Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Analysing Jurisdictional complexities in the cyberspace: The Indian perspective

Unnati Khanna[a]

[a]Symbiosis International University, Pune, India

Received 25 December 2021; *Accepted* 06 January 2022; *Published* 10 January 2022

In an era of globalization and digitalization, businesses operate on a global level through the use of the Internet, which has its web spread across the globe. Cyberspace facilitates cross-border transactions that can be formulated and concluded with a few clicks. Consequently, these transactions may result in cross-border disputes between parties sitting countries apart. The Internet has revolutionised the way the working of the world, however, every coin has two sides. The Internet has undeniably and inevitably created a space where anonymity, accessibility, and distance have made it easier to commit cybercrimes. The challenges brought forth by these disputes and crimes in cyberspace are unprecedented and necessitate exploration and development of laws on internet governance that are required to regulate this borderless technological space. Among the various challenges and hurdles that the developing cyberlaw faces, the jurisdictional issue is a primary concern on the legal front. This paper attempts to answer the question that why is internet jurisdiction an issue. It further analyses the international as well as Indian legislative framework with respect to cyberspace jurisdiction. The paper also delves into the United States, Canadian, and Indian judicial approaches to internet jurisdiction to study various tests that have been imported and evolved. Lastly, it provides suggestions to tame down the jurisdictional challenges with respect to cyberspace.

Keywords: *cyberspace, jurisdiction, internet, cybercrime, India.*

INTRODUCTION

Cyberspace can be defined as a virtual space, created with the help of computers, that facilitates the global transfer of data and information. The primary feature of this virtual world is the extremely interactive environment accessible to an incredibly huge participant base at the same time. This space provides its users with a platform to share data, conduct discussions, engage in social interactions and create media content. It further facilitates e-commerce, virtual-gaming collaborations among several other activities. A chief characteristic associated with the internet is that it is borderless i.e., it does not recognize territorial boundaries that create geographic divides among nations. The juncture where this borderless cyberspace collides with national laws governing different nations is where the issue of cyberspace jurisdiction finds its roots.

In general terms, jurisdiction refers to legislative, administrative, and judicial competence and it is a legal facet of state sovereignty.[1] Despite being a facet of sovereignty, jurisdiction is not conterminous with it. The national laws may have an extra-territorial operation, thereby expanding the jurisdiction beyond territorial and sovereign boundaries of the nation. This becomes problematic, particularly in the case of the Internet which does not recognize territorial or sovereign limitations. In the absence of universally applicable, uniform international law on jurisdiction, the disputes arising in the realms of cyberspace are construed as matters under the private international law domain.[2]*For instance,* an online legal publication or conduct may be legal in one country, yet illegal in some other country. In absence of a uniform code dictating jurisdictional rules with respect to the internet, the legal fraternity is left in a conundrum.

A single cyberspace transaction can be governed by laws of three different jurisdictions: (1) national laws of the state where the user resides, (2) national laws of the State the server which hosts the transaction has its locus, and (3) the national laws governing the business or person

[1] Tushar KantiSaha, '*Cyberspace−Conflicting Jurisdictional Spheres of Litigating IPR Claims*', 15 Journal of Intellectual Property Rights 364, 366 (2010)
[2] Prevy Parekh and Tarunya Roy, '*Cyberspace and Jurisdiction*', 2 Journal on Contemporary Issues of Law 1, 12 (2016)

with whom the user transacts. This paper aims at exploring the evolution of traditional jurisdiction principles to become amenable to disputes and crimes happening on the internet. In this paper, *Part I* analyses why are jurisdiction a challenge with respect to the Internet. *Part II* sheds light upon the International and Indian legislative framework of Internet Jurisdiction. *Part III* further gives an insight into the judicial approach to jurisdiction issues in cyberspace and various tests that have been evolved globally with special emphasis on the approach adopted by the Indian Judiciary. *Part IV* discusses two theories evolved by researchers to address the issue of cyberspace jurisdiction and their criticism. Finally, *Part V* provides a suggestion that can be enforced for better development of jurisdictional laws in cyberspace.

WHY IS INTERNET JURISDICTION AN ISSUE?

The existing International Legal System is held together by pieces of separate and territorially defined national jurisdictions. However, the transnational nature of the internet necessitated the expansion of the legal system to pierce the technological arena to formulate laws that are not dependent on the territory.[3] This posed a challenge to the Westphalian Model under international law which supports exclusive state sovereignty and non-interference. As far as the internet is concerned, several factors are important in the determination of the applicable law such as (1) location of internet users, (2) location of the servers storing the data, (3) location of Internet Companies running the services in question, and (4) the registrars through which the domain name has been registered.[4] This overlapping and conflicting territorial criterion makes the determination and enforcement of applicable laws become difficult and inefficient in trans-border cybercrimes cases. The international principles of "*non-interference*" and "*separation of sovereignties*" render the enforcement of judicial pronouncements inefficient and difficult and deter cross-border cooperation which is needed to deal with cyber disputes effectively. Such issues continue cropping out as the internet is widespread across the globe with users from countries that have divergent and conflicting national laws, social sensitivities, and cultures.

[3] Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation'(*Global Commission on Internet Governance,* April 2016) <https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf> accessed 06 November 2021

[4] Prevy Parekh and Tarunya Roy (n 2)

To exemplify, Internet jurisdiction problems could arise involving hate speech on the Internet as a publication of certain information might be protected in one country whereas prohibited in another. In such cases, issues arise as to the ability of the latter to have jurisdiction over the person publishing such information on the internet.[5] Another major issue revolves around professional licensing. For instance, if a doctor in the USA offers online medical advice through a website, does any other country's government claim that such doctor is practicing medicine in that country without a license and hold him liable for the same by invoking the jurisdiction of the appropriate forum. The issues are unprecedented and require creative solutions. The current situation necessitates cooperative collaboration between all stakeholders i.e. the government, Internet platforms, civil society groups, technical operators, international organisations, and internet users.[6] Additionally, the jurisdictional challenge to Internet governance inevitably impacts other policy challenges which include the development of global digital economies, providing clear and predictable legal environments, ensuring the protection of fundamental human rights, cybersecurity, and public order.[7] Therefore, active involvement of all the stakeholders is necessary to settle online jurisdictional tensions and prevent Internet fragmentation. Understanding and acknowledging the magnitude of this jurisdictional challenge is the first step in order to find a common solution.

DECODING THE LEGAL FRAMEWORK ON INTERNET JURISDICTION

Principles on Jurisdiction under International Law

International law recognizes three categories of jurisdiction: (a) jurisdiction to prescribe, (b) jurisdiction to enforce, and lastly, (c) jurisdiction to adjudicate. In the context of cyberspace, we are mostly concerned with the jurisdiction to prescribe which as it pertains to the States' right to make domestic laws governing that State, applicable to the activities, status of persons, relations, or interest of persons in things.[8] Under International law, the commonly accepted

[5] Justice S. Muralidhar, 'Jurisdictional Issues in Cyberspace', 6 Indian Journal of Law & Technology 1-42 (2010)
[6] Michael Gilden, 'Jurisdiction and the Internet: The Real World Meets Cyberspace', 7 ILSA Journal of International and Comparative Law Review 149 (2000)
[7] Kevin A. Meehan, 'The Continuing Conundrum of International Internet Jurisdiction', 31 B.C. Internaltional and Comparative Law Review 345 (2008)
[8] Tushar KantiSaha (n 1)

grounds/theories under which the State's claim of jurisdiction is permitted and the prescription of the State's rule of law over the activity in question is facilitated, in general order of their preference, are as follows: (1) subjective territoriality, (2) objective territoriality, (3) nationality, (4) protective principle, (5) passive nationality, and (6) universality. This must be further coupled with the prerequisite of reasonability with regard to the exercise of such jurisdiction.[9] The theory of subjective territoriality is the most significant among the six. It stipulates that if the activity has been carried out within the geographic confines of the forum state, then such state shall have the jurisdiction to prescribe laws governing such activity. Objective territoriality theory comes into play when the activity has been carried out outside the territorial boundaries of the forum state, yet the forum state is "*primarily affected*" by such activity.[10] This is generally referred to as the "*effects*" principle and has been adopted by courts in several cases while addressing the conundrum of internet jurisdiction.

Indian Legislative Framework

In India, jurisdictional principles are encoded in several Indian Legislations. Primarily the Code of Civil Procedure 1908[11], codifies the law on jurisdiction, however, additionally (as *lex specialis*), Section 13 of the Information Technology Act, 2000[12], Section 11 of the Consumer Protection Act, 1986[13], Section 62(2) of Copyright Act, 1957[14], and Section 134(2) of Trademark Act, 1999[15] supplement it. Though the legislative framework is applicable in cases of national cyber-crimes, however, the same has been liberally interpreted by the judiciary to cover trans-national cybercrimes.

Code of Civil Procedure, 1908

[9] Darrel C. Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces', 4 Michigan Telecom Technical Law Review 69 (1998).
[10] Betsy Rosenblatt, 'Principles of Jurisdiction'(*Cyber Law Harvard*) <http://cyber.law.harvard.edu/property99/domain/Betsy.html> accessed 06 November 2021
[11] Code of Civil Procedure, 1908
[12] Information Technology Act, 2000, s 13
[13] Consumer Protection Act, 1986, s 11
[14] Copyright Act, 1957, s 62(2)
[15] Trademark Act, 1988, s 134(2)

The general rule on territorial jurisdiction is encoded in **Section 20**[16]. It lays down two basic procedural rules for determination of jurisdiction in of competent court in civil cases (1) the place where the defendant actually and voluntary resides, or carries on his business, or personally works for-profit and, alternatively, (2) the place where the cause of action arises, either wholly or in part.

Information and Technology Act, 2000

With respect to E-contracts, **Section 13(3)** of the IT Act lays down that an electronic record is deemed to be received at the place of the business of the addressee of that communication. This implies that jurisdiction arises at the place of business of the person who receives the acceptance of the offer. Additionally, **Section 75**[17] provides extraterritorial jurisdiction to the Indian Courts as often need to assume jurisdiction over foreign subjects would arise with an increase in activity on the Internet. However, section 75 has its own implementational inadequacies and may not prove to be effective as what might be considered a crime in one country might not be illegal in another.

Consumer Protection Act, 1986

In the case of consumer contracts, **Section 11**[18] provides that an action can be brought in the court where either the claimant(s) or defendant(s) reside, carry on business, have a branch office, or personally works for gain or where the cause of action arises, provided that the dispute is a small claim dispute under a certain value. This provision provides the claimant with maximum flexibility as it relates to several different connecting factors, relating to both, the claimant and the defendant

Copyright and Trademark Laws

Section 62 of the Copyright Act, 1957 and the similar **Section 134(2)** of the Trademarks Act, 1999 form an exception to the general rule of territorial jurisdiction encoded in CPC. The

[16] Code of Civil Procedure, 1908, s 20
[17] Information Technology Act, 2000, s 75
[18] Consumer Protection Act, 1986, s 11

general rule postulates that a suit shall be filed where the defendant is based, these two sections provide an option to the plaintiff to bring an action in a court in whose jurisdiction the plaintiff is based, irrespective of where the defendant's locus or where the cause of action has arisen.

JUDICIAL APPROACH TO INTERNET JURISDICTION

"*The lack of territorial precision in an online environment necessarily leads to geographically complex facts. Accordingly, domestic courts addressing these disputes will first have to localize the transaction prior to assuming jurisdiction.*"[19]

The abovementioned lines emphasize the need for the domestic court to entertain the dispute, to "localize the transaction" before assuming jurisdiction. To address this need, the judiciary of several countries has evolved several tests. In this Section, the focus remains on legal tests evolved by the Indian judiciary. India has been walking in the footsteps of the United States Courts with respect to cyberspace jurisdiction. Therefore, a brief analysis of US case laws that have influenced the response of the Indian Judiciary in addressing the need to "localize the transaction" to be able to assume jurisdiction in a dispute presented before the court.

USA

The US courts first faced the conundrum of internet Jurisdiction in ***International Shoe Co. v Washington***[20] In this case, the plaintiff didn't own any property in Washington, however, earned substantial income there. The plaintiff was imposed with taxes enacted by the State on companies doing business in Washington. When the plaintiff approached the court for redress, the issue of internet jurisdiction popped up and the courts introduced the "**Minimum Contacts test**" and observed that the court can exercise jurisdiction over a non-resident defendant if a sufficient minimum level of contacts exist with the forum state such that maintenance of the suit is not opposed to the traditional ideals of substantial justice and fair play. It was further held that lower courts ought to quantity the contact of the defendant with

[19] Wendy A. Adams,' Intellectual Property Infringement in Global Networks: The Implications of Protection Ahead of the Curve' 10 International Journal of Law & Information Technology 71 (2002)
[20] *International Shoe Co. v Washington* [1945] 326 U.S. 310 [1945]

the forum state coupled with the relationship between such contacts prior to the exercise of personal jurisdiction.

This principle was further restricted to "**purposeful availment**" of the defendant to the forum state in ***Hanson v Denckla.***[21]As per this principle, the forum court can exercise jurisdiction over any non-resident defendant, not physically located where an alleged injury arises out of or relates to actions by the Defendant himself that are *purposefully directed* towards residents of the forum state. The Minimum Contacts test has two significant functions which are relatable yet severable: (1) Safeguarding the defendant against the burden of litigating in an inconvenient or distant forum, (2) Ensuring that States remain within the limitations imposed upon them by the virtue of their status as co-equal sovereigns [22] , Therefore, the courts had evolved a three-pronged test with respect to exercise of State's jurisdiction over any non-resident defendant provided that: (a) defendant must be having sufficient "minimum contacts" with the State, (b) the claim that is being asserted by the plaintiff against such defendant should arise out of such contacts, and (c) the principle of reasonability must dictate the exercise of jurisdiction.[23]

However, the holistic analysis of the quality and nature of business-related activities of a site in terms of jurisdiction determination was considered in the case of ***Zippo Manufacturing Co. v Zippo Dot Com, Inc***.[24], where the courts evolved the **'Sliding Scale Test'** based on passive, active, and interactive nature of the websites. Court held that merely passive websites do not form personal jurisdiction, however, the websites that contemplate business with forum state enabling parties of that state to enter into commercial contracts may confer jurisdiction.[25]

[21] *Hanson v Denckla* [1958] 357 U.S. 235
[22] *World-Wide Volkswagen v Woodson* [1980] 444 U.S. 286, 291-92
[23] Jonathan Spencer Barnard, 'A Brave New Borderless World: Standardization Would End Decades of Inconsistency in Determining Proper Personal Jurisdiction in Cyberspace Cases', 40 Seattle University Law Review 249 (2016)
[24] *Zippo Manufacturing Co. v Zippo Dot Com, Inc.*[1997]952 F. Supp. 1119
[25] Trademark Act, 1988, s 134(2)

Prior to this, in the iconic case of ***Calder v Jones***[26], the Court held that when an action is directed towards a particular forum state, even if there is minimum contact, the '**Effects Test'**must be applied. In this case, an article concerned a Californian resident was written and edited in Florida, relying on sources in California. The Court observed that the tortious act was intentional and expressly directed at California. This test implies that where an intentionally done act, has an 'effect' within the forum state and is aimed at the forum state, then jurisdiction shall be satisfied. The effect test is applied in cases with insufficient interactivity or minimum contacts but where the action is targeted at a particular forum. The abovementioned tests have been religiously relied upon by American as well as Indian courts in several other cases.

CANADA

The Canadian Supreme Court evolved the "real and substantial connection" test for internet jurisdiction determination in the case of *Morguard Investments Ltd. v De Savoye*.[27] It was held in this case that the jurisdiction can be exercised when there exists is a connection which is real and substantial, between the forum State, plaintiff, and the defendant, such that the rights of the parties involved are balanced reasonably and appropriately. In another case, the following factors were taken into consideration by the court with respect to cyberspace jurisdiction: (a) the connection between plaintiff's claim and the forum, (b) connection between defendant and forum, (c) whether assuming jurisdiction shall be unfair to the defendant, (d) whether assuming jurisdiction shall be unfair to the plaintiff, (e) Interests of other parties involved in the suit, (f) willingness of the court to support recognition and enforcement of a similar extra-provincial judgement, deriving on grounds of same jurisdictional basis, (g) Nature of the case (International or inter-provincial), (h) Standard and comity of jurisdictions prevailing in other States.[28] The significance of this judgement primarily lies in point (f) as this stresses post-verdict enforcement of the decision and the need for reciprocity with respect to enforcement of

[26] *Calder v Jones* [1984]465 U.S. 783
[27] *Morguard Investments Ltd. v De Savoye* [1990] 3 SCR 1077
[28] *Muscutt v Courcelles* [2002] 213 D.L.R. (4th) 577

the decision in case of a non-resident defendant by the domestic courts of the State where the defendant resides.

INDIA

The first Indian case to ponder over the jurisdictional challenges in cyberspace was ***Casio India Co. V Ashita Tele Systems Pvt. Ltd***[29], wherein in the passing off action, the court prohibited the Defendant from using the website because the website of Defendant is accessible in Delhi, which is sufficient to invoke the territorial jurisdiction of the Delhi High Court. It was observed that the mere ability to access the website gave the court territorial jurisdiction to adjudicate the can brought before it. However, in another case, the Court held that the mere accessibility of a website from one jurisdiction may not be enough or sufficient for a court to exercise its jurisdiction.[30]

The judicial stance on Internet jurisdiction was clarified in ***Banyan Tree Holding Pvt. Limited v A. Murali Krishna Reddy.***[31] Here, none of the parties to the case were situated in Delhi, however, both their websites were accessible there. The court took a different view and held that mere accessibility of a website in Delhi is not enough to confer jurisdiction on the Court. On the lines of US judicial pronouncements, the Court observed that the plaintiff must show the defendant's 'purposeful ailment directed towards the forum state, implying that the website was used for entering into a commercial transaction with the site user which led to an injury or damage to the plaintiff. The Indian Court applied the effects test and the sliding scale test. It also concluded dependence of the law of determining internet jurisdiction following factors:

a) A commercial transaction should have taken place through the website.
b) The defendant should have particularly targeted the forum state.
c) The plaintiff must have suffered an injury as a result of the defendant's actions.
d) The plaintiff must have a presence in the forum state.

[29] *Casio India Co. v Ashita Tele Systems Pvt. Ltd* 2003 (27) PTC 265 (Del)
[30] *Independent News Service Pvt. Limited v India Broadcast Live LlcAndOrs*, 2007 (35) PTC 177 (Del)
[31] *Banyan Tree Holdings v A. Murali Krishna Reddy,* 2009 SCC OnLine Del 3780

Though the test established in Banyan Tree is quite descriptive yet a 'one size fits all' test has not been formulated as this test is applicable in the domain of commercial transaction and intellectual property, but cannot be extended to areas of torts such as defamation. In India's case, cross-border defamation is adjudged as per **Section 19** of the CPC, considering the defendant's location or where the wrong has been done. Additionally, India has also adopted the **double actionability rule**, which requires the offending act to be an actionable tort and non-justifiable as per the laws of the State, to adjudge applicable law in such matters. However, if the tort is committed beyond the Indian boundaries, then Section 19 yields to Section 20 of the CPC[32], and the territorial jurisdiction is adjudged accordingly.[33]

The law on internet jurisdiction was further clarified in ***World Wrestling Entertainment, Inc. v M/s Reshma Collection &Ors,***[34] where the Court observed that due to the spontaneous nature of the transactions over the internet, the cause of action is deemed to have occurred at the place the customer carried out his part of the transaction. In the case of ***Baba Ramdev and Anr.*** **v** ***Facebook Inc.***,[35] a book based on the plaintiff was being globally circulated via social media platforms, like Facebook. The primary issue was whether a global takedown order of the book could be passed by the Court. The Court observed that if the content was either uploaded in India, or from an IP address in India, the content can be taken down and blocked globally, however, if uploaded from outside India, the Court cannot exercise its jurisdiction. In the Banyan Tree Holding case, 2 the Delhi High Court was dealing with an inter-state issue of jurisdiction and not an international dispute. Interestingly, the plaintiff was a foreign company that had invoked the jurisdiction of an Indian court to seek an injunction against the alleged violator of its trademark. The court by and large followed the development of common law in the USA, the UK, and some other Commonwealth countries. Indigenous law is yet to be developed for India.

The laws in the US are quite liquid on the point of personal jurisdiction as compared to the fact-specific tests evolved in India which are more or less inspired by the US jurisprudence on

[32] Code of Civil Procedure, 1908, s 19, 20
[33] *Sarine Technologies v Diyora and BhanderiCorpn.*, 2020 SCC OnLineGuj 140
[34] *World Wrestling Entertainment, Inc. v M/s Reshma Collection &Ors* 2013 SCC OnLine Del 3987
[35] *Baba Ramdev and Anr. v Facebook Inc,* 2019 SCC OnLine Del 630

the subject matter of Internet Jurisdiction. Thus, Indian courts exercise jurisdiction either very narrowly or very broadly, however, always observe the minimum standard. The concept of personal jurisdiction is given a wide berth with a multi-dimensional interpretation in India. The courts in both the countries have ensured a balance between the defendants who are not dragged before a foreign court when they could not foresee being accountable for their actions in a foreign court and the defendants who breach plaintiff's legal rights remotely from a foreign land cannot do so without impunity.[36] This is a challenging balance to make and entertain and the laws will have to evolve with the challenges thrown by the complex space that the internet creates.

THEORIES ON CYBERSPACE JURISDICTION

In this Part, the author attempts to shed light upon two important theories that researchers have evolved with a view to resolve the issue of internet jurisdiction.

The Uploader and Downloader Theory

Cyberspace provides people with an interactive environment that facilitates the flow of information and data amongst individuals. An individual can make use of cyberspace in two possible ways i.e., as an uploader and as a downloader.[37] The uploader makes information accessible to the downloader by placing it in cyberspace. Generally, this transaction is anonymous. The theory of Uploader and Downloader postulates if a foreign jurisdiction gets offended by the information uploaded by the Uploader on the internet, then the jurisdiction shall lie with the State where the offence was "committed and consummated" and not in the State where the person who got offended by such content resides. Therefore, the uploader cannot be tried by a foreign jurisdiction merely because the content he uploaded offended the nationals of that jurisdiction. Therefore, as per this theory, a website should be ascribed to the nationality of its uploader (creator) and cannot be subject to the law governing the downloader.

[36] Julia Hörnle, 'The Conundrum of Internet Jurisdiction and How US Law has Influences the Jurisdiction Analysis in India', 14 Indian Journal Of Law and Technology 183 (2018).
[37] Darrel C. Menthe (n 9)

Theory of International Space

The International space theory gives weightage to nationality instead of territoriality. This theory has been derived from parallel theories governing other borderless spaces such as the seas, outer space, and Antarctica. All these three spaces are not physically similar yet they all possess the characteristic of being sovereign less and international. They share the same characteristic with respect to jurisdiction i.e., the absence of territorial jurisdiction. These spaces are international spaces, like cyberspace. Consequently, this theory postulates that cyberspace must be governed by similar laws which regulate the other international spaces. These three spaces have a regime-specific treaty governing them whereby nationality is of considerable importance for the purpose of jurisdiction establishment. Therefore, cyberspace must also be governed by similar principles and significant consideration must be given to the nationality of the webpage creator, uploader, the maintainer of the webpage with respect to jurisdiction determination.

The disputes in the international spaces are further complexed by two complicated and opposing principles of *res nullius*, which literally means "a thing of no one". This principle asserts that sovereignty can be asserted by any state provided the territorial claim is backed by traditional tests of the validity of such claims.[38] Contrastingly, the principle of *res communis* asserts the notion of equal sovereignty which reflects in United Nations charters. It must be noted that the above theories can be only applied in case of criminal violations whereby the violator can be made subject to the laws governing the State of which he is a national. However, these theories do not address the plight of a person whose civil rights have been violated in cyberspace, as making the defendant subject only to the courts having jurisdiction with respect to his nationality shall be inconvenient for the plaintiff, thereby rendering the plaintiff remediless.

[38] Darrel C. Menthe (n 9)

ROADMAP FOR THE FUTURE

In this section, the author attempts to provide feasible suggestions that can be enforced for better redressal of the jurisdictional challenge cropped out by the use of the Internet on the legal front. United Nations should adopt a ***model law on cyberspace*** jurisdiction and encourage member states to formulate national laws in line with the model law so as to bring about uniformity in national laws governing cyber jurisdiction. Successful cyberspace governance by way of formulation of a model law calls for collaborative efforts between the stakeholders involved, which include the States, international organizations, technical operators, academia, civil society, and Internet platforms. Therefore, the collective approach of various stakeholders must result in the formulation of procedures and norms that establish mutual commitments among the stakeholders while distributing their responsibilities. These norms or policy standards must specify the criteria for decision-making.

In addition to the above, an ***impartial statutory international body*** deriving its authority from the model law on cyberspace adopted by the UN must be instituted to act as a dispute resolution body to deal with the cyberspace disputes that take place between people from different countries. This body may have a minimum monetary slab for purpose of having pecuniary jurisdiction over the dispute. This body shall adjudicate upon cases involving illicit behavior online and breach of commercial transactions that are concluded on the internet. It can have original and appellate jurisdiction. National bodies must be instituted in member states to adjudicate upon national cyberspace disputes and to ensure enforcement of international and national decisions with respect to cyberspace disputes. Since the model law shall be developed through a multi-stakeholder process, it will be based on the consensus of the stakeholders and this will result in successful adoption by the States.

CONCLUSION

Jurisdiction over the internet is a very important area of the law and it is in its nascent stages of development. Though the evolution of international cyber law provides a reasonable basis for cyberspace conflicts, yet there are miles to go before an ideal framework emerges. The

courts are trying to settle and dial down the complexities revolving around jurisdictional challenges posed by the internet. However, there is a lack of effective legislative effort on the international level to handle the unprecedented challenges that internet jurisdiction brings to the table. Moreover, exercising jurisdiction practically consists of exercise and enforcement. The court's intervention is futile unless the decision pronounced against the foreign defendant is enforced. Therefore, the need of the hour is to view the issue of cyberspace jurisdiction holistically and provide redressal with respect to jurisdiction determination in cyberspace conflict as well as a mechanism for enforcement of the decision of the court exercising jurisdiction. The users of the internet are now policing each other and websites often contain a legal disclaimer suggesting the kind of information contained on the site. This self-regulation by creators of websites has helped reduce cyberspace conflicts. However, as the usage of the internet increases, cyberspace management must also become better by the creation of a responsible cyber-community, such that the burden of the courts is reduced. Moreover, addressing Internet governance-related issues needs a paradigm shift: from international cooperation only among countries to trans-national cooperation among all the stakeholders; from purely inter-governmental treaties to policy standards; and from intergovernmental institutions to issue-based governance networks.