International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersquatting: Legal Framework, Judicial Response and Emerging Challenges in The Regulation of Domain Name Abuse

Ashwin Yadav[1], Bharti Yadav[2]

[1]Ph.D. Scholar, Amity Law School, Amity University, Gwalior
[2]Assistant Professor, College of Law, IPS Academy, Indore

Abstract:
Domain names have evolved from mere technical addresses into valuable commercial identifiers, a transformation that has, since the mid-1990s, given rise to the practice known as cybersquatting: the bad-faith registration of internet domain names identical or confusingly similar to the trademarks, service marks or names of others, undertaken with intent to profit from the goodwill attached to those marks. This paper examines the conceptual contours and typology of cybersquatting, surveys the international legal response embodied in the Uniform Domain Name Dispute Resolution Policy and the United States' Anticybersquatting Consumer Protection Act, and analyses how Indian courts, in the absence of dedicated domestic legislation, have extended trademark and passing-off principles to protect domain names, from *Yahoo!, Inc. v. Akash Arora* to the Supreme Court's decision in *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.* The paper further evaluates the .IN Domain Name Dispute Resolution Policy administered by the National Internet Exchange of India, identifies persisting gaps in the Indian regulatory framework, and concludes with recommendations for reform.

Keywords: Cybersquatting; Domain Names; Trademark Law; Passing Off; UDRP; INDRP; Anticybersquatting Consumer Protection Act.

I. INTRODUCTION

Since the commercialisation of the internet in the mid-1990s, the domain name system has functioned as the address book of cyberspace, translating numerical internet protocol addresses into memorable alphanumeric strings through which businesses, institutions and individuals are located online. Because domain names are allocated on a first-come, first-served basis by registrars who do not, as a rule, verify whether an applicant holds any pre-existing right in the string sought to be registered, a structural gap opened up between the technical process of domain registration and the substantive, rights-based logic of trademark law. That gap was quickly exploited. Persons unconnected with a business would register domain names incorporating well-known trademarks, either to sell them back to the rightful owner at an inflated price, to divert traffic for commercial gain, or simply to prevent the trademark owner from establishing an online presence under its own name. This practice came to be known as cybersquatting, a term coined by analogy with the older practice of squatting on land or property belonging to another.

As electronic commerce grew from a novelty into critical business infrastructure, the domain name attached to a trademark ceased to be a mere technical convenience and became, in itself, a valuable

commercial asset, carrying with it goodwill, consumer recognition and, frequently, considerable resale value. Cybersquatting accordingly emerged as a distinct and economically significant form of intellectual property abuse, prompting a coordinated international response led by the World Intellectual Property Organization and the Internet Corporation for Assigned Names and Numbers, as well as domestic legislative intervention in jurisdictions such as the United States. India, by contrast, has never enacted a cybersquatting-specific statute; the task of adapting trademark doctrine to the digital domain name space has instead fallen almost entirely upon the judiciary.

This paper undertakes a doctrinal examination of cybersquatting law. Part II sets out the conceptual meaning and principal typologies of cybersquatting. Part III surveys the international legal response, focusing on the Uniform Domain Name Dispute Resolution Policy and the United States' Anticybersquatting Consumer Protection Act. Part IV traces the evolution of Indian law through the principal judicial decisions and examines the .IN Domain Name Dispute Resolution Policy. Part V offers a comparative assessment, Part VI identifies emerging challenges, Part VII proposes recommendations for reform, and Part VIII concludes.

II. CONCEPTUAL FRAMEWORK: MEANING, ORIGIN AND TYPOLOGY

Cybersquatting has no single, universally codified definition, but its essential contours are well settled across jurisdictions and dispute-resolution regimes. The WIPO Report that preceded the UDRP described the practice as the deliberate, bad-faith registration of domain names in violation of the rights of trademark owners, an activity that consulted stakeholders across the internet community regarded as indefensible and warranting a dedicated administrative remedy.[1] The United States' ACPA supplies the most precise statutory formulation, imposing liability on a person who has a bad-faith intent to profit from a mark and who registers, traffics in or uses a domain name that is identical or confusingly similar to a distinctive mark, or identical, confusingly similar to, or dilutive of a famous mark.[2]

Distilled from these sources, cybersquatting is generally understood to require: first, the registration, trafficking in, or use of a domain name; second, identity or confusing similarity between that domain name and a trademark, service mark or, in some regimes, a personal name in which another party holds rights; third, the absence of any right or legitimate interest on the part of the registrant; and fourth, bad faith, ordinarily evidenced by an intention to sell the domain to the rights holder for valuable consideration in excess of documented registration costs, an intention to prevent the rights holder from reflecting its mark in a corresponding domain, an intention to disrupt the business of a competitor, or an intention to attract internet users for commercial gain by creating a likelihood of confusion.

Several recurring typologies may be identified within this broad definition. The first is classic or blatant cybersquatting, in which a person registers a domain identical to a well-known mark with no intention of using it for any legitimate purpose other than resale to the rights holder, illustrated by the American decision in *Panavision International, L.P. v. Toeppen*, where the registrant sought thirteen thousand dollars from the trademark owner in exchange for releasing domain names corresponding to its marks.[3] The second is typosquatting, in which the registrant adopts a domain name that is a deliberate misspelling

[1]World Intellectual Property Organization, The Management of Internet Names and Addresses: Intellectual Property Issues, Final Report of the WIPO Internet Domain Name Process, paras. 135-168 (Apr. 30, 1999).

[2]The Anticybersquatting Consumer Protection Act, 1999, 15 U.S.C. § 1125(d)(1)(A) (U.S.).

[3]*Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316 (9th Cir. 1998).

or minor visual variant of an established mark, calculated to capture traffic from internet users who make typing errors; the Indian decision concerning the domain "radiff.com", registered in apparent imitation of "rediff.com", is a well-known illustration.[4] Closely related is the registration of domains that trade on the phonetic or visual similarity of generic or descriptive terms once those terms have, through use, acquired secondary meaning associated with a particular business, as occurred in the dispute between "naukri.com" and "naukari.com".[5]

A third category is name-jacking, the registration of a living or deceased person's name as a domain, which several jurisdictions address separately from ordinary trademark-based cybersquatting; the ACPA, for instance, contains a distinct provision protecting any living person against the bad-faith registration of a domain name consisting of that person's name where the domain is registered with the intent to profit by selling it for financial gain.[6] A fourth, and inverse, category is reverse domain name hijacking, where a trademark owner, rather than a squatter, misuses dispute-resolution mechanisms in an attempt to wrongfully wrest a domain name away from a registrant who in fact possesses a legitimate right or interest in it; both the UDRP and its Indian counterpart recognise this as an abuse of process in its own right.[7] It is equally important to distinguish genuine cybersquatting from legitimate uses that merely resemble it on the surface, such as bona fide prior registration, non-commercial criticism or "gripe" sites, and coincidental registration of generic or descriptive strings, since dispute-resolution panels and courts alike require proof of bad faith and absence of legitimate interest before intervening.

III. THE INTERNATIONAL LEGAL RESPONSE

A. The WIPO Process and the Uniform Domain Name Dispute Resolution Policy

Recognising that the cross-border character of the internet made conventional litigation an unsatisfactory response to domain name abuse, WIPO, at the request of its member states and the nascent ICANN, conducted an extensive international consultation between 1998 and 1999, culminating in a report that recommended the creation of a mandatory administrative procedure for the resolution of abusive registrations.[8] Acting on those recommendations, the ICANN Board of Directors adopted the Uniform Domain Name Dispute Resolution Policy at its meeting in Santiago, Chile, on 25-26 August 1999, and the accompanying procedural rules on 24 October 1999; the Policy became fully operative on 1 December 1999.[9] Because the UDRP is incorporated by reference into the standard registration agreement that every registrant of a generic top-level domain such as ".com", ".net" or ".org" must accept, it binds registrants contractually rather than through direct state action, giving it a genuinely global reach unattainable through domestic legislation alone.

Under paragraph 4(a) of the Policy, a complainant must establish, cumulatively, that the disputed domain name is identical or confusingly similar to a trademark or service mark in which the complainant has

[4] *Rediff Communication Ltd. v. Cyberbooth & Anr.*, AIR 2000 Bom 27.

[5] *Info Edge (India) Pvt. Ltd. v. Shailesh Gupta*, 98 (2002) DLT 499 : (2002) ILR 1 Del 220.

[6] The Anticybersquatting Consumer Protection Act, 1999, 15 U.S.C. § 1129 (U.S.).

[7] Uniform Domain Name Dispute Resolution Policy, Rules for Uniform Domain Name Dispute Resolution Policy, r. 1 (defining "Reverse Domain Name Hijacking"); .IN Domain Name Dispute Resolution Policy, Rules of Procedure, r. 3 (as amended Sept. 2020).

[8] World Intellectual Property Organization, supra note 1, paras. 135-168.

[9] Internet Corporation for Assigned Names and Numbers, Uniform Domain Name Dispute Resolution Policy (adopted by the ICANN Board of Directors, Santiago, Chile, 25-26 Aug. 1999, effective 1 Dec. 1999).

rights; that the registrant has no rights or legitimate interests in respect of the domain name; and that the domain name has been registered and is being used in bad faith.[10] The procedure is conducted almost entirely on the papers, without discovery or oral hearing, before a single or three-member panel appointed by an ICANN-accredited dispute-resolution service provider, principal among them the WIPO Arbitration and Mediation Centre, and typically concludes within roughly sixty days of filing.[11] The available remedies are narrow but effective for their purpose: cancellation of the offending registration, or transfer of the domain name to the complainant; the UDRP does not provide for monetary damages, which has the effect of keeping the procedure inexpensive but leaves deterrence to be achieved through other means. The Policy's first ever decision, delivered in January 2000, ordered transfer of a domain name registered in apparent anticipation of a professional wrestling promotion's internet presence, and set the template for the thousands of decisions that followed.[12]

B. The United States: The Anticybersquatting Consumer Protection Act, 1999

The United States supplemented the UDRP with dedicated federal legislation. The ACPA, enacted on 29 November 1999 as an amendment to section 43 of the Lanham Act and codified at 15 U.S.C. section 1125(d), creates a civil cause of action against a person who has a bad-faith intent to profit from a mark and who registers, traffics in, or uses a domain name identical or confusingly similar to a distinctive mark, or identical, confusingly similar to, or dilutive of a famous mark.[13] Congress supplied courts with nine non-exhaustive statutory factors for assessing bad faith, ranging from the registrant's own trademark rights and prior use of the domain for a bona fide offering of goods or services, to an intent to divert consumers for commercial gain and a pattern of registering multiple domains known to be identical or confusingly similar to the marks of others.[14] Unlike the UDRP, the ACPA authorises a genuine damages remedy: a successful plaintiff may elect to recover either actual damages and the defendant's profits, or statutory damages ranging from one thousand to one hundred thousand dollars per domain name, as the court considers just, in addition to injunctive relief and forfeiture, cancellation or transfer of the domain.[15] Where the registrant cannot be found or is not subject to personal jurisdiction, the Act further permits an action in rem against the domain name itself, an innovation designed to address the practical difficulty of pursuing anonymous or foreign cybersquatters.[16] A separate provision protects any living person against bad-faith registration of a domain name consisting of that person's name for purposes of financial gain by sale to that person or a third party.[17]

Even before the ACPA came into force, American courts had begun to address cybersquatting-like conduct through existing trademark dilution law. In *Panavision International, L.P. v. Toeppen*, the Ninth Circuit Court of Appeals held that a scheme of registering the marks of well-known companies as domain names, with the object of extracting payment for their release, amounted to a commercial use in commerce

[10] Uniform Domain Name Dispute Resolution Policy, para. 4(a).

[11] WIPO Arbitration and Mediation Center, Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).

[12] *World Wrestling Fed'n Entm't, Inc. v. Bosman*, WIPO Case No. D1999-0001 (Jan. 14, 2000).

[13] The Anticybersquatting Consumer Protection Act, 1999, 15 U.S.C. § 1125(d)(1)(A)-(B) (U.S.).

[14] 15 U.S.C. § 1125(d)(1)(B)(i) (setting out nine non-exhaustive factors for assessing bad faith).

[15] 15 U.S.C. § 1117(d).

[16] 15 U.S.C. § 1125(d)(2) (in rem jurisdiction over the domain name).

[17] 15 U.S.C. § 1129.

sufficient to dilute the value of the marks, notwithstanding that the registrant never used the domains to sell any competing goods or services.[18] Later decisions have continued to construe the ACPA's bad-faith requirement expansively; in *DSPT International, Inc. v. Nahum*, the Ninth Circuit held that using a protected mark in a domain name to gain leverage in an unrelated business dispute was itself sufficient to establish bad-faith intent to profit.[19]

IV. THE INDIAN LEGAL LANDSCAPE

A. Absence of Dedicated Legislation

India has not enacted any statute specifically addressing cybersquatting. The Trade Marks Act, 1999, which came into force in September 2003, replacing the earlier Trade and Merchandise Marks Act, 1958, contains no reference whatsoever to domain names.[20] Its infringement provision and the remedial provisions governing suits for infringement and passing off, principally sections 29, 134 and 135, apply to domain name disputes only indirectly, through judicial interpretation extending their scope to conduct occurring in cyberspace.[21] Where the complainant's mark is unregistered, as was frequently the case in India's earliest domain name disputes, the only available cause of action is the common law tort of passing off, which requires proof of goodwill in the mark, a misrepresentation by the defendant likely to deceive the public into believing that the defendant's business or goods are those of, or connected with, the claimant, and resulting or probable damage to that goodwill. The entire edifice of Indian cybersquatting law has accordingly been built upon judicial extension of this pre-digital doctrine to an online context that its original architects could scarcely have anticipated.

B. Judicial Evolution

The foundational decision is *Yahoo!, Inc. v. Akash Arora & Anr.*, decided by the Delhi High Court on 19 February 1999, in which the defendant had begun offering services under the domain "yahooindia.com" in apparent imitation of the plaintiff's globally recognised "Yahoo!" mark.[22] Applying sections 27 and 29 of the then-applicable Trade and Merchandise Marks Act, 1958, and notwithstanding that the "Yahoo!" mark was not, at the relevant time, registered in India, the court held that internet users were likely to be confused into believing that the defendant's services originated from or were associated with the plaintiff, and granted an injunction restraining further use of the domain.[23] This was the first Indian judicial recognition that a domain name is entitled to protection equivalent to that afforded a trademark, and it established passing off, rather than any dedicated statute, as the operative Indian remedy against cybersquatting.

The Bombay High Court reached a similar conclusion the following year in *Rediff Communication Ltd. v. Cyberbooth & Anr.*, restraining the defendant's use of the domain "radiff.com" as deceptively similar to the plaintiff's established "rediff.com", and describing internet domain names as significant, valuable

[18] *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1325 (9th Cir. 1998).

[19] *DSPT Int'l, Inc. v. Nahum*, 624 F.3d 1213, 1218-20 (9th Cir. 2010).

[20] The Trade Marks Act, 1999 (Act 47 of 1999), brought into force w.e.f. Sept. 15, 2003, repealing the Trade and Merchandise Marks Act, 1958 (Act 43 of 1958).

[21] The Trade Marks Act, 1999, ss. 29, 134 & 135.

[22] *Yahoo!, Inc. v. Akash Arora & Anr.*, 1999 IIAD (Delhi) 229 : 78 (1999) DLT 285.

[23] *The Trade and Merchandise Marks Act, 1958, ss. 27 & 29, as applied in Yahoo!, Inc. v. Akash Arora & Anr.*, 1999 IIAD (Delhi) 229.

corporate assets meriting protection comparable to that given to trademarks.[24] The Delhi High Court subsequently applied the same reasoning on a larger scale in *Tata Sons Ltd. v. Manu Kosuri & Ors.*, restraining the registration of an entire cluster of domain names incorporating the well-known "TATA" mark, and expressly relying on both *Yahoo!* and *Rediff* for the proposition that domain names are corporate assets of considerable value, deserving of protection equivalent to registered trademarks.[25] A further refinement followed in *Info Edge (India) Pvt. Ltd. v. Shailesh Gupta*, in which the Delhi High Court protected the domain "naukri.com", a Hindi word rendered in Roman script, against the deceptively similar "naukari.com", holding that even an ostensibly generic or descriptive term could acquire secondary distinctiveness through use, sufficient to found an action in passing off once the defendant's adoption of the similar domain was shown to be motivated by dishonest intent to divert traffic.[26]

The Supreme Court of India settled the matter definitively in *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*, decided on 6 May 2004, arising from a dispute between two businesses employing variants of the coined term "Sify" in their respective domain names.[27] The Court held that a domain name is capable of possessing all the distinguishing characteristics of a trademark, that the provisions of the Trade Marks Act, 1999 and the common law of passing off accordingly apply to domain name disputes with the same force as to conventional trademark disputes, and that the use of a confusingly similar domain name may divert internet users seeking one business to the website of another, generating misrepresentation, confusion and consequent injury to goodwill sufficient to satisfy the classical elements of passing off.[28] The Court further observed that, unlike trademarks, which can validly coexist in different territorial jurisdictions or classes of goods, domain names are inherently exclusive and global in character, a feature that, in the Court's view, justified an even stricter insistence on protecting established marks online than in the physical marketplace. *Satyam Infoway* remains the leading Indian authority on domain name protection and continues to be applied in subsequent decisions of the High Courts.

C. The Information Technology Act, 2000: A Limited Penumbra

The Information Technology Act, 2000, India's principal legislation governing electronic transactions and cybercrime, does not create any cause of action specific to cybersquatting.[29] Certain of its provisions may nevertheless assume incidental relevance in extreme cases: section 66C, which penalises fraudulent or dishonest use of another person's identifying feature such as a password or unique identification feature, and section 66D, which penalises cheating by personation using a computer resource, both inserted by the Information Technology (Amendment) Act, 2008, could conceivably apply where a cybersquatted domain is deployed to impersonate an individual or entity for fraudulent purposes.[30] These provisions, however, are criminal in character, aimed at personation and identity theft rather than domain name abuse as such, and cannot substitute for a dedicated civil cybersquatting remedy. The absence of any such remedy in the

[24] *Rediff Communication Ltd. v. Cyberbooth & Anr.*, AIR 2000 Bom 27.

[25] *Tata Sons Ltd. v. Manu Kosuri & Ors.*, 90 (2001) DLT 659 : 2001 IIIAD (Delhi) 545.

[26] *Info Edge (India) Pvt. Ltd. v. Shailesh Gupta*, 98 (2002) DLT 499.

[27] *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*, (2004) 6 SCC 145 : AIR 2004 SC 3540.

[28] Id.

[29] The Information Technology Act, 2000 (Act 21 of 2000).

[30] The Information Technology Act, 2000, ss. 66C & 66D, inserted by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009).

IT Act, 2000 leaves trademark law and the law of passing off as India's sole general-purpose civil weapons against cybersquatting.

D. The .IN Domain Name Dispute Resolution Policy

For disputes concerning India's own country-code top-level domain, ".in", and its variants such as ".co.in" and ".net.in", the National Internet Exchange of India administers the .IN Domain Name Dispute Resolution Policy, introduced in 2005 and substantially amended in September 2020.[31] Modelled closely on the UDRP but administered entirely within India through a panel of NIXI-empanelled arbitrators rather than the WIPO Centre, the INDRP requires a complainant to establish, cumulatively, that the disputed domain is identical or confusingly similar to a mark or name in which the complainant has rights, that the registrant has no rights or legitimate interest in the domain, and that the domain has been registered or is being used in bad faith, a formulation clarified by the 2020 amendment to remove earlier ambiguity as to whether the three elements were cumulative or disjunctive.[32] The efficacy of the mechanism is illustrated by decisions such as *Maruti Suzuki India Ltd. v. Nitin Bhamri*, in which the arbitrator found bad-faith registration of the domain "marutisuzukieeco.co.in", holding that the addition of descriptive or generic elements to a well-known mark does not avoid a finding of confusing similarity.[33] As under the UDRP, the principal remedy available to a successful complainant under the INDRP is the transfer of the disputed domain name; the Policy makes no provision for monetary compensation.[34] The mechanism has nevertheless proved administratively efficient, with commentary noting that NIXI resolved more than eleven hundred disputes in the policy's first fifteen years, with complainants prevailing in an overwhelming majority of cases, and with pleadings conducted on paper and subject to strict word limits, offering claimants a comparatively swift and inexpensive alternative to civil litigation.[35]

V. COMPARATIVE ASSESSMENT

A comparison of the three regimes surveyed above reveals significant structural differences. The United States operates a dual-track system, permitting rights holders to proceed either under the UDRP for a swift, low-cost transfer or cancellation remedy, or under the ACPA in federal court, where a genuine damages remedy, including statutory damages of between one thousand and one hundred thousand dollars per domain name, together with in rem jurisdiction over untraceable foreign registrants, is available at the cost of a lengthier and more expensive proceeding. India, by contrast, offers only a single formal administrative track, the INDRP, and that track is confined to the ".in" country-code domain; disputes over domains registered under generic top-level domains such as ".com" must instead be pursued either through the UDRP itself, insofar as the complainant can invoke WIPO's jurisdiction, or through ordinary civil litigation grounded in the Trade Marks Act, 1999 and the common law of passing off.

India's reliance on judicially developed passing-off doctrine, beginning with *Yahoo!* in 1999 and consolidated by the Supreme Court in *Satyam Infoway* in 2004, has demonstrated considerable adaptability

[31].IN Domain Name Dispute Resolution Policy, National Internet Exchange of India (introduced 2005, as amended Sept. 2020).

[32].IN Domain Name Dispute Resolution Policy, para. 4, as amended in September 2020 to clarify that cls. (a)-(c) must be read cumulatively.

[33]Maruti Suzuki India Ltd. v. Nitin Bhamri, INDRP Case No. 136.

[34].IN Domain Name Dispute Resolution Policy, para. 10 (remedies).

[35]"15 Years On: A Relook at the INDRP Policy", Lexology (July 2, 2020).

and has kept Indian law reasonably abreast of international developments without the need for a dedicated statute. That adaptability, however, comes at a cost. Because relief under passing off is contingent on proof of established goodwill, a likelihood of deception, and resulting or probable damage, newer trademark holders, individual professionals and public figures without a pre-existing commercial reputation may find it considerably harder to obtain relief than a rights holder proceeding under the ACPA's more precisely codified bad-faith test, or under the ACPA's separate personal-name provision, for which Indian law has no direct counterpart. Further, whereas the ACPA couples injunctive relief with a meaningful damages remedy calculated to deter repeat and serial cybersquatters, both the INDRP and Indian civil litigation for passing off are, in practice, oriented overwhelmingly towards transfer of the offending domain and injunctive relief, with damages rarely quantified or awarded in a manner proportionate to the commercial harm caused by systematic cybersquatting.

VI. EMERGING CHALLENGES

Several developments complicate the continued adequacy of the existing legal architecture. The considerable expansion in the number of generic top-level domains available for registration since ICANN's New gTLD Program began accepting applications in 2012 has multiplied the number of domain strings in which a given trademark can potentially be cybersquatted, correspondingly increasing the monitoring and enforcement burden placed on rights holders. The growing sophistication and resourcing of large corporate trademark portfolios has also generated a converse concern, namely reverse domain name hijacking, in which well-resourced complainants pursue UDRP or INDRP proceedings against registrants who in fact possess a legitimate interest in a domain, relying on the asymmetry of resources between a corporate complainant and an individual respondent to extract a transfer that the merits do not support.

Privacy-protective WHOIS practices, increasingly widespread following global data-protection reforms, have made it considerably more difficult for rights holders to identify the true registrant behind a cybersquatted domain, complicating both the gathering of evidence necessary to establish bad faith and, in ACPA-style regimes, the service of process necessary to found personal jurisdiction. Relatedly, the emergence of blockchain-based and decentralised naming systems operating entirely outside the traditional Domain Name System presents a more fundamental challenge, since such systems fall outside the contractual reach of the UDRP, the INDRP and, arguably, the ACPA itself, all of which were designed around a centralised registrar-registry architecture that decentralised naming protocols are specifically engineered to avoid. For India in particular, the absence of any codified statutory definition of cybersquatting means that novel fact patterns, such as disputes between two concurrent legitimate users of similar marks in different classes of goods, or disputes over inherently generic or descriptive domain names that have not yet acquired secondary meaning, must continue to be resolved through incremental judicial extension of a doctrine developed for an entirely different, physical-marketplace context, with the attendant risk of inconsistent outcomes across different High Courts.

VII. RECOMMENDATIONS

Drawing on the foregoing analysis, several reforms merit consideration. First, Parliament could usefully amend the Trade Marks Act, 1999, or enact a free-standing provision, expressly recognising domain names as protectable subject matter and codifying the elements of cybersquatting along the lines of the UDRP's three-element test or the ACPA's bad-faith formulation, thereby reducing continued dependence on the

sometimes uneven and fact-intensive common law of passing off. Second, a calibrated statutory damages mechanism, proportionate to Indian economic conditions, would strengthen deterrence considerably beyond the transfer-only remedy presently available under the INDRP, particularly against serial or repeat cybersquatters who register multiple domains as part of an organised scheme. Third, explicit statutory protection against the bad-faith commercial registration of personal names, comparable to the ACPA's separate provision, would benefit the growing population of individual professionals, artists and public figures who maintain a significant commercial online identity but may lack the established institutional goodwill traditionally required to succeed in a passing-off action. Fourth, clearer procedural coordination between INDRP proceedings and civil litigation, including express clarification of the preclusive or non-preclusive effect of an INDRP award on a subsequent civil suit, would reduce the risk of duplicative or inconsistent outcomes. Finally, continued vigilance against reverse domain name hijacking, whether through cost-shifting sanctions against abusive complainants or through robust panel scrutiny of complainant good faith, remains essential to ensure that reform directed at strengthening rights holders' remedies does not, in turn, prejudice registrants who hold a genuine and legitimate interest in their domain names.

VIII. CONCLUSION

Cybersquatting sits squarely at the intersection of trademark law and internet governance, and continues to test the capacity of legal frameworks conceived for a physical marketplace to adapt to a borderless digital environment. The international community's response, through the WIPO-inspired UDRP and the United States' ACPA, has combined a fast, contractually grounded administrative remedy with, in the American case, a more robust statutory cause of action carrying meaningful damages. India has travelled a different path, relying almost entirely on judicial extension of the common law of passing off, beginning with the Delhi High Court's pioneering decision in *Yahoo!, Inc. v. Akash Arora* and culminating in the Supreme Court's authoritative pronouncement in *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*, supplemented domestically by the reasonably efficient, if remedially narrow, INDRP mechanism administered by NIXI. That judicial and administrative architecture has served India tolerably well for a quarter of a century, but the persisting absence of a codified statutory definition, a meaningful damages regime, and explicit personal-name protection, together with the fresh challenges posed by an expanding universe of generic top-level domains and the prospect of naming systems operating entirely outside the traditional Domain Name System, suggest that the time may have come for calibrated legislative intervention to complement, rather than continue to be substituted by, judicial ingenuity.

TABLE OF CASES

DSPT Int'l, Inc. v. Nahum, 624 F.3d 1213 (9th Cir. 2010)
Info Edge (India) Pvt. Ltd. v. Shailesh Gupta, 98 (2002) DLT 499
Maruti Suzuki India Ltd. v. Nitin Bhamri, INDRP Case No. 136
Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998)
Rediff Communication Ltd. v. Cyberbooth & Anr., AIR 2000 Bom 27
Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd., (2004) 6 SCC 145
Tata Sons Ltd. v. Manu Kosuri & Ors., 90 (2001) DLT 659
World Wrestling Fed'n Entm't, Inc. v. Bosman, WIPO Case No. D1999-0001
Yahoo!, Inc. v. Akash Arora & Anr., 1999 IIAD (Delhi) 229

REFERENCES:

1. The Trade Marks Act, 1999 (Act 47 of 1999).
2. The Trade and Merchandise Marks Act, 1958 (Act 43 of 1958).
3. The Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
4. The Anticybersquatting Consumer Protection Act, 1999, 15 U.S.C. § 1125(d) (U.S.).
5. Uniform Domain Name Dispute Resolution Policy and Rules, Internet Corporation for Assigned Names and Numbers (1999).
6. .IN Domain Name Dispute Resolution Policy, National Internet Exchange of India (2005, as amended 2020).
7. World Intellectual Property Organization, The Management of Internet Names and Addresses: Intellectual Property Issues, Final Report of the WIPO Internet Domain Name Process (Apr. 30, 1999).