Bridging the Gap: Telecom Spam Regulation and Trademark Protection in the Era of Caller-ID and SMS Spoofing in India

Joyaani Thapa[1]

ABSTRACT

Millions of Indian mobile users receive calls and texts every day that seem to be from government agencies, banks, or e-commerce sites, but are actually the product of fraudsters who have "spoofed," or fabricated, the sender's identity. In addition to deceiving specific customers, this dishonesty subtly damages the reputation of the company whose name was appropriated without permission. The Trade Marks Act of 1999, which governs trademark law, and the Telecom Regulatory Authority of India (TRAI), which regulates telecom spam, are two legal systems that seldom interact.

This study explores an understudied junction between these two legal systems. In addition to asking whether TRAI's steadily growing anti-spam architecture, which is based on the Principal Entity-Telemarketer (PE-TM) traceability chain, the Distributed Ledger Technology (DLT) platform, and the 2025 header-suffix rule, offers brand owners any practical path to relief, it also asks whether the unauthorized use of a registered or well-known mark in a spoof caller ID or SMS header amounts to actionable trademark dilution.

The study concludes that although the Trade Marks Act's Section 29(4) is theoretically capable of covering reputation-based harm brought on by impersonation, it has never been tested against telecom spoofing, and TRAI's regulations are completely silent on trademark rights despite significant enforcement activity. The study suggests a coordination mechanism that would allow brand owners to register their marks with TRAI's current detection systems, enabling quicker, more focused action against impersonators. It draws a brief comparison with the United States' twin-track model under the Lanham Act and the Truth in Caller ID Act.

KEYWORDS

Trademark Dilution, Caller ID Spoofing, Telecom Regulatory Authority of India, Trade Marks Act 1999, Brand Protection, Consumer Fraud, and TCCCPR.

[1] Student, CHRIST (Deemed to be University), Bengaluru.

INTRODUCTION

Whether it's a call confirming a delivery or an SMS alerting them to a bank transaction, telecommunication has emerged as the main way Indian consumers engage with the companies they trust.[2] However, fraudsters now choose to use this same channel. Nowadays, thieves frequently alter their calls and texts to appear like a reputable bank, telecom provider, or online retailer. This technique, known as "spoofing."[3] The victim who answers such a call or opens such a message is tricked not because the fraudster has replicated a product, but rather because the fraudster has stolen a name, taking advantage of decades of goodwill that the legitimate brand invested years of time and money to cultivate. The victim who answers such a call or opens such a message is tricked not because the fraudster has replicated a product, but rather because the fraudster has stolen a name, taking advantage of decades of goodwill that the legitimate brand invested years of time and money to cultivate.

This issue is impacted by two distinct legal systems, neither of which was created with the other in mind. The Trade Marks Act of 1999 codifies trademark law, which shields registered and well-known marks from unauthorized usage that could confuse consumers or lessen their unique qualities.[4] The Telecom Regulatory Authority of India Act, 1997 gave TRAI the authority to administer telecom law. In recent years, TRAI has developed a complex system to prevent fraudulent messaging and unsolicited commercial communications (UCC), most prominently through the Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR).[5] These two regimes have developed in different ways. Telecom regulation speaks the language of sender-ID registration, traceability chains, and blacklisting while trademark law speaks the language of confusion, dilution, and passing off. When a fake SMS spoofs a brand's name, the brand is unable to invoke either with ease.

This study looks into that gap. It poses three related queries. First, since the impersonator is not "selling" anything bearing the mark in the traditional sense, could the unauthorized use of a company's name in a spoof caller ID or SMS header constitute trademark infringement or dilution under Indian law? Second, despite its vigorous enforcement, does TRAI's regulatory

[2] Telecom Regulatory Authority of India, Press Release No. 104/2026, Highlights of Telecom Subscription Data at the End of June 2026 (July 28, 2026), https://www.trai.gov.in/sites/default/files/2026-07/PR_No104of2026_0.pdf.
[3] *Caller ID Spoofing*, Fed. Commc'ns Comm'n, https://www.fcc.gov/spoofing (last visited Oct. 26, 2026).
[4] The Trade Marks Act, 1999, No. 47, Acts of Parliament, 1999 (India).
[5] The Telecom Regulatory Authority of India Act, 1997, No. 24, Acts of Parliament, 1997 (India); Telecom Commercial Communications Customer Preference Regulations, 2018 (India).

structure provide trademark owners with any significant path to relief, or does it function as a stand-alone system that only protects the message's recipient rather than the owner of the borrowed name? Third, what workable method may bridge the gap between the two regimes without necessitating the complete reconstruction of either regime?

The article makes the case that Section 29(4) of the Trade Marks Act, which protects well-known marks even outside of their registered class of goods or services, is conceptually well-suited to spoofing cases because it only requires evidence of harm to the mark's distinctive character or reputation rather than proof of confusion about the source of goods.[6] However, there is no established precedence for brand owners to rely on because this clause has never been judicially proven against telecom imitation. In the meantime, a brand owner who wants to report name spoofing has no official, accelerated method separate from the standard consumer complaint process because TRAI's regulations are completely silent on trademark rights, despite blocking millions of bogus numbers. In order to close this gap, the report concludes by suggesting a coordination mechanism that is based on a brief comparison with the United States.

METHODOLOGY

The interaction between trademark law and telecom regulation in India is examined in this research using a doctrinal and comparative approach. The main focus is a close reading of Section 29 of the Trade Marks Act, 1999, specifically the dilution clause in Section 29(4), read in conjunction with the general framework of infringement and passing off established by Indian courts in cases like *Cadila Health Care Ltd. v. Cadila Pharmaceuticals Ltd*.[7] The paper treats *Yahoo!, Inc. v. Akash Arora & Anr.* and *Tata Sons Ltd. v. Manu Kosuri & Ors.,* two significant rulings on domain-name misuse, as precedent for the idea that Indian courts have previously stretched trademark doctrine to cover new digital fact patterns without waiting for legislative amendment.[8]

In addition to this doctrinal reading, the paper conducts a regulatory review of TRAI's anti-spam architecture using the Telecom Commercial Communications Customer Preference Regulations, 2018, its 2025 amendment, and TRAI's public guidelines regarding the SMS

[6] The Trade Marks Act, 1999, § 29(4), *supra* note 4.
[7] Cadila Health Care Ltd. v. Cadila Pharmaceuticals Ltd., (2001) 5 S.C.C. 73 (India).
[8] Yahoo!, Inc. v. Akash Arora, (1999) 19 PTC 201 (Del.) (India); Tata Sons Ltd. v. Manu Kosuri, 2001 PTC 432 (Del.) (India).

header-suffix rule and the Principal Entity-Telemarketer traceability chain.[9] When available, official TRAI press releases and gazette notifications are used. In cases where the underlying regulatory text could not be directly retrieved, the paper relies on secondary reporting from specialized telecom-compliance sources, which is cross-checked for consistency across several independent publications.

In order to determine whether jurisdictions that have already combined brand protection with telecom-fraud regulation offer a viable model for India, the paper concludes with a brief comparative analysis of the United States' parallel framework of the Lanham Act's dilution provision and the Truth in Caller ID Act.[10] Given the stark contrasts between the regulatory frameworks in India and the United States, the comparative material is utilized illustratively rather than as a push for widespread transplantation.

RESEARCH OBJECTIVE

The central objective of this paper is to determine whether Indian trademark law, as it presently stands, is capable of addressing the reputational harm caused when a brand's name is impersonated through caller-ID or SMS spoofing, and whether the telecom regulatory framework built to curb such spoofing offers brand owners any usable point of entry. The paper does not seek to argue that spoofing is presently unregulated; TRAI's enforcement record demonstrates the contrary. Instead, it seeks to demonstrate that spoofing is regulated only from the perspective of the recipient-consumer, and that the brand owner whose name is misappropriated remains, for practical purposes, outside the existing enforcement architecture.

This question is important because, up until now, Indian trademark research has mostly focused on cybersquatting and domain-name disputes or confusion-based infringement in the marketplace for products and services.[11] Very little attention has been paid to the telecom layer, even though spoofed calls and texts now constitute one of the most common forms of brand impersonation encountered by ordinary Indian consumers. By situating trademark dilution doctrine alongside TRAI's technical anti-spam machinery, this paper aims to identify a concrete, actionable gap in enforcement, and to propose a coordination mechanism that connects the two regimes without requiring fresh primary legislation.

[9] Telecom Commercial Communications Customer Preference Regulations, 2018 (India), *supra* note 5.
[10] 15 U.S.C. § 1125(c) (2018); 47 U.S.C. § 227(e) (2018).
[11] Yahoo!, Inc., (1999) 19 PTC 201; Tata Sons Ltd., 2001 PTC 432, *supra* note 8.

ANALYSIS

The Doctrinal Conundrum: Does Brand Name Spoofing Qualify as "Use" Under Section 29?

Infringement is defined as the unlawful use of a mark that is identical to or confusingly similar to a registered mark in connection with goods or services in the course of commerce (Section 29 of the Trade Marks Act, 1999).[12] The classic infringement analysis, which was developed in *Cadila Health Care Ltd. v. Cadila Pharmaceuticals Ltd.,* considers factors like phonetic similarity, the nature of the goods, and the class of purchaser to determine whether the rival mark is likely to cause confusion among consumers as to the source of goods.[13] When two rival pharmaceutical companies market medications with identical names, this structure easily fits the situation. It fits far less securely onto a fraudster who is only using the borrowed name to make a phone call or send a text message appear authentic and is not actually offering any goods or services under that name.

The paper's first doctrinal conundrum is this one. There is no product, no storefront, and frequently no continuing business contact with the victim beyond the one fraudulent encounter, therefore a spoofer does not provide products or services "in the course of trade" as the Act seems to envision.[14]

However, the damage to the brand owner is real: each successful fraud that shows "SBI" or "Amazon" on a victim's screen erodes the confidence that the legitimate business has spent years cultivating, and each unsuccessful hoax still makes the recipient more wary of sincere communications from that brand. Therefore, the question is whether courts would interpret "use in the course of trade" broadly enough to include this type of parasitic, non-commercial impersonation, or if spoofing would be completely exempt from Section 29's ordinary infringement provisions if no goods or services were being offered under the mark. The study argues that the more promising solution is found elsewhere in the same section and that regular infringement law, which is based on consumer misunderstanding between competing commercial products, is not the natural home for this issue.

[12] The Trade Marks Act, 1999, § 29(1), *supra* note 4.
[13] Cadila Health Care Ltd., (2001) 5 S.C.C. 73, *supra* note 7.
[14] The Trade Marks Act, 1999, § 29(6), *supra* note 4.

Dilution Without Confusion: The Well-Known Marks Route and Section 29(4)

The Trade Marks Act's Section 29(4) provides an alternative and more appropriate doctrinal basis. It states that if a registered mark is well-known in India,[15] its use by someone else in connection with any goods or services, even ones that are completely different from those for which the mark is registered, constitutes infringement if the use, without justification, unfairly exploits or damages the mark's reputation or distinctive character.[16] Importantly, this clause does not call for evidence that customers were perplexed about the origin of the products. Just evidence of damage to the mark's uniqueness or reputation is needed.[17] Because of this structural characteristic, Section 29(4) is conceptually well-matched to spoofing: the scammer's use of "HDFC Bank" or "Flipkart" as a sender ID is clearly capable of harming the goodwill associated with that name, which is exactly the kind of harm Section 29(4) was intended to prevent.

The problem is that, to the best of the paper's knowledge, no published Indian decision has ever tested this clause against telecom impersonation. In contrast to situations involving criminal impersonation with no underlying business offering at all,[18] Section 29(4) has typically been utilized in disputes between two commercial entities, one of which is using the fame of the other's mark to sell unrelated items.[19] This leaves an open doctrinal question: would a court treat a scammer's use of a spoofed sender ID as "use... in relation to goods or services" for the purposes of Section 29(4), given that the scammer is not really dealing in goods or services but is using the name purely as camouflage for fraud? The paper argues that a purposive reading of Section 29(4), consistent with its underlying rationale of protecting reputation rather than merely policing competitive confusion, should extend to this scenario. But until a court says so, brand owners are left relying on an untested legal theory rather than settled precedent.

How Indian Courts Have Previously Extended Trademark Law

It is instructive to remember how Indian courts handled a similar doctrinal stretch in the past. As business went online in the late 1990s and early 2000s, courts had to deal with

[15] The Trade Marks Act, 1999, § 2(1)(zg), *supra* note 4.
[16] The Trade Marks Act, 1999, § 29(4), *supra* note 4.
[17] See ITC Ltd. v. Philip Morris Products SA, (2010) 42 PTC 572 (Del.) (India); The Trade Marks Act, 1999, § 29(4)(a)-(c), *supra* note 4.
[18] The Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India); The Bharatiya Nyaya Sanhita, 2023, § 319, No. 45, Acts of Parliament, 2023 (India).
[19] ITC Ltd., (2010) 42 PTC 572, *supra* note 17.

cybersquatters registering domain names that included well-known marks even though they didn't provide any directly competing goods in the conventional sense. The Delhi High Court prohibited the defendant in *Yahoo!, Inc. v. Akash Arora & Anr.* from using the domain name "yahooindia.com," ruling that a domain name should have the same level of protection as a trademark and that the defendant's use was likely to mislead internet users into thinking the plaintiff was associated with the defendant.[20] Without waiting for a domain-name-specific regulation, the court arrived at its decision using the standard passing-off framework.[21]

A similar strategy was used in *Tata Sons Ltd. v. Manu Kosuri & Ors.,* where the Delhi High Court prevented the defendant from registering a number of domain names that included the well-known "TATA" mark. The court held that domain names serve as more than just internet addresses and should be protected similarly to trademarks, clearly defining the harm in terms of both passing off and dilution.[22] Both rulings show that Indian courts have previously been open to interpreting current trademark law in a way that allows them to reach a new technological fact pattern, which is cybersquatting, that lawmakers did not foresee when the statute was drafted.[23] This essay makes the case that caller-ID and SMS spoofing are structurally comparable issues. There is a reasonable doctrinal path by which courts could extend Section 29(4) to telecom spoofing without further legislative intervention, provided a suitable case is brought, just as the courts in Yahoo! and Tata Sons did not require Parliament to amend the Trade Marks Act before extending its protection to domain names.

LAW JURIST LEGAL JOURNAL

The Anti-Spam Architecture of TRAI: A Parallel Universe That Never Discusses Trademarks

While TRAI's telecom regulation has been practically highly active but conceptually silent on trademark rights, trademark law has been theoretically competent but practically untested. In accordance with the Telecom Commercial Communications Customer Preference Regulations, 2018, TRAI required all bulk SMS senders to register a legitimate Sender ID on the Distributed Ledger Technology (DLT) platform. This required them to separate transactional messages from promotional ones and to remove Do-Not-Disturb registered numbers from marketing campaigns.[24] Telecom service providers were prohibited from sending messages containing

[20] Yahoo!, Inc., (1999) 19 PTC 201, *supra* note 8.
[21] The Trade Marks Act, 1999, § 27(2), *supra* note 4.
[22] Tata Sons Ltd., 2001 PTC 432, *supra* note 8.
[23] See Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd., (2004) 6 S.C.C. 145 (India).
[24] Telecom Commercial Communications Customer Preference Regulations, 2018 (India), *supra* note 5.

unapproved URLs, APKs, or callback numbers starting in September 2024.[25] In December 2024, TRAI implemented the Principal Entity-Telemarketer (PE-TM) traceability chain, which requires them to trace the origin of every commercial message and reject any message where that chain is undefined or mismatched.[26] In order to make it easier for recipients to determine the type of message they are receiving, an additional amendment that went into effect in May 2025 mandated that every SMS sender ID include a suffix: "-T" for transactional, "-S" for service, "-P" for promotional, and "-G" for government messages.[27]

This architecture has a significant enforcement record. Over 800 companies were blacklisted and 1.8 million mobile numbers were disconnected in a matter of months after TRAI ordered operators to terminate and blacklist unregistered promotional senders in August 2024.[28] Due in great part to public complaints sent through TRAI's own reporting methods, the cumulative amount had increased by November 2025, with TRAI reporting action against over twenty-one lakh bogus numbers and about one lakh businesses over the previous year.[29] One noteworthy feature of all these enforcement actions and regulatory tools is the total lack of any mention of "trademark," "brand," or "Section 29."

The protection of the message recipient from unwanted or fraudulent communication is TRAI's stated goal throughout, not the protection of the organization whose name has been used fraudulently. Since banning a spoof "SBI" message protects both the deceived consumer and SBI's reputation, the two goals often overlap in reality. However, the regulation design never regards the brand owner as a rights-holder with standing to activate the system directly. To put it succinctly, there is no official way for a business to say, "This is my registered trademark, and someone is using it to defraud my customers," and have TRAI's current detection and blacklisting mechanism take action.

[25] Telecom Regulatory Authority of India, Press Release No. 80/2024, *TRAI's Continued Efforts to Combat Spam Calls and SMS Abuse* (2024), https://trai.gov.in/sites/default/files/PR_No.80of2024.pdf (describing the Direction of Aug. 20, 2024).
[26] Telecom Regulatory Authority of India, Direction No. D-27/1/(2)/2024-QoS (E-13563) (Oct. 28, 2024), https://trai.gov.in/sites/default/files/Direction_28102024.pdf.
[27] Telecom Commercial Communications Customer Preference Regulations, 2018 (India), *supra* note 5.
[28] *TRAI Blacklists Over 800 Entities, Disconnects 1.8 Million Mobile Numbers to Curb Spam Calls & SMS Fraud*, News on Air (Oct. 28, 2024), https://www.newsonair.gov.in/trai-blacklists-over-800-entities-disconnects-1-8-million-mobile-numbers-to-curb-spam-calls-sms-fraud.
[29] *TRAI Blocks 21 Lakh Fraudulent Numbers, Urges Users to Report Spam*, News on Air (Nov. 24, 2025), https://newsonair.gov.in/trai-blocks-21-lakh-fraudulent-numbers-urges-users-to-report-spam/.

The Enforcement Vacuum: Why Neither Can Regime Alone Catch the Spoofer

TRAI's own data recognizes the limitations of enforcement, even in areas where it has been most active. Despite years of regulatory tightening, spam still spreads through so-called "grey routes," unregistered senders, and incorrectly provisioned SIM connections that completely avoid the DLT framework; in 2023 alone, TRAI recorded over 1.2 million complaints against unregistered telemarketers.[30] This persistence highlights a systemic issue that cannot be resolved by trademark remedies alone. Criminal penalties under Sections 103 to 105, as well as civil remedies under the Trade Marks Act, injunctions, damages, and account of profits,[31] all require an identifiable defendant who may be served, sued, or prosecuted.[32] In contrast, spoofers are often anonymous, use offshore infrastructure or throwaway numbers, and disappear before any civil lawsuit could actually be brought and decided. An individual brand owner pursuing a civil trademark claim without access to telecom traceability data faces an even greater practical obstacle if TRAI's own specialized detection technologies and cross-operator blacklisting are unable to keep up with grey-route senders.

This is the core of the enforcement gap identified in this paper. The extent of TRAI's blocking operations makes it evident that neither regime is helpless. It is that the strengths of the two regimes do not now come together. Although TRAI has the cross-operator blacklist, honeypot numbers, traceability chain, and technical infrastructure, it does not incorporate the legal notion of trademark harm into its decision-making process. Although Section 29(4) of trademark law embodies the legal idea of reputational loss, it lacks the technical infrastructure necessary to identify or track down an anonymous spoofer. Instead of being able to leverage the qualities of both tools at once, a brand owner now has to pick between two imperfect tools.

A Comparative Look at the Twin-Track Model in the United States

A quick examination of the US is helpful, not as a model for direct transplantation but as proof that a coordinated model is feasible. In contrast to their Indian equivalents, American federal law tackles this issue along two parallel statutory tracks that are noticeably closer together. Similar to India's Section 29(4), the Lanham Act's dilution provision,[33] found at 15 U.S.C. § 1125(c), permits the owner of a well-known mark to obtain an injunction against dilution by

[30] *SMS Regulations in India: Comprehensive Guide to Promotional and Transactional Messaging: Complete TRAI & DLT Compliance Guide*, Talk-Q (Aug. 28, 2025), https://talk-q.com/sms-messaging-regulation-in-india.
[31] The Trade Marks Act, 1999, § 135, *supra* note 4.
[32] The Trade Marks Act, 1999, §§ 103-105, *supra* note 4.
[33] Trademark Dilution Revision Act of 2006, Pub. L. No. 109-312, 120 Stat. 1730 (amending 15 U.S.C. § 1125(c)).

blurring or tarnishment, regardless of the existence or absence of actual confusion, competition, or economic injury.[34] Separately, it is illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain something of value under the Truth in Caller ID Act,[35] which is codified at 47 U.S.C. § 227(e) and later expanded by the RAY BAUM'S Act to cover text messages and calls originating from outside the United States.[36]

It is instructive that American regulators have at least conceptually recognized caller-ID spoofing as a fraud-and-harm issue sitting alongside, rather than apart from, brand-protection law and have developed technical countermeasures like the STIR/SHAKEN call-authentication framework[37] with fraud and impersonation squarely in mind. This is true even though these two statutes are administered by different agencies, the Federal Communications Commission for the Truth in Caller ID Act and the Federal Trade Commission and courts for the Lanham Act.[38] Through DLT and the PE-TM chain, India's TRAI has constructed similarly advanced technical infrastructure, but it lacks the conceptual connection to brand damage that even the loosely coordinated American model implicitly bears. According to this comparison, the connection between trademark-based reputational injury and India's telecom detection infrastructure is not conceptually original; rather, it is more in line with a connection that other jurisdictions have previously started to make, albeit poorly.

Overcoming Disparities: A Suggested Coordination System

Building on the preceding analysis, this paper proposes a modest, practically achievable coordination mechanism rather than a wholesale legislative overhaul. First, TRAI's existing DLT Building on the previous research, instead of a complete legislative change, this report suggests a small, workable coordinating mechanism. First, well-known and registered trademark owners could register their marks defensively using TRAI's current DLT platform, which is currently used to register the identities of entities that send bulk communications. This would create a reference list against which incoming sender IDs and message content could be automatically screened for close or identical matches. Second, a fast-track complaint channel could be established specifically for verified trademark owners, separate from the regular

[34] 15 U.S.C. § 1125(c), *supra* note 10.
[35] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, 124 Stat. 3572 (2010) (codified at 47 U.S.C. § 227(e)).
[36] 47 U.S.C. § 227(e) (2018); RAY BAUM'S Act of 2018, Pub. L. No. 115-141, div. P, § 503, 132 Stat. 348, 1091 (2018).
[37] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, Pub. L. No. 116-105, § 4, 133 Stat. 3274 (2019).
[38] Rules and Regulations Implementing the Truth in Caller ID Act of 2009, 76 Fed. Reg. 43,195 (July 20, 2011).

consumer UCC complaint route. This would enable a business to report suspected impersonation of its registered mark and have that report sent straight into TRAI's honeypot-and-blacklist detection pipeline instead of the general consumer grievance queue. Third and most crucially, in order for this cooperation to function as an enforceable right rather than a regulator's optional courtesy, it would require a clear regulatory or statutory anchor. This could be either an amendment to the TCCCPR that explicitly recognizes trademark impersonation as an aggravated category of UCC that warrants expedited blacklisting, or a clarificatory reading of Section 29(4) confirming its application to non-commercial telecom impersonation. The technical detection capability of TRAI and the notion of reputational harm in trademark law would just need to be directed toward the same goal in order for such a mechanism to function; neither regime would need to give up its current design.

Findings

The analysis presented in this paper leads to three related conclusions. First, because Section 29(4) of the Trade Marks Act, 1999 asks only whether the unauthorized use damages the mark's distinctive character or reputation rather than requiring consumer confusion about the source of competing goods, it is doctrinally capable of addressing the reputational harm caused by caller-ID and SMS spoofing of well-known marks.[39] In contrast to the similar cybersquatting issue, which courts addressed in rulings like *Yahoo!, Inc. v. Akash Arora* and *Tata Sons Ltd. v. Manu Kosuri* by extending the standard passing-off and infringement doctrine without requiring Parliament to enact a domain-name-specific remedy, this capability has not yet been tested in Indian courts.[40]

Second, as demonstrated by the disconnection of millions of numbers and the blacklisting of hundreds of entities, TRAI's telecom regulatory framework, which includes the TCCCPR, the DLT sender-ID registration system, the PE-TM traceability chain, and the 2025 header-suffix rule, has developed significant technical capacity to detect and block fraudulent communications. However, this framework lacks a legal mechanism that would allow a trademark owner to use its detection or blacklisting power in relation to its own brand rights. Instead, it is theoretically focused solely on safeguarding the message recipient.

Third, this mismatch creates an enforcement gap since telecom regulation lacks the legal vocabulary of dilution and reputational harm that would allow it to treat brand impersonation

[39] The Trade Marks Act, 1999, § 29(4), *supra* note 4.
[40] Yahoo!, Inc., (1999) 19 PTC 201; Tata Sons Ltd., 2001 PTC 432, *supra* note 8.

as a separate, aggravated category of violation, while trademark law lacks the technical infrastructure to track anonymous, frequently offshore spoofers. A comparison of the Truth in Caller ID Act and the Lanham Act dilution clause in the United States indicates that India does not need to abandon any of its current regimes in order to achieve a coordinated, though not necessarily unified, strategy.

CONCLUSION

The goal of this study was to investigate a legal nexus where trademark protection and telecom spam regulation meet, which has not yet gotten any consistent attention in Indian academia. Although Section 29(4) of the Trade Marks Act, 1999 has never been judicially applied to this specific fact pattern, it has argued that the unauthorized use of a well-known brand's name in a spoof caller ID or SMS is not only a consumer-protection issue for TRAI to handle alone but also a trademark dilution issue that falls squarely within its purview.

The study has proposed that a comparable doctrinal extension to telecom spoofing is both principled and feasible, based on the precedent set by Indian courts in cybersquatting cases, where trademark doctrine was extended to a new technical setting without waiting for legislative modification. However, the paper has demonstrated that TRAI's extensive technical and regulatory apparatus, while effective on a large scale, functions completely without reference to trademark rights, depriving brand owners of a direct and expedited channel into a detection and enforcement system that is essentially already designed to apprehend the very actors who abuse their names.

A workable, incremental solution to close this gap without requiring the reconstruction of either regime is provided by the proposed coordination mechanism, which includes a defensive trademark registry layered onto the current DLT platform, a fast-track complaint channel for verified brand owners, and a clear regulatory anchor recognizing impersonation as an aggravated category of violation.

Future studies could be helpful in determining whether India's more recent Telecommunications Act, 2023[41] provides additional statutory hooks for such coordination. They could also monitor whether courts are willing to apply Section 29(4) to this situation in the same way that their predecessors applied trademark doctrine to the internet a generation

[41] The Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India).

ago, should a suitable dispute arise. Until then, the company whose name is stolen each time a bogus call goes through is trapped between two regimes that were never designed to communicate with one another.

LAW JURIST
LEGAL JOURNAL