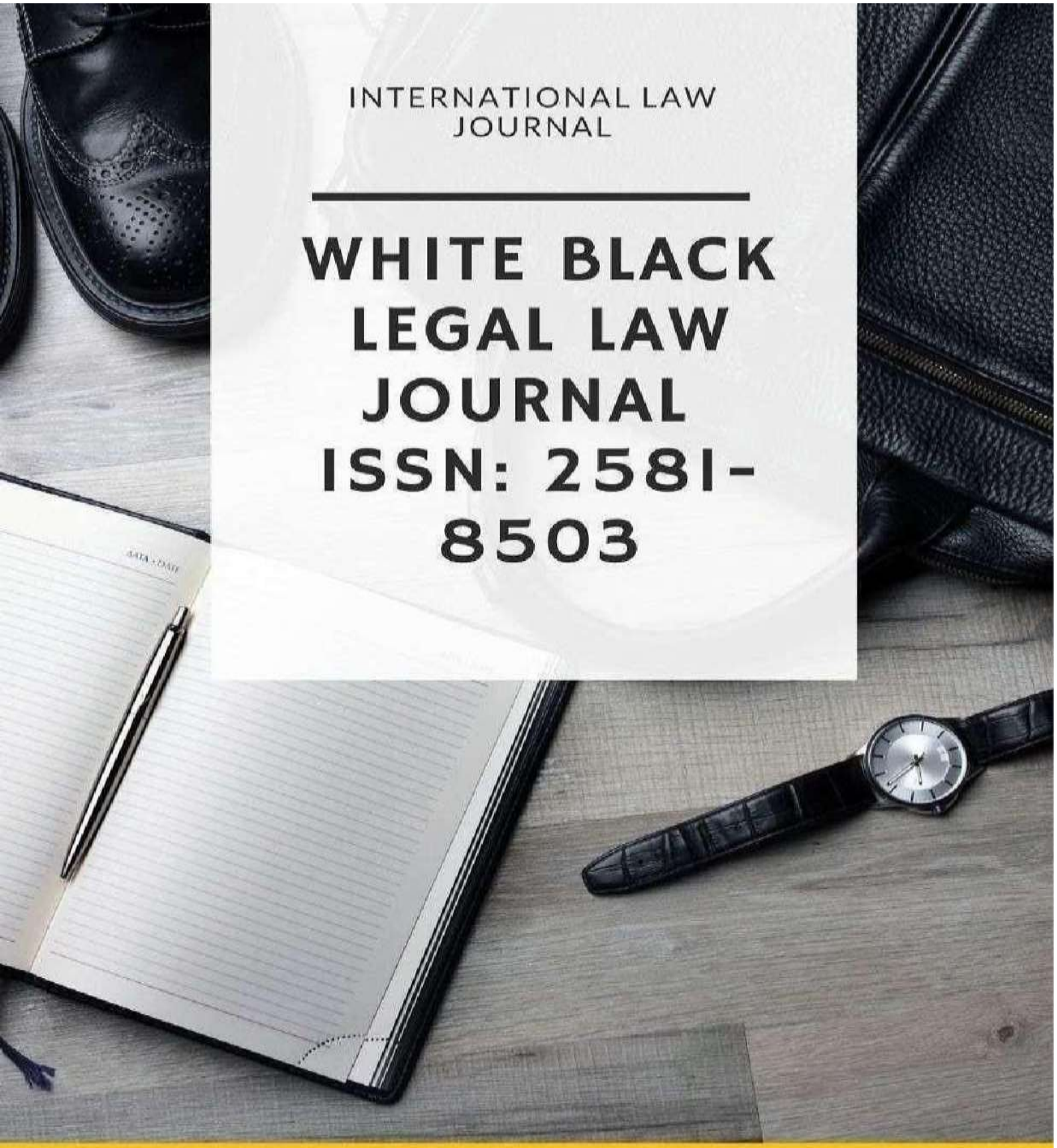

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

JURISDICTION SHOPPING IN CYBERSPACE: ABUSE OF FORUM CONVENIENCE[1]

AUTHORED BY - AYUSHI VAID

ABSTRACT

The internet has no boundaries. Law does. This dislocation forms a structural vacuum in which jurisdiction shopping occurs where litigants select legal arenas due to favourable laws as opposed to any actual association with the dispute.

This paper discusses how conventional jurisdictional concepts, which are based on the physical presence and territory, do not work well in cyberspace. It follows the history of judicial reactions in the United States, the United Kingdom, European Union, and India, especially in relation to the targeting standard that was adopted by India in Banyan Tree Holding v Murali Krishna Reddy and how this standard has evolved since then.

The article finds the most practical evils of unrestrained jurisdiction shopping, such as incompatible verdicts, litigation expenditure as a weapon and legal unpredictability that terrorizes speech and business. It ends with six reform proposals that would enhance the jurisdictional system of India and to enhance international coordination.

Keywords: *Cyberspace, Jurisdiction Shopping, Cross-border Disputes, DPDPA 2023, Banyan Tree Standard, IT Act 2000.*

I. INTRODUCTION

The internet has changed the way we live, work and coexist with one another. Imagine that you are sitting in your room in Delhi, browsing social media and suddenly being dragged to a California court about a comment that you posted online. This had ceased to be a far-fetched future and become the reality of cyberspace today. When a legal conflict is created as a result of such action the very first question that courts and lawyers are to address is not necessarily regarding the right and wrong but rather about which country's court has the right to hear the case at all. The internet which had originated in the late sixties under the form of ARPANET to be used by the U.S. military, burst into a world phenomenon in the 1990s. It has a following

[1] Ayushi Vaid, LLM Student at Faculty of Law, University of Delhi

of more than 5 billion people today and India alone has over 800 million users[2].

Online commerce, content and communication have increased to evolve virtually all forms of life in the day to day life and as such, there has been an increase in the number of cross-border internet disputes and with them, it has been realised that it can make a huge difference which court they go to. When a plaintiff succeeds in one law system, he/she may fail in another. Such reality has created the phenomenon of the so-called juridiction shopping whereby the choice of a legal forum is made not on any actual relationship between the dispute and the specific court, but due to the fact that the laws of a particular court are just conducive to the party that is doing the selecting[3].

Jurisdiction shopping is not a recent development; lawyers have always been in search of conducive forums. But the internet has opened up a wide jurisdictional area and lessened obstacles to litigation over distance. Therefore, what used to be a restricted and controllable practice has become a structural attribute of cyber litigation. The doctrine of *forum non conveniens* which was created to ensure that forum selection was not abused was created in a time characterized by geographical limits and physical inconvenience. This doctrine has found it more difficult to work in the digital arena. This paper examines the problem of jurisdiction shopping in cyberspace with the seriousness that its scale demands.

The central argument is that existing legal tools are valuable but structurally insufficient, and that targeted reform is needed both in Indian law specifically and in the international framework more broadly.

The paper draws on primary sources including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Civil Procedure Code, 1908, and significant judicial decisions from Indian and foreign courts. With the rapid expansion of digital interactions and the growing complexity of cross-border disputes, jurisdiction shopping has emerged as an increasingly relevant issue in contemporary cyber litigation. The tension between traditional jurisdictional principles and the borderless nature of cyberspace calls for a closer examination of existing legal frameworks and judicial approaches. This paper seeks to analyse these developments and contribute to the broader discourse on adapting jurisdictional principles to the evolving realities of the digital age.

[2] Internet and Mobile Association of India (IAMAI) & Kantar, *India Internet 2023 Report* (2023)

[3] Jack L Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 1-3.

II. JURISDICTION IN CYBERSPACE

Meaning of Jurisdiction

The concept of jurisdiction refers to the authority of a legal body whether a court, a legislature, or an executive agency, to act with legal force in a given situation. In international law, the term is typically broken down into three distinct but related senses: *prescriptive jurisdiction* (the authority of a state to enact laws governing particular conduct), *adjudicative jurisdiction* (the authority of a court to hear and decide a particular dispute), and *enforcement jurisdiction* (the authority to give practical effect to laws or judgments).[4]

In the Indian context, the basic rules governing a civil court's adjudicative jurisdiction are laid down in the Code of Civil Procedure 1908. Section 20 of the CPC provides that a suit may be instituted where the defendant resides or carries on business, or where the cause of action arises. This framework was plainly conceived with physical persons and physical locations in mind. A shopkeeper operates from premises that can be identified on a map. A tort is committed at a place that can be specified in an address. An internet platform, by contrast, may have no physical presence in any particular country, may serve users across dozens of jurisdictions simultaneously, and may be incorporated in a country entirely different from the ones where its operators live and its users reside.

Traditional principles of jurisdiction

Classical international law acknowledges a number of accepted principles, which a state can base its claim to jurisdiction. The territorial principle is that a state is in control of all individuals and happenings in its geographical regions. This is the principle which was upheld in the famous Lotus case[5] is the basis of the modern doctrine of jurisdiction. The principle of nationality gives a state authority over its own citizens no matter where they are in the world. The effects doctrine allows the jurisdiction to apply to foreign acts that cause adverse effects on the territory of the state, although the actor did not enter the state. The protective principle enables jurisdiction to be taken over foreign acts that pose a threat to important national interests like national security or integrity of state currencies.[6]

When courts are considering the application of international law, they consider connecting

[4] Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press 2007) 1-5

[5] SS Case (The Lotus) (France v Turkey) PCIJ Rep Series A No 10 (1927) 18-19 (Permanent Court of International Justice).

[6] F Mann, "The Doctrine of Jurisdiction in International Law" (1964-I) 111 Hague Recueil des Cours 1, 9.

factors, which tie a case to a specific legal system: domicile, habitual residence, place of contract formation, place of performance, place of the tort. These aspects are fairly functional in situations where the concerned individuals and occurrences can be traced to a geographical point. This pinning becomes impossible or at most very artificial which is the structural problem which the internet introduces.

Why cyberspace creates such difficulties

The internet was designed to route information around damage. It was not designed to route legal authority around jurisdictional conflicts. That asymmetry is the source of most of what follows.

Cyberspace fundamentally challenges each of the three traditional principles. Three structural features of the internet are particularly relevant to the jurisdiction problem.

1. The first is *ubiquity*: any content uploaded on the web can be accessed anywhere in the world as long as that country is connected. When sheer accessibility sufficed to establish jurisdiction, the courts of all countries would proclaim themselves the right to hear any internet dispute. When a defamatory article is posted on the internet, it is published everywhere the internet is available, and not in one place. The author could be in Singapore, the server could be in the United States, the readers could be in India and the topic of defamation could be in the United Kingdom. What are the governing jurisdictions of these territorial relationships?[7]
2. The second structural difficulty is *anonymity and technical evasion*. The traditional principles of jurisdiction rely on the knowledge of party locations and party identity. On the Internet, an actor can act anonymously, hide his or her geographic location with a Virtual Private Network, or direct his or her activity via corporate arrangements distributed in several jurisdictions. The process of determining the physical presence of an online actor to have jurisdiction over it can be both technically difficult and factually unclear.[8]
3. *Regulatory divergence* is the third and, at least as far as present purposes are concerned, the most important structural challenge. Various nations have radically disparate laws regarding defamation, privateness, intellectual property, and data protection. What may

[7] Michael A Geist, "Is There a There There? Toward Greater Certainty for Internet Jurisdiction" (2001) 16 Berkeley Technology Law Journal 1345, 1348.

[8] Dan Jerker B Svantesson, *Private International Law and the Internet* (3rd edn, Kluwer Law International 2016) 3-7.

be defamation in England or criminal hate speech in Germany may qualify as a constitutionally defamed statement under the First Amendment to the United States Constitution. This deviation establishes a structural incentive which becomes permanent, that parties to a dispute will seek to find the most favourable law to themselves, and will then build what connecting factor exists to have their case heard in that forum.[9]

Cross-Border Internet Disputes: Categories

Understanding why jurisdictional clarity matters requires a brief survey of the kinds of disputes that arise from cross-border internet activity. *Online defamation* cases arise where content posted in one country damages a person's reputation, most significantly, in another. *Intellectual property disputes* involve websites or applications that infringe trademarks, copyrights, or patents while operating across multiple jurisdictions. *Data protection violations* occur where personal data of users in one country is collected, processed, or traded by entities operating elsewhere. *E-commerce and contract disputes* arise from online transactions between parties in different countries governed by different consumer protection laws. In each category, the jurisdiction question is not peripheral: it determines which law applies, what remedies are available, and whether any judgment can be enforced.[10]

It is also worth noting the specific position of India in this landscape. India is simultaneously one of the world's largest internet user markets, a significant exporter of digital services, and a jurisdiction whose citizens and businesses are frequently affected by the conduct of foreign-incorporated digital platforms. The stakes of the jurisdiction question for Indian law are therefore unusually high, a point that shapes the analysis throughout this paper.

III. JURISDICTION SHOPPING AND FORUM CONVENIENCE

Jurisdiction shopping is the practice of selecting a legal forum to hear a dispute based primarily on the favourability of that forum's laws, rather than on any genuine connection between the forum and the subject matter of the dispute. It is, at its core, a form of strategic arbitrage: the shopper is not asking which court has the most natural connection to the case but which court will deliver the best result. In the internet context, this practice is particularly prevalent because the borderless nature of online activity creates a large, and in some cases almost unlimited,

[9] JR Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1998) 76 Texas Law Review 553, 555.

[10] HH Perritt Jr, "Jurisdiction in Cyberspace" (1996) 41 Villanova Law Review 1, 7-8.

menu of potentially available forums.

In traditional litigation, even an opportunistic plaintiff needed to establish some plausible physical connection to the chosen jurisdiction. Online, the ubiquity of internet content means that almost any country can credibly assert some nexus to any online dispute, since the content was presumably accessible from its territory. The practical constraint of physical connection has been dramatically weakened.[11]

Reasons for Jurisdiction Shopping

A) The most documented reason is *substantive law advantage*. The most striking example is "libel tourism," the practice of foreign plaintiffs choosing English courts for defamation claims because English law placed the burden of proof on defendants and did not extend the constitutional protection afforded to American defendants.[12] Parliament's response in the Defamation Act 2013, which requires courts to verify that England is "clearly the most appropriate" forum for claims against foreign defendants,[13] was a direct legislative intervention against this form of jurisdiction shopping. Similar dynamics appear in Indian trademark and copyright disputes, where foreign rights-holders sometimes prefer Indian courts for their ability to grant ex parte interim injunctions against local defendants.

B) A second reason is *procedural advantage*. Some forums offer more favourable rules on interim relief, discovery or class actions. An Indian plaintiff seeking urgent removal of online content may prefer the Delhi High Court for its relatively speedy interim relief mechanism, even if the underlying dispute has stronger connections to another jurisdiction.

C) A third reason, particularly relevant to defendants rather than plaintiffs, is *evasion of accountability through structural arbitrage*. By incorporating in jurisdictions with minimal regulatory obligations, structuring data flows through countries with permissive privacy laws, or locating servers in places where enforcement actions are difficult, online businesses can effectively insulate themselves from the jurisdiction of countries whose users they serve. This "race to the most permissive jurisdiction" has been a persistent feature of the global internet economy.

[11] F Reynard, "Defamation Tourism and the Internet: Protecting Freedom of Expression in a World Without Borders" (2012) 35 Boston College International and Comparative Law Review 217, 229.

[12] *New York Times Co v Sullivan* 376 US 254 (1964) 279-80 (Brennan J).

[13] Defamation Act 2013 (UK), s 9(2) (requirement that England and Wales be the 'clearly most appropriate' place for claims against defendants domiciled outside the United Kingdom).

The doctrine of Forum Conveniens and its abuse

The common law's primary response to forum shopping is the doctrine of forum non conveniens, which permits a court to decline jurisdiction in favour of a clearly more appropriate foreign forum. In English law, the doctrine was definitively stated by the House of Lords, describig the applicable test as follows:

The basic principle is that a stay will only be granted on the ground of forum non conveniens where the court is satisfied that there is some other available forum, having competent jurisdiction, which is the appropriate forum for the trial of the action, i.e. in which the case may be tried more suitably for the interests of all the parties and the ends of justice[14].

In the United States, the parallel doctrine was established which directs courts to weigh private interest factors, such as access to evidence and the compellability of witnesses, and public interest factors, such as court congestion and the local community's interest in the dispute.[15] American courts give the plaintiff's choice of forum considerable presumptive weight, especially when the plaintiff is domiciled in the chosen forum.[16]

The fundamental limitation of forum non conveniens is that it was designed to address geographic inconvenience: the difficulty of litigating in a physically remote place. In cyberspace, there is no such inconvenience. A claimant in Delhi can file proceedings in an English court and conduct much of the litigation remotely at modest additional cost. The inconvenience the doctrine was meant to prevent, the burden of travelling to a distant country to litigate, has been substantially reduced by technology. What remains is the substantive legal inconvenience of being judged by a foreign legal system that the defendant did not choose and has no real connection to, and this is precisely the kind of inconvenience that the doctrine is least well-equipped to address.

IV. JUDICIAL TESTS FOR DETERMINIG JURISDICTION IN CYBERSPACE

Because the traditional rules of jurisdiction were not designed for a borderless medium, courts in common law jurisdictions have had to develop new analytical frameworks for deciding when they have the authority to hear internet-based disputes. Four principal tests have emerged from

[14] *Spiliada Maritime Corporation v Cansulex Ltd* [1987] AC 460 (HL) 476 (Lord Goff).

[15] *Gulf Oil Corp v Gilbert* 330 US 501 (1947) 508-09 (Jackson J) (private and public interest factors for forum non conveniens).

[16] *Piper Aircraft Co v Reyno* 454 US 235 (1981) 241 (Marshall J) (plaintiff's choice of home forum entitled to great deference).

this process, and between them they represent most of the analytical toolkit available to any court approaching a cyber-jurisdiction question.

1. *The Minimum Contacts Test*

The minimum contacts test was established by the US Supreme Court in International Shoe Co v Washington (1945), which held that the exercise of jurisdiction is constitutionally permissible where a defendant has established minimum contacts with the forum state such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice. The Court held that the exercise of jurisdiction by Washington courts was constitutionally permissible because the company had established certain minimum contacts with the state.

...To the extent that a corporation exercises the privilege of conducting activities within a state, it enjoys the benefits and protection of the laws of that state. The exercise of that privilege may give rise to obligations; and, so far as those obligations arise out of or are connected with the activities within the state, a procedure which requires the corporation to respond to a suit brought to enforce them can, in most instances, hardly be said to be undue[17].

In the cyberspace context, the central difficulty is identifying what constitutes a "contact" with a forum state when all interaction occurs digitally. The Court in *World-Wide Volkswagen Corp v Woodson* had already clarified that contacts must result from the defendant's own deliberate choices, not from the "unilateral activity of another party."[18] this means that mere website accessibility in a state is insufficient. The defendant must have made deliberate choices that created meaningful connections with the forum.

2. *The Effects Test*

The effects test was articulated by the Supreme Court in *Calder v Jones*, a case where the plaintiff, a California actress claimed that a National Enquirer article written by Florida-based journalists had defamed her. The question was whether California courts had personal jurisdiction over the Florida defendants. The Court said yes, on the basis that the article was "aimed at" California and the brunt of its harm was felt there.[19]

The appeal of the effects test in internet cases is obvious which is that the digital conduct typically produces its most significant consequences not at the place where the defendant is physically located, but at the place where the affected person lives and where their reputation,

[17] *International Shoe Co v Washington* 326 US 310 (1945) 316 (Stone CJ).
[18] *World-Wide Volkswagen Corp v Woodson* 444 US 286 (1980) 297 (White J).
[19] *Calder v Jones* 465 US 783 (1984) 788 (Rehnquist J).

business relationships, and property interests exist. For Indian claimants harmed by foreign online conduct, an effects-based approach would allow Indian courts to hear cases in which the harm is experienced in India, regardless of where the defendant operated from.[20]

The risk of the effects test, if taken too far, is that it threatens to produce jurisdiction everywhere. Harmful online content produces effects in every country where it is read. The solution is to insist on something more than mere effects. the defendant must have *deliberately aimed* their conduct at the forum state, knowing that the effects would be felt there.

3. *The Purposeful Availment Test*

The purposeful availment doctrine was introduced in *Hanson v Denckla*, where the Supreme Court held that the constitutional test for personal jurisdiction requires that the defendant have "purposefully avail[ed] itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws."[21] The word "purposefully" does a great deal of work here: it prevents a defendant from being haled into a foreign court because of contacts created entirely by someone else's choices.

In *Burger King Corp v Rudzewicz*, the Court elaborated that the key question is whether the defendant has deliberately engaged with the forum, such that it is "reasonably foreseeable" that they might be required to defend themselves there.[22] Applied to the internet, this means asking: did this defendant make deliberate choices to engage with this country's market? Did they advertise in its language, accept its currency, target its consumers, or enter into contractual relationships with its residents? If yes, it is fair to require them to answer for those choices before that country's courts. If the only connection is that their website happened to be technically accessible from that country, the answer should generally be no.

4. *The Zippo Sliding Scale Test*

The Zippo test proposed a sliding scale based on the interactivity of a defendant's website, from passive informational sites having no jurisdiction to fully commercial interactive ones having jurisdiction. The test has not aged well: by the 2010s, virtually every commercial website had become "interactive." Courts have since supplemented Zippo with the purposeful availment standard, requiring that the defendant have directed its electronic activity into the state with the manifest intent of engaging its residents — producing functional equivalence with the Indian

[20] ibid 789.

[21] *Hanson v Denckla* 357 US 235 (1958) 253 (Warren CJ).

[22] *Burger King Corp v Rudzewicz* 471 US 462 (1985) 475 (Brennan J).

targeting test.

V. JUDICIAL APPROACHES TO JURISDICTION SHOPPING

United states

The constitutional purposeful availment framework is used by American courts as the leading approach to jurisdiction shopping. The Due Process Clause of the Fourteenth Amendment establishes an outer limit on the state court jurisdiction over non-residents, and offers structural resistance to the plaintiff-side forum shopping: a plaintiff cannot simply shop to a state forum where the defendant does not have any meaningful connections. The forum non conveniens doctrine was reaffirmed as an added check in *Piper Aircraft Co v Reyno*, but a domestic plaintiff continues to enjoy a high level of deference in his selection of home forum.

Yahoo! Inc v La Ligue Controle le Racisme et lAntisemitisme was an example of the opposite side. A French court had requested Yahoo to prevent French users access to auctions of Nazi memorabilia on its US-based site on the ground of French law. Yahoo wanted the order in California to be declared unconstitutional by the First Amendment, yet the en banc Ninth Circuit ruled it off on grounds of personal jurisdiction. The case made it clear that jurisdiction shopping can be done in both directions as the plaintiffs want to find favourable substantive forums and the defendants want to find protective ones to shield themselves against foreign judgments that they find intolerable.

United Kingdom

The English courts in the past have dealt with jurisdiction shopping by two main tools: the doctrine of forum non conveniens and the authority to order anti-suit injunctions. Following Spiliada, English courts will decline jurisdiction where another forum is "clearly more appropriate" for the dispute. Anti-suit injunctions are used to prevent parties to initiate proceedings in a foreign court that is initiated in violation of an exclusive jurisdiction clause or in unsuitable circumstances, and have been used in cases where there is an online aspect to the case.[23]

The most direct legislative intervention was the Defamation Act 2013 which, as observed in Chapter 3, placed a condition that England demonstrates itself to be by far the most suitable venue to take action against defendants domiciled outside the UK. Parliament reacted to this

[23] *King v Lewis* [2004] EWCA Civ 1329, [27]; see also *Airbus Industrie GIE v Patel* [1999] 1 AC 119 (HL) 133 (Lord Goff).

by seeking to limit the continued use of English courts by foreign litigants who had only a very loose connection to England, as a way of using the friendliness of English law to defamation claims to keep their critics, who mostly practised elsewhere, quiet. The problem of internet multi-publication with EU law had already been determined in *Shevill v Presse Alliance SA*, where the House of Lords decided that the damage in each country should be subject to the jurisdiction of the court in that country, and that the damage in the country of residence of the publisher should be subject to the jurisdiction of the court of the country of residence.[24]

European Union

The European Union has developed the most institutionally structured approach to cross-border internet jurisdiction. The Brussels I Recast Regulation provides that in tortious matters, a defendant may be sued in the courts of the place "where the harmful event occurred or may occur."[25] The CJEU has interpreted this progressively in the online context. In *eDate Advertising GmbH v X*, the court held that for online defamation, a claimant can sue either in the courts of the member state where the publisher is established (for all damages) or in the courts of the member state that forms the "centre of gravity" of their interests, typically the state of their habitual residence (again for all damages), or in the courts of each member state where the content was accessible (but only for local damage).[26]

This framework was developed further in *Bolagsupplysningen OU and Ilsjan v Svensk Handel AB*, where the CJEU held that an application for rectification or removal of online content must be brought in the courts with jurisdiction over the entirety of the damage, since a partial-damage court cannot effectively order removal of content that is globally distributed. The centre-of-gravity approach has the virtue of anchoring jurisdiction in a genuinely significant human reality, the place where the claimant's life and interests are concentrated, rather than in the technical accident of which servers happen to host the content.[27]

Indian Approach

Early Phase

The judicial involvement of India in internet jurisdiction started in early 2000s. In *SMC*

[24] *Shevill v Presse Alliance SA* [1995] AC 18 (HL); applied in the online context in *King v Lewis* [2004] EWCA Civ 1329.

[25] Regulation (EU) No 1215/2012 (Brussels I Recast), Art 7(2) (special jurisdiction in matters relating to tort, delict or quasi-delict).

[26] C-509/09 and C-161/10 *eDate Advertising GmbH v X* [2011] ECR I-10269, [48]-[52] (CJEU).

[27] C-194/16 *Bolagsupplysningen OU and Ilsjan v Svensk Handel AB* [2017] EU:C:2017:766, [47] (CJEU).

Pneumatics (India) Pvt Ltd v Jogesh Kwatra the Delhi High Court ordered an injunction on an employee who was using an India-associated address to send defamatory emails to the business associates of the plaintiff. The case was fairly easy to understand, yet the facts laid down in it gave the court the readiness to address online disputes.

Casio India Co Ltd v Ashita Tele Systems Pvt Ltd went even further by deciding that there was jurisdiction in an online trademark dispute in part due to the fact that the site of the defendant was also accessible in Delhi. This argument of accessibility was a plausible initial step, although unsustainable in the long run - had accessibility become sufficient, the courts of Delhi would have to have authority over all sites on the web.

Banyan Tree: The Targeting Standard

The doctrine of Indian cyber-jurisdiction is now founded on a 2009 ruling by the Delhi High Court in *Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy*. A Singapore hospitality company filed a plaintiff alleging that an Indian hotel web site had infringed its trademarks. The defendant claimed that the Delhi High Court did not have territorial jurisdiction. The court in a thoroughly thorough and analytically splendid judgment reviewed both American and international jurisprudence and reached the conclusion that accessibility standard must be rejected in favour of a targeting test.[28]

The mere fact that a website is accessible in Delhi does not automatically give Delhi courts territorial jurisdiction. What is required is something more: evidence that the defendant's website specifically targeted or was directed at consumers or users in Delhi, such as by transacting business there or causing harm there.

The court found tangible evidence of targeting: using Indian currency, providing Indian contact information, specifically targeting Indian consumers, and having actual transactions with Indian users. All these would have added up to the something more necessary to prove that the Delhi cause of action was in existence and that the Delhi courts had therefore jurisdiction under Section 20 of the CPC.[29]

The Banyan tree standard was used and perfected in the subsequent cases. In *World Wrestling Entertainment Inc v Reshma Collection*, the court upheld the jurisdiction in cases where the defendant had his site where he supplied goods to Indian consumers and received payment in

[28] *Banyan Tree Holding (P) Ltd v A Murali Krishna Reddy* (2009) 40 PTC 291 (Delhi HC) [22]-[27] (Manmohan Singh J).

[29] ibid [27]. The court drew on the American purposeful availment doctrine while grounding its analysis firmly in the language of CPC s 20.

rupees[30]. In *Super Cassettes Industries Ltd v MySpace Inc*, the court held that the advertising revenue earned by a US-based platform by India and serving Indian users was enough to amount to targeting[31]. The principle was applied in *Intex Technologies v Papst* licensing to patent cases in which negotiations on licensing had been directed at Indian manufacturers. The Banyan Tree standard was applied and refined in the cases that followed.

Platform Jurisdiction: Swami Ramdev, Adarsh Kumar, and Beyond

The proliferation of large social media platforms from 2015 onwards raised a new set of jurisdictional questions, centred on the challenge of suing foreign corporations that lacked a locally incorporated Indian subsidiary. In *Swami Ramdev v Facebook Inc*, the Delhi High Court asserted jurisdiction over the American corporation on the basis of its significant commercial operations directed at Indian users and its employment of Indian-based staff, developing an implied-presence or agency-based approach to jurisdiction in the absence of formal incorporation.[32]

A cleaner resolution came in *Adarsh Kumar v Google LLC*, where the court held that Google India (Private) Limited, as a separately incorporated Indian company that carries on business in Delhi, constitutes Google's "carrying on of business" within the meaning of Section 20 of the CPC, grounding jurisdiction over the global parent company's operations affecting Indian users. This judgment is significant because it confirmed that the mandatory appointment of Indian subsidiaries and compliance officers by major platforms, as required by the IT Rules 2021, has a direct jurisdictional consequence.[33]

The most technologically novel development in recent Indian cyber-jurisdiction law is *Anil Kapoor v Simply Life India and Others* (2023), in which the Delhi High Court issued India's first dynamic injunction against AI-generated deepfakes of a public figure. The court asserted jurisdiction over foreign AI platforms on the targeting standard and extended its order prospectively to cover AI-generated content matching specified parameters in the future. The prospective and dynamic character of this injunction represents a significant development in the reach of Indian courts into the online environment.[34]

[30] *World Wrestling Entertainment Inc v Reshma Collection* (2014) 60 PTC 452 (Delhi HC) [19].

[31] *Super Cassettes Industries Ltd v MySpace Inc* (2011) 47 PTC 49 (Delhi HC) [21]-[23].

[32] *Swami Ramdev v Facebook Inc* CS(OS) 27/2019 (Delhi HC, order dated 23 August 2019) [8]-[12] (Rajiv Sahai Endlaw J).

[33] *Adarsh Kumar v Google LLC* 2022 SCC OnLine Del 4100, [16]-[20] (Delhi HC).

[34] *Anil Kapoor v Simply Life India and Others* CS(COMM) 652/2023 (Delhi HC, 20 September 2023) [14]-[18] (Amit Bansal J) (first Indian judgment deploying a dynamic injunction against AI-generated deepfakes of a public figure).

The IT Act as a Jurisdictional Foundation

Beyond the CPC framework, Section 75 of the Information Technology Act 2000 provides an explicit statutory basis for extraterritorial jurisdiction. It reads:

The provisions of this Act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India[35].

Section 75 anchors Indian jurisdiction in the location of the targeted infrastructure rather than the location of the offender. Its scope is, however, limited: the provision requires a nexus with a computer *located* in India, not merely one accessible from India. A foreign attacker who harms Indian users by accessing data stored entirely on foreign servers may fall outside this provision's reach. The IT Rules 2021 have partially addressed this gap by requiring significant social media intermediaries to appoint resident compliance officers in India,[36] creating jurisdictional anchors for the largest platforms that persist regardless of their formal country of incorporation.[37]

The constitutional dimension of this statutory framework was highlighted by the Supreme Court in *Shreya Singhal v Union of India*, where Section 66A was struck down as unconstitutionally overbroad.[38]

"Section 66A is cast in terms so wide that virtually any opinion on any subject would be within its reach... The possibility of its misuse, with respect to expressions that are clearly protected, calls for its invalidation in entirety."

- Nariman J, Shreya Singhal v Union of India (2015)

The Shreya Singhal decision matters for jurisdiction shopping in a specific way: before it was decided, Section 66A had been regularly exploited as a tool of strategic forum selection, with complainants filing FIRs in distant districts precisely to impose maximum inconvenience on accused persons who had to travel there for bail hearings. The striking down of Section 66A removed this particular instrument from the jurisdiction shopper's toolkit, but the broader problem of using criminal jurisdiction strategically in internet matters persists and has not been comprehensively addressed.[39]

[35] Information Technology Act 2000 (India), s 75(1).

[36] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), r 4(4).

[37] Information Technology Act 2000 (India), s 1(2) read with s 75; see also Information Technology (Amendment) Act 2008.

[38] *Shreya Singhal v Union of India* (2015) 5 SCC 1, [93] (Nariman J).

[39] *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC) (nine-judge bench unanimously recognising the right to privacy as a fundamental right under Art 21 of the Constitution).

VI. CHALLENGES AND LEGAL ISSUES

1. **Conflicting Judgments:** Producing irreconcilably conflicting judgments is one of the most apparent effects of unchecked jurisdiction shopping. This was clearly demonstrated by Yahoo!, where different courts in France and the US came to different conclusions on the legality of the same online activity, creating a state of legal incoherence whereby adherence to one court ruling would equate to non-adherence to the constitutional provisions of another legal framework. To personal bloggers, small online companies and academic researchers, this type of conflict is not just inconvenient, but is virtually crippling.
2. **Increased Litigation Costs:** In cases where a plaintiff initiates a case in a jurisdiction and has no real association with the case, the defendant will incur the entire burden of defense in an unknown court system. In the case of large multinationals, this becomes expensive but can be done. To a single journalist, a small start-up or a researcher at a university, the expense of litigating in foreign proceedings is literally devastating even when the underlying allegation is factually incorrect. This asymmetry contributes to the strategic importance to jurisdiction shopping in the case that a claimant is aware that the defendant is unable to afford the expense of a foreign proceeding: a claimant does not always need to prevail on the merits. This type of abuse is dubbed by scholars as strategic litigation against public participation (SLAPs), and the application of multi-jurisdiction internet proceedings as a SLAPS device is a proven and increasingly prevalent issue.
3. **Harassment via Parallel Proceedings:** Related to cost problem is the tactic of commencing parallel proceedings in multiple jurisdictions simultaneously. Although none of the people going through might be merited, the aggregate load of handling various actions at once might be high enough to submit. This takes advantage of the very characteristic of internet law that allows jurisdiction shopping to be possible: that there are multiple potential competent forums. The period before the Shreya Singhal case marked many cases of criminal charges against internet users in districts selected to be as remote as possible to the accused. The civil aspect of this issue is yet to be covered after Shreya Singhal.
4. **Legal Uncertainty:** The above challenges are merely symptomatic of a more profound and systemic issue: a fundamental legal uncertainty regarding which country law applies to online activity, and which courts is empowered to adjudicate online disputes.

This ambiguity is not just a nuisance but a structural flaw in legal framework surrounding one of the most significant economic and communicative spaces in human history. To the people, the law is uncertain and it sends a chilling effect on freedom of expression. An individual that is unaware of what law of defamation in which country his or her online writing falls is not in a position to tailor their speech to a specific legal norm. In the case of businesses, it renders operational planning impossible. The Digital Personal Data Protection Act 2023 makes a significant step, with an overt extraterritorial scope clause, and the IT Rules 2021 give clarity on the jurisdictional anchors of large platforms.

VII. CONCLUSION AND SUGGESTIONS

Suggestions

The following six suggestions address both the internal gaps within India's legal architecture and the external gaps in the international framework.

1. **A Statutory Cyber Jurisdiction Framework.** India needs to establish a particular statutory provision, either via an amendment to the CPC or as a separate Cyber Disputes Jurisdiction Act, to codify the Banyan Tree targeting standard, delimiting the evidentiary requirements of targeting, clear rules of process service on foreign defendants acting through locally appointed compliance officers, and specifying the circumstances under which Indian courts may stay proceedings in favour of a more appropriate foreign forum.
2. **Immediate Constitution of the Data Protection Board.** The Data Protection Board of India should be established as an issue of priority. With no operational Board, the extraterritorial provisions of the DPDPA have little impact on foreign data controllers. Adequate investigative powers, enforcement tools such as the power to request the help of foreign authorities to assist in an investigation should be provided to the Board, as well as the staffing and resources required to run it.
3. **Accession to Hague Convention Instruments.** India needs to become a signatory to the Hague Convention on Choice of Court Agreements 2005 and actively participate in the Hague Judgments Convention 2019. These tools would enable a multilateral structure of recognition and enforcement of judgments and greatly increase the structural incentive to make a judgment-shopping decision and increase the enforceability of Indian court orders in other countries.

4. **Procedural Protections Against Jurisdictional Harassment.** The Indian procedural law is in need of revision to offer anti-SLAP in jurisdiction shopping cases. Courts ought to be enabled to strike out proceedings at an early stage where claimant is unable to prove the genuine connecting factor between the forum and the content of the proceedings and to impose costs on claimants who use cross-border proceedings as a tool of harassment.
5. **A Proportionality Framework for the IT Rules 2021 Traceability Obligation.** The WhatsApp traceability case pending in the Delhi High Court is a real constitutional dilemma between the right to privacy (upheld in Justice K.S. Puttaswamy v Union of India (2017)) and the interest of the state in proper law enforcement. A proportionality-based solution: such as restricting the traceability requirement to particular types of serious crimes and imposing disclosure orders subject to independent judicial approval would address both interests without necessarily compromising either.
6. **An Evidentiary Framework for VPN and Technical Evasion.** With the normalisation of the use of VPNs, Indian courts require a more precise direction on how to assess the geolocation evidence, which could be technically inaccurate. The onus of proving VPN-based obfuscation ought to be on the party contesting the geolocation evidence. It needs to encourage courts to add corroborating evidence of targeting that goes beyond raw IP logs, including payment history, device configuration, and geographical distribution of user base of a platform.

CONCLUSION

The eventual result of jurisdiction shopping within cyberspace is a symptom of the underlying structural issue: the complete incompatibility of global architecture of the internet with the territorial architecture of the law. The internet was designed to disregard borders. They were the law. Until that tension is constructively resolved, be it by international treaty, by harmonisation of legislation, or by convergence on the agreed minimum standards among the judiciary, the more sophisticated parties will keep playing the game, and the less sophisticated ones will keep paying the price. The weight, as usual, goes down to the weakest to sail through it.

India is not an onlooker to this challenge. Its courts have done their part in the international law of jurisdiction in the internet, and its legislature has passed progressive laws that point to a keen awareness of the digital era. Good doctrine and good legislation are not in themselves

sufficient. In the absence of an institutional apparatus to implement them, in the absence of an international system to provide them with effective scope, the most well-considered principles of law are apt to be mere aspirations and not functioning.

The six recommendations presented in the paper are feasible measures that can be taken in bridging that gap. They do not demand the wholesale reinventing of sovereignty and the establishment of new supranational institutions. They request, less pompously, that there should be better co-ordination, more openness and a common determination to see that the law stays abreast of the technology it is supposed to regulate.

The internet has reduced the world to a smaller size. It has united individuals, cultures, and economies in a manner that was inconceivable 10 years ago. The law is to make this interconnection be met by responsibility, and not also to make the world which the internet has built to be a more lawless world.