, without testing that gap against the two contrasting legislative models, one civil and one criminal, that this paper places side by side. This paper attempts to fill that space by reading all five works together against a common comparative framework. That gap is the starting point for the analysis that follows.

Research Gap

The existing literature on cybersquatting predominantly focuses either on the UDRP as an international domain-name dispute-resolution mechanism or on the domestic law of a single jurisdiction. Although India's legal position has received some independent attention, there is limited comparative scholarship evaluating it against contrasting regulatory models: the United States' civil enforcement regime and Nigeria's criminal-law response. This study therefore undertakes a comparative analysis of these three jurisdictions to assess the extent to which civil remedies, criminal sanctions, or a calibrated hybrid framework can most effectively address cybersquatting in India. The analysis is directed particularly at the needs of India's expanding e-commerce ecosystem, where domain-name misuse may affect trademark owners, online businesses, consumers, and market confidence.

Statement of the Research Problem

In effect, India protects domain names against cybersquatting through borrowed instruments. Trademark infringement needs a registered mark and passing off needs proven goodwill, both of which sit uneasily with a new online business whose reputation lives mostly on the internet.[12] The INDRP is confined to .in domains, and the UDRP, which covers .com and other generic domains where most Indian e-commerce actually trades, offers only transfer or cancellation and no damages.[13] At the same time, the United States has a statute with express bad-faith factors, safe harbours and statutory damages, and Nigeria has a criminal provision.[14] The

[10]Aladokiye E Gabriel-Whyte and Chukwuma O Ajie, 'The Cybercrimes (Prohibition, Prevention, etc) Act 2015: Legislative Ineptitude or Lack of Tact in Internet Matters?' (2025) 8(3) African Journal of Law, Ethics and Education (AJLEE) <https://ajleejournal.com> accessed 28 September 2026.

[11]Olanrewaju Adesola Onadeko and Abraham Femi Afolayan, 'A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria' <https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf> accessed 28 September 2026.

[12]See *Satyam Infoway* (n 5).

[13]ICANN, Uniform Domain Name Dispute Resolution Policy (approved 24 October 1999) para 4(i).

[14]15 U.S.C. § 1125(d)(1)(B) and § 1117(d).

problem this paper addresses is whether India's reliance on the "Trade Marks Act", the INDRP and the UDRP is adequate for the e-commerce sector, or whether the comparative models show a legislative gap that needs to be closed.

Research Objectives

The objectives of this study are:

(a) to identify and critically examine the legal sources through which cybersquatting is presently addressed in India, namely the "Trade Marks Act, 1999", judicial doctrine, the INDRP and the UDRP;

(b) to analyze the structure of the ACPA of the United States and "section 25" of the Nigerian "Cybercrimes Act, 2015", including their standards of liability and remedies;

(c) to compare the three systems on defined criteria, particularly the bad-faith standard, the forum, the remedies and the protection of legitimate registrants; and

(d) to assess the adequacy of the Indian framework for e-commerce businesses and to suggest reforms that follow from the comparison.

Research Questions

The study is guided by the following questions, which are framed to probe the reasons behind the legal position and not merely to describe it:

(1) To what extent can the absence of a dedicated cybersquatting statute in India be justified, given that Indian courts and the INDRP have already built a workable body of doctrine?

(2) How does the bad-faith standard differ under the INDRP, the UDRP, the ACPA and "section 25" of the Nigerian Act, and what consequences does each difference have for brand owners and for legitimate registrants?

(3) Why does an administrative or arbitral route succeed in cases of phishing and typosquatting where a court-based route is slow, and what does this reveal about the design of remedies in each system?

(4) Which features of the American civil model and of the Nigerian criminal model, if any, are suitable for adoption in India without over-protecting trademark owners?

Scope and Limitation of the Study

The study is confined to the abusive registration and use of domain names that correspond to trademarks, with particular attention to online commerce. On the Indian side it covers the "Trade Marks Act, 1999", the leading judicial decisions, the INDRP and the UDRP as applied to Indian parties. On the comparative side it covers the ACPA, "section 25" of the Nigerian "Cybercrimes Act, 2015", and the Nigerian registry's dispute policy in outline. Other jurisdictions, such as the United Kingdom and the European Union, are not covered. Broader issues such as trademark dilution generally, data protection, and the technical workings of the domain name system are also outside the scope. The study also has some limitations. It is a purely doctrinal work and does not contain empirical data such as a systematic count of INDRP awards. It relies on published statutes, decisions and secondary writing, and where a primary text could not be examined directly (for example, individual INDRP awards) it depends on reliable secondary summaries. Reported Nigerian judicial decisions on "section 25" were not located in the sources consulted, so the Nigerian analysis rests on the statutory text and commentary. Lastly, statutory penalties and policies are stated as they appear in the sources available at the time of writing, and they may since have been amended.

Research Methodology

This paper follows the doctrinal method combined with the comparative method. The doctrinal method is suited to a question about what the law is and whether it is adequate, because the materials are statutes, policies and judicial decisions and not human respondents. For the same reason no research hypothesis has been framed. Instead, the inquiry is structured through the research questions. The comparative part follows the functional approach associated with Zweigert and Kötz, under which different legal systems are compared by asking how each solves the same practical problem.[15] The common problem is the bad-faith use of a trademark as a domain name. Each system is compared on six criteria: the legal source; the test for liability; the bad-faith standard; the forum; the remedies; and the safeguards for legitimate registrants.

Primary sources were collected from official or authoritative repositories: the text and legislative history of the ACPA from the United States Congress, the INDRP text from the .IN Registry, the UDRP framework as described by WIPO, and the Nigerian Cybercrimes Act from Nigerian government-hosted copies. Case law was drawn from law reports and from court publications. Secondary sources were drawn from peer-reviewed journals and, where these were silent on recent developments, from practitioner commentary, which is treated with corresponding caution. The material has been analyzed by interpreting the text, tracing how courts and panels have applied it, and then placing the three systems against the six criteria. The possible weaknesses of this method are its dependence on the accuracy of secondary summaries and the absence of quantitative evidence.

Findings: The Indian Framework

Trade mark law and passing off

The "Trade Marks Act, 1999" does not mention domain names or cybersquatting. Protection is obtained by fitting the domain name within the general concepts of the Act. Registered mark owners may sue for infringement under "section 29", and "section 27(2)" preserves the common-law action for passing off.[16] The "Information Technology Act, 2000" contains offences relating to computer misuse, but none of them is directed at the bad-faith registration of a domain name, and commentators note that the general cyber offences do not comprehensively cover cybersquatting.[17]

The judicial response

Indian courts stepped in early to fill the gap. In *"Yahoo! Inc v Akash Arora"* the Delhi High Court granted an injunction against the use of the name 'Yahoo India' for similar services, treating the domain name as capable of protection against passing off.[18] In *"Rediff Communication Ltd v Cyberbooth"*, the Bombay High Court restrained the use of 'radiff.com', which was confusingly similar to 'rediff.com', and recognized the

[15]Konrad Zweigert and Hein Kötz, *Introduction to Comparative Law* (3rd edn, Oxford University Press 1998).

[16]Trade Marks Act 1999 (India), ss 27(2), 29.

[17]International Journal of Legal Science and Innovation, 'Pursuing Cybersquatting as a Trademark Infringement under the IP Regime' vol 6 issue 2, 297 <https://ijlsi.com/paper/pursuing-cybersquatting-as-a-trademark-infringement-under-the-ip-regime/> accessed 28 September 2026 (noting the absence of tailored legislation and the inadequacy of the Indian Penal Code and Information Technology Act).

[18]*Yahoo! Inc v Akash Arora* 1999 PTC 201 (Del).

commercial value of a domain name as a corporate asset.[19] *"Tata Sons Ltd v Manu Kosuri"* extended the same reasoning to the registration of well-known names by persons with no connection to the brand.[20]

The Supreme Court's decision in *"Satyam Infoway"* is the anchor. The Court observed that no Indian statute expressly governs domain names, but held that this did not exclude protection under the law of passing off, and it recognised that a domain name has evolved from a mere technical address into a business identifier that distinguishes goods and services.[21] The consequence of this deserves attention. A plaintiff in India must still prove the classic trinity of goodwill, misrepresentation and damage, so a business that has not yet built reputation, or whose reputation is in another country, may find the route difficult. This is the practical weakness that keeps recurring through the rest of the paper.

The .IN Domain Name Dispute Resolution Policy

The INDRP is administered by the National Internet Exchange of India (NIXI) through the .IN Registry and applies to .in domain names. Under "paragraph 4", a complainant must show that the domain name is identical or confusingly similar to a name, trademark or service mark in which it has rights, that the registrant has no rights or legitimate interests, and that the domain name has been registered or is being used in bad faith.[22] The drafting is worth noticing, because the third ground is disjunctive. Registration or use in bad faith is enough, whereas the UDRP requires both. The Registry appoints an arbitrator from its panel, and proceedings are conducted under the "Arbitration and Conciliation Act, 1996", as amended in 2019.[23] Remedies are limited to cancellation or transfer of the domain name, with costs at the arbitrator's discretion, and decisions are published.

A practitioner review of the first fifteen years of the INDRP reported that more than 97 per cent of decisions had favoured complainants, but also observed a shift, with arbitrators dismissing complaints where the respondent had adopted the name earlier and used it for a genuine business, and holding that a mere fear of future sale cannot by itself establish bad faith.[24] Because the policy operates as arbitration, a party dissatisfied with an award must look to the challenge routes of the "Arbitration and Conciliation Act, 1996", and not to a dedicated appeal.[25]

The UDRP and Indian e-commerce

For .com and other generic domains, an Indian brand owner must use the UDRP or the courts. The UDRP requires the complainant to establish three cumulative elements: identity or confusing similarity with a mark,

[19]*Rediff Communication Ltd v Cyberbooth* AIR 2000 Bom 27.

[20]*Tata Sons Ltd v Manu Kosuri* 2001 PTC 432 (Del).

[21]*Satyam Infoway* (n 5).

[22].IN Registry, '.IN Domain Name Dispute Resolution Policy (INDRP)' <https://www.registry.in/domaindisputeresolution> accessed 28 September 2026.

[23]ibid; Arbitration and Conciliation Act 1996 (India) (No 26 of 1996), as amended by the Arbitration and Conciliation (Amendment) Act 2019 (No 33 of 2019).

[24]Mondaq, '15 Years On: A Relook At The INDRP Policy' (6 July 2020) <https://www.mondaq.com/india/trials-appeals-compensation/962248/15-years-on-a-relook-at-the-indrp-policy> accessed 28 September 2026. This is practitioner commentary and the statistic should be read accordingly.

[25]Lexology, 'Frequently Asked Questions (FAQ) on .in Domain Dispute Resolution' (20 February 2025) <https://www.lexology.com/library/detail.aspx?g=4858c97f-5885-4d44-a2aa-5fe155ee5dd2> accessed 28 September 2026.

the absence of rights or legitimate interests, and registration *and* use in bad faith.[26] The proceedings are generally document-based and comparatively quick and inexpensive, and the usual remedies are transfer or cancellation.[27] Even large Indian companies run into the limits of the UDRP. In a 2025 decision, Reliance Industries, holding a large portfolio of RELIANCE marks, was refused transfer of a domain name registered by another Indian company that was using it for its own wood-manufacturing business.[28] The outcome shows that a genuine business use by the registrant weighs heavily against a finding of bad faith, which is arguably the right result for a policy aimed at abuse and not at every overlapping name.

Findings: The United States Model

The ACPA was enacted in 1999 as "section 43(d)" of the "Lanham Act", codified at "15 U.S.C. § 1125(d)".[29] It makes a person liable in a civil action to the owner of a mark if that person has a bad-faith intent to profit from the mark and registers, traffics in or uses a domain name that is identical or confusingly similar to a distinctive mark, or identical, confusingly similar or dilutive of a famous mark.[30] The statute applies without regard to the goods or services of the parties, which means the defendant need not be a competitor.

What sets the Act apart is its list of nine non-exclusive factors that a court may consider in judging bad faith. They include the defendant's own intellectual property rights in the name, prior bona fide use, bona fide non-commercial or fair use, the intent to divert consumers in a way that could harm goodwill, an offer to sell the name without having used it, and false contact information at registration.[31] The statute also contains a safe harbour for a person who believed, and had reasonable grounds to believe, that the use of the domain name was lawful.[32] Courts have relied on these tools to separate abuse from legitimate expression. The Ninth Circuit has held that using another's mark in a domain name to gain leverage in a business dispute is enough to show bad-faith intent,[33] whereas the Fourth Circuit found no liability for a critic who registered a domain name

[26]Lexology, 'When your name is taken: domain name dispute resolution, cybersquatting, and the limits of policy-based justice in brand protection' (26 August 2026) <https://www.lexology.com/library/detail.aspx?g=78853699-f7a7-49d9-9875-29e427a7d915> accessed 28 September 2026.

[27]ICANN, Uniform Domain Name Dispute Resolution Policy (approved 24 October 1999) paras 4(a), 4(i).

[28]Lavoix, 'UDRP complaint: counterfeiting is not equivalent to cybersquatting' (22 September 2025) <https://www.lavoix.eu/udrp-complaint-counterfeiting-is-not-equivalent-to-cybersquatting/?lang=en> accessed 28 September 2026.

[29]Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (Pub L 106-113); S Rep No 106-140 (1999) <https://www.congress.gov/committee-report/106th-congress/senate-report/140/1> accessed 28 September 2026.

[30]15 U.S.C. § 1125(d)(1)(A)(i)–(ii).

[31]15 U.S.C. § 1125(d)(1)(B)(i). See also the summary in Revision Legal, 'Cybersquatting Bad Faith Factors: The ACPA's 9-Factor Test' <https://revisionlegal.com/internet-law/cybersquatting-lawyer/cybersquatting-bad-faith-factors/> accessed 28 September 2026.

[32]15 U.S.C. § 1125(d)(1)(B)(ii).

[33]*DSPT International Inc v Nahum* 624 F 3d 1213 (9th Cir 2010); see the Ninth Circuit Manual of Model Civil Jury Instructions, 'Anti-Cybersquatting (15 U.S.C. § 1125(d))' <https://www.ce9.uscourts.gov/jury-instructions/civil/chapter-15/15-33-anti-cybersquatting-15-u-s-c-1125-d/> accessed 28 September 2026.

resembling that of a well-known preacher in order to respond to his views.[34] The Second Circuit, in an early decision, applied the Act to a domain name registered to prevent a competitor from using it.[35]

On remedies, the ACPA goes beyond transfer. A court may order forfeiture, cancellation or transfer of the domain name, and the plaintiff may elect statutory damages per domain name instead of proving actual loss.[36] The Act also allows an in rem action against the domain name itself in certain circumstances, which is helpful where the registrant is anonymous or abroad.[37] Trademark owners are free to choose between a federal suit and the UDRP.[38]

Findings: The Nigerian Model

"Section 25(1)" of the Nigerian "Cybercrimes (Prohibition, Prevention, etc.) Act, 2015" makes it an offence for a person to intentionally take or make use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by an individual, a body corporate or a government body, on the internet or any other computer network, without authority or right, and for the purpose of interfering with its use by the owner, registrant or legitimate prior user.[39] The reported penalty is imprisonment for up to two years or a fine of up to five million naira.[40] "Section 25(2)" directs a court on the factors to consider in awarding a penalty.[41] The Act was amended in February 2024, but the summaries consulted for this paper describe changes to surveillance, data retention, levies and other provisions, and do not indicate a change to the substance of "section 25".[42]

Three features of the Nigerian model stand out. First, its mental element is drafted as intent to interfere with the owner's use, which is different from the American 'bad-faith intent to profit' and from the two-limbed UDRP standard. Second, the offence is prosecuted by the State, so a brand owner can report a squatter but does not itself control the proceeding. Third, private and administrative routes continue to exist alongside the offence: the .ng registry, the Nigeria Internet Registration Association (NiRA), operates a dispute resolution

[34] *Lamparello v Falwell* 420 F 3d 309 (4th Cir 2005).

[35] *Sporty's Farm LLC v Sportsman's Market Inc* 202 F 3d 489 (2d Cir 2000).

[36] 15 U.S.C. § 1125(d)(1)(C) and § 1117(d). The statutory range is US$1,000 to US$100,000 per domain name.

[37] 15 U.S.C. § 1125(d)(2).

[38] The Fashion Law, 'What is the Anticybersquatting Consumer Protection Act?' <https://www.thefashionlaw.com/resource-center/anticybersquatting-consumer-protection-act/> accessed 28 September 2026.

[39] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria), s 25(1), as quoted in Global Law Experts, 'Cyber-squatting And The Protection Of Domain Names In Nigeria' (20 August 2023) <https://globallawexperts.com/cyber-squatting-and-the-protection-of-domain-names-in-nigeria/> accessed 28 September 2026. The full text is available at <https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf>.

[40] Gabriel-Whyte and Ajie (n 10).

[41] Cybercrimes Act 2015 (Nigeria), s 25(2); see the text at <https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf> accessed 28 September 2026.

[42] Hamu Legal, 'Highlights of Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024' (17 May 2024) <https://hamulegal.com/highlights-of-cybercrimes-prohibition-prevention-etc-amendment-act-2024/> accessed 28 September 2026.

policy modelled on the UDRP, and the "Trade Marks Act" remains available for infringement.[43] Nigeria thus has three overlapping layers, although the statutory layer is penal in design.

Findings: Comparative Summary

Comparative Summary of the Indian, American and Nigerian Frameworks

Criterion	India	United States	Nigeria
Legal source	Trade Marks Act 1999; passing off; INDRP (for .in); UDRP (for gTLDs). No dedicated statute.	ACPA, 15 U.S.C. § 1125(d); UDRP also available.	Cybercrimes Act 2015, s 25; NiRA dispute policy; Trade Marks Act.
Nature of liability	Civil (tort/infringement) and arbitral.	Civil statutory liability.	Criminal offence, plus administrative policy.
Bad-faith standard	INDRP: registered OR used in bad faith. UDRP: registered AND used in bad faith.	Bad-faith intent to profit, judged on nine non-exclusive factors.	Intentional use without right, for the purpose of interfering with the owner's use.
Forum	High Courts/District Courts; NIXI arbitrators; UDRP providers.	Federal courts (including in rem); UDRP providers.	Criminal courts; registry-level policy.
Remedies	Injunction and damages (courts); transfer or cancellation (INDRP/UDRP).	Forfeiture, cancellation, transfer; statutory damages of US$1,000 to US$100,000 per domain name.	Imprisonment up to 2 years or fine up to N5,000,000 (as reported).
Safeguards for legitimate registrants	Legitimate-interest limb in policies; goodwill requirement in passing off.	Statutory factors, fair-use and safe harbour.	Requirement of intent and absence of right; no detailed statutory factors.

Source: compiled by the author from the Indian, American and Nigerian statutes, policies and decisions discussed in the findings sections of this paper

Discussion

Bad faith as the fault line

The comparison shows that all three systems use the idea of bad faith or wrongful intent as the gatekeeper, but they draw it differently. The UDRP asks for registration and use in bad faith, a conjunctive test that protects registrants who acquire a name innocently and change their conduct later. The INDRP, by asking for registration or use, lets a complainant succeed where a name was innocently acquired but is being used abusively. This is a more complainant-friendly formulation, and it may partly explain the high success rate reported for complainants, though causation cannot be claimed without a systematic study. The ACPA offers the most structured approach because its factors give both sides something concrete to argue, and the Nigerian

[43] 1st Attorneys, 'Domain Name Registration and Protection in Nigeria: Legal Frameworks and Emerging Trends' (2 November 2024) <https://1stattorneys.com/articles/2024/10/24/domain-name-registration-and-protection-in-nigeria-legal-frameworks-and-emerging-trends/> accessed 28 September 2026. See also Mondaq, 'Cybersquatting In Nigeria: Challenges And Countermeasures' (13 September 2024) <https://www.mondaq.com/nigeria/technology/1517092/cybersquatting-in-nigeria-challenges-and-countermeasures> accessed 28 September 2026.

provision offers the least structure. Gey's focus on bad faith is therefore not a narrow point. In the end, the standard decides who wins.

Is the Indian patchwork adequate for e-commerce?

The first research question asks whether the absence of a statute can be justified. The honest answer is a mixed one. On the positive side, Indian courts and INDRP arbitrators have produced coherent doctrine, and *"Satyam Infoway"* gives a firm base. In clear cases of phishing or typosquatting the arbitral route works fast and cheaply. However, three weaknesses appear on closer reading.

The first weakness lies in the dependence on goodwill. Passing off protects reputation that already exists, so a new marketplace or a D2C brand that has registered its trademark but has not yet built a reputation is protected less securely than the ACPA's framework, which needs only a distinctive mark. The second weakness is the limitation of remedies. Under both the INDRP and the UDRP the successful complainant receives the domain name and nothing more, and serial squatters face no financial deterrent. Statutory damages of the American type would change that calculation.[44] The third weakness is coverage. The INDRP reaches only .in, yet e-commerce businesses commonly operate on .com, where they must go to the UDRP, which is designed for speed but does not create any Indian-law remedy. Lipton's warning that a trademark-owner-centred model can over-reach does, however, apply in the other direction as well. The INDRP contains no statutory list of fair-use factors comparable to the ACPA's, and it leaves to individual arbitrators the task of protecting criticism sites and honest namesakes.

Speed against safeguards

The third research question asks why administrative routes succeed where courts are slow. E-commerce fraud based on look-alike domains causes harm within hours, and a suit for injunction in a civil court cannot match the time-scale of a UDRP or INDRP complaint. The literature on the UDRP nonetheless reminds us that speed carries costs. Helfer and Dinwoodie's analysis of the UDRP as a non-national system shows that a fast contractual process draws its legitimacy from procedural fairness and reasoned, published decisions. The INDRP's requirement that decisions be published is therefore a real strength, and it should be preserved in any reform.

What India can learn from the two models

From the United States, India can take the structured factors, the safe harbour and the statutory damages, which respond directly to the weaknesses identified above. The American experience also shows that a statute can accommodate free speech, as in *"Lamparello"*, if the factors are drafted with care.[45] From Nigeria, the lesson is narrower: a criminal provision has some value, but only where the conduct is aggravated and clearly fraudulent, such as phishing or impersonation, since the Nigerian experience shows that criminal liability alone gives trademark owners no transfer remedy of their own and generates little visible judicial interpretation. The paper therefore argues that India's primary response should be civil, built on the ACPA's structured approach within the "Trade Marks Act", with criminal liability retained only as a narrow, secondary tool for the clearest cases of fraud.

Conclusion

This paper examined whether India's reliance on the "Trade Marks Act, 1999", the INDRP and the UDRP adequately protects e-commerce against cybersquatting, against the American statutory model and the

[44]15 U.S.C. § 1117(d).

[45]*Lamparello* (n 34).

Nigerian criminal model. The study finds the Indian position only partly defensible. Judicial and arbitral doctrine handles obvious cases well, but it still carries the goodwill requirement of passing off and offers no remedy beyond transfer or cancellation.

The real divide among the four systems is the bad-faith standard: the INDRP is disjunctive, the UDRP conjunctive, the ACPA structured around nine factors and a safe harbour, and the Nigerian offence built on intent to interfere. Administrative routes succeed where courts are slow because they are document-based and quick, though that speed depends on reasoned, published decisions to stay legitimate. Between the two comparators, the American civil model offers India more to work with than Nigeria's criminal one, provided its safeguards for legitimate registrants travel along with its remedies. This matters all the more because Indian e-commerce runs on consumer trust in web addresses, and a framework that protects only established reputations with only a transfer remedy leaves newer, more vulnerable businesses the least protected. The study therefore concludes that India's current patchwork, while workable for clear-cut cases, is inadequate for a fast-growing e-commerce sector, and that India should adopt an enhanced civil-law framework as its primary response to cybersquatting, modelled on the ACPA's structured approach, while permitting narrow criminal liability only for aggravated and clearly fraudulent cases.

Suggestions and Future Directions

(1) A statutory provision within the "Trade Marks Act, 1999", as the primary civil remedy. Parliament could insert a specific provision on bad-faith domain name registration, with a bad-faith test, a non-exhaustive list of factors and a safe harbour, taking the ACPA structure as a reference point but drafting it in the language of Indian trademark law. Protection should extend to distinctive registered marks without a separate goodwill requirement, and to well-known marks in line with the Act's existing provisions. This civil route should remain the primary response to cybersquatting in India.

(2) A narrow, secondary criminal offence for aggravated fraud. Drawing on the Nigerian experience, criminal liability should not be the primary tool but a limited, secondary one, confined to aggravated and clearly fraudulent cybersquatting such as phishing or impersonation, where the harm is immediate and dishonest intent is plain. The civil route under recommendation (1) should remain the main protection for ordinary trademark owners.

(3) Statutory damages and a defined role for costs. A range of statutory damages per domain name, together with a power to award costs, would give courts a deterrent tool against serial squatters and would remove the difficulty of proving actual loss.

(4) Sanction against abusive complaints. Since the INDRP is reported to be heavily complainant-favouring, the policy should expressly recognise reverse domain name hijacking and allow arbitrators to record a finding against a complainant who uses the policy in bad faith.

(5) Clearer legitimate-use factors in the INDRP. The policy could adopt an illustrative list of fair-use and non-commercial-use factors, so that outcomes for criticism sites and honest namesakes depend less on the individual arbitrator.

(6) Rapid response for phishing. An expedited track, with cooperation from the Registry and registrars, for domains that are used to impersonate banks or online marketplaces would respond to the speed at which such harm occurs.

(7) Transparency. NIXI should publish periodic statistics on INDRP filings and outcomes, which would make future empirical study possible and would strengthen the legitimacy of the process.

Future Directions for Research

Several lines of further inquiry follow naturally from this study. An empirical study of INDRP awards, measuring outcomes, timelines and the reasons for dismissal, would allow the arguments made here about the disjunctive bad-faith test to be tested with data, and would justify a proper hypothesis. A study of Nigerian prosecutions and court decisions under "section 25" would fill the gap identified in this paper. The UDRP itself is under review, and WIPO-linked commentary refers to a 2025-26 review of the policy, which India should follow closely.[46] Finally, developments such as new top-level domains, the .Bharat script domains and non-DNS naming systems raise the question of whether a domain-name-specific statute would age well, or whether a broader online-identifier provision would be a wiser drafting choice.

Journal intended for publication: Indian Journal of Integrated Research in Law (IJIRL), ISSN 2583-0538. The paper is formatted according to this journal's submission guidelines.

[46]Lexology (n 26).