ISSN 2582 - 211X

LEX RESEARCH HUB JOURNAL

ON LAW & MULTIDISCIPLINARY ISSUES

VOLUME I, ISSUE IV

JULY, 2020

Website - journal.lexresearchhub.com
Email - journal@lexresearchhub.com

DISCLAIMER

EDITORIAL BOARD

Assistant Editors

ABOUT US

Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) is an Online Journal is quarterly, Peer Review, Academic Journal, published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essays in the field of Law and Multidisciplinary issues.

Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. **Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X)** welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

JURISDICTION: THE ISSUE OVER THE INTERNET

Author –

Sanjita Mittal

Advocate (LL.B, LL.M)

Promod Verma and Associates

ABSTRACT

This article explores the history of Internet contact jurisprudence. It introduces the concerns over the Internet rewriting the law on personal jurisdiction. The article provides a brief analysis of a court's ability to confer jurisdiction over out-of-state defendants through Internet contacts with the help of case laws. Moreover, the article traces a historical trajectory of five different approaches to exercise jurisdiction over the internet. Lastly, the article argues that the exercise of state power through assertions of jurisdiction can and should be used to advance the development of more granular technologies and new service markets for legal compliance.

Keywords - *Internet Jurisdiction, internet safeguards, technological enforcement, out-of-state defendants.*

MAIN PREMISE OF EVALUATION:

The sovereign states are involved in a power struggle to assert and exercise their right to combat illicit internet activities and establish “minimum contact” via personal jurisdiction.

OVERALL EVALUATION:

Judicial ambiguity, differences in legal requirements among sovereign states and inability to transgress constitutionally guaranteed rights of citizens hinder the employment of safeguards in harmonizing judicial effort across the globe.

A. INTRODUCTION

The internet has manifested itself as an indispensable tool and has led to the virtual coagulation of the legal mechanism to cope with its developments marked by separatism and mutually exclusive realms rather than coexisting ones. The ambiguity surrounding jurisdiction limits that can be exercised by public authorities within the legal framework is attributed to the overlapping of laws and its application. The internet has essentially discarded the doctrine of

personal jurisdiction when it pertains to the enforcement of traditional instruments of law to cross-border activities that undermine fair play and substantive justice.

Despite a worldwide scenario of the court's efforts to police such activities in the past by upholding traditional notions by devising principles of minimum contacts and purposeful an ailment, yet the geographical divorce lends an ambiguity as to which jurisdiction would apply. Confronted with these struggles, legal systems seem to be engaged in a conventional fight between existing regulatory standards with new technologies. However, in essence, it is a power struggle of sovereign states to assert and exercise their right to set rules for online activities. Defendants are often witnessed to resort to forum shopping (a colloquial term for the practice of litigants having their legal case heard in the court thought most likely to provide a favorable judgment) to deny the application and ultimately the enforcement of the law which impedes their cause. This leads to an escape from indictment as a "denial-of-service"[1] defense mechanism which can be viewed as a technological assault on the affected state's personal jurisdiction.

The transgression of virtual activities beyond geographical borders have more often than not incapacitated state authorities from regaining jurisdictional control even when the impugned activities' "effects" are primarily witnessed in the forum state. This can be exemplified by the acceptance of the argument by the U.S district court posed by Yahoo! that France was not competent to try a U.S company in French Courts as personal jurisdiction cannot be exercised on images stored on a server in the U.S.[2] The verdict was, however, turned over on account of misinterpretation of a distorted translation of french law in the U.S.

Another example that can be posed pertains to the case of *Lakin v. Prudential Services, Inc.*[3], where the U.S Court of Appeals for the Eighth Circuit wherein the case was remanded for "additional jurisdictional discovery" for lack of evidence corroborating the "nature and quality" of contacts apart from its quantity. Similarly in *ALS Scan, Inc. v. Digital Service Consultants Inc.*[4], the scope of jurisdiction was diminished when the U.S Court for the Fourth Circuit stated that they were not prepared to recognize a state's general jurisdiction over out-of-state

[1] Joel R. Reidenberg, *Technology and Internet Jurisdiction,* 6 UNIVERSITY OF PENNSYLVANIA LAW REVIEW, 1951, 1953 (2005)

[2] Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisémitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

[3] Lakin v. Prudential Sec., Inc., 348 F.3d 704, 711 (8th Cir. 2003).

[4] ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 713 (4th Cir. 2002).

defendants activities which were as passive and inadequate to evoke personal jurisdiction.[5] Moreover, the state authorities are impeded from applying such long-arm statutes when it encroaches on a citizen's constitutionally acquired rights. For example, in the U.S the first Amendment Jurisprudence which warrants a justification of any harm caused by technological enforcement instruments. Similarly, the European Convention for Protection of Human Rights and Fundamental Freedoms, the U.N charter, the Agreement Establishing the World Trade Organisation set substantive obligations for the states to curtail interference of public authorities.[6] However, judicial efforts have evolved and extended to carve out certain approaches to inculcate virtual activities within traditional instruments. They have been discussed below.

B. APPROACHES TO ESTABLISH PERSONAL JURISDICTION

The legal systems across the world have been grappling with developing a protective legal mechanism that is commensurate with technological advancements and its jurisdictional transgression and to bridge the separatism that characterizes it. Over the years, many approaches have shed light on how courts assert personal jurisdiction by perusing the extent and scope of contact with the relevant forum. The following are the approaches and the cases adhering to them.

I. REASONABLENESS APPROACH

Premise: Reasonable Apprehension

It is an exacting approach and restricts personal jurisdiction to defendants which purposely avail themselves of the forum i.e. the court's competence to adjudicate is directly proportional to the extent of the defendant's nexus with the forum state. If users and technologies can be reasonably established then it justifies the state to employ long-arm statutes and assert authority. This approach sets the extremist Inset Approach in motion that is discussed subsequently.

[5] Alan L. Farkas, *Trimming the Claws of The Internet's Jurisdictional Reach,* 46 TORT TRIAL & INSURANCE PRACTICE LAW JOURNAL, 761, 771-772 (2011)

[6] REIDENBERG *Supra note* 1, at 1961-1969

Case/Example:

- ***World-Wide Volkswagen v. Woodson* (1980)**

It was held that a defendant needs to exhibit conduct and connection with the forum state such that he should reasonably anticipate being held liable to suit. [7]

- **Brussels and Lugano Conventions**

The Conventions on jurisdiction for intra-European disputes adopt the above approach and establish forms of contact between defendants and the state asserting jurisdiction.[8]

II. EFFECT APPROACH

Premise: End-point

Traditional public order rules prevalent in the place of initiation of internet activity are often in conflict with the penultimate location of the effects of the impugned activity. But the courts find themselves in a fix to address such issues due to lack of uniformity of the nuances of foreign public order decisions across various jurisdictions. Regulating illicit internet activity becomes all the more challenging when internet participants operate from remote locations and can exercise discretion over their target audience in a location where the impugned activity may be permitted as against prohibited where it is initiated.

Cases:

- ***People v. Worldwide Interactive Gaming* (1999)**

In this case, it was held that an offshore Internet site does not void New York gambling interdiction. As internet technologies are accessed at and by remote locations. The interdicted party themselves make a discretion in conducting their online activities or directing its efforts at the forum state and hence justify the application of personal jurisdiction. [9]

- ***Twentieth Century Fox Film Corp. v. I Crave TV* (2000)**

[7] World-Wide Volkswagen v. Woodson, 444 U.S. 286, 297 (1980).

[8] Convention 88/592/EEC on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, 1988 O.J. (L 319) 9, 10-11 (Lugano Convention); Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, 1978 O.J. (L 304) 77, 79-80 (Brussels Convention).

[9] People v. World Interactive Gaming Corp., 714 N.Y.S.2d 844, 851.

Twentieth Century Fox, a film studio successfully argued "to apply U.S. copyright law to streaming video on the Internet and obtained an injunction against a Canadian service that could legally stream video in Canada.".[10]

- ***Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisémitisme* (2001)**

As aforementioned, even though yahoo was successful in convincing the U.S district court to oust personal jurisdiction from indicting transmission of images of Nazi objects from a server in the U.S, the Court of Appeals, however, overturned the decision and held that the French Courts were well within their right to hold Yahoo! accountable as its ultimate effect was violative of the local laws.[11]

III. INSET APPROACH

Premise: Web Accessibility

This approach raised the spectre of responsibility dramatically and blurred the lines between specific and general jurisdiction. It expanded the area of personal responsibility, giving the court the power to exercise personal jurisdiction on an out-of-state defendant on the discovery of **the mere presence** of a website owned or maintained by the defendant in the relevant forum. This approach was marked with the courts failing to take purposeful or legitimate acts of the defendant into account which was an indicator that this approach was extremist and infinite in reach. Naturally, it gradually lost judicial support.

Cases:

- ***Inset Systems v. Instruction Set* (1996)**

The court held that an out-of-state defendant operating or maintaining a website and a toll-free number was sufficient to establish minimum contact to evoke personal jurisdiction. The case exponentially expanded the reach of personal jurisdiction to the mere presence of websites owned and operated by the out-of-state defendant. [12]

- ***Bunn-O-Matic Corp v. Bunn Coffee Servs. Inc* (1998)**

[10] Nos. Civ. A. 00-121, Civ. A. 00-120, 2000 WL 255989, at *3 (W.D. Pa. Feb. 8, 2000).

[11] Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisémitisme, 169 F. Supp. 2d 1181, 1185 (N.D. Cal. 2001).

[12] Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996).

The court established that the growth of technological advancements should be commensurate with the scope of permissible jurisdiction and ultimately broadened the scope of the clutches of the jurisdictional predicament that employed the inset approach.[13]

- ***Millennium Enters., Inc. v. Millennium Music*** **(1997)**

The court expressed its affliction in supporting the inset approach as it kept the legitimate and purposeful activities of the defendants out of its purview or consideration. Ultimately the inset approach lost its support as being justifiable. It reflects that extremism even in dispensing justice cannot stand the long run. [14]

IV. ZIPPO APPROACH

Premise: Content and level of interaction of websites

This approach fundamentally requires "something more" than just mere internet presence for an internet activity to subsequently yield to personal jurisdiction. Specifically intended activity directed towards the forum state acts as a prerequisite to minimum contacts requirement to evoke "contact" jurisdiction. It identifies a "sliding scale" which comprises three levels of cyber interactivity i.e. 1) commercial, 2) interactive, and 3) passive. These activities differ in the level of interaction between out-of-state defendants and the forum. The level of interaction is directly proportional to the possibility of evoking minimum contact and personal jurisdiction.

1. **Commercial:** Premeditated and repeated commercial transaction connecting defendants with the forum through the defendant's website

Case:

Zippo Manufacturing Co. v. Zippo Dot Com, Inc. **(1997)**

The seminal authority for jurisdictional decisions, the Pennsylvania court identified the above-mentioned levels of interactivity and concluded that since the defendant contacted a large number of individuals and internet service providers, the scale of the operations fell under the category of commercial activity and hence held the defendants liable. [15]

[13] Bunn-O-Matic Corp. v. Bunn Coffee Servs. Inc., 1998 U.S. Dist. LEXIS 7819, at *6 (C.D. 111. Apr. 1, 1998)

[14] Millennium Enters., Inc. v. Millennium Music, LP, 33 F. Supp. 2d 907, 923 (D. Or. 1999).

[15] Zippo Manufacturing Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119 (W.D. Pa. 1997).

2. **Interactive:** This middle tier requires court discretion and depends on variables like interactivity, the extent of contact and commerciality.

Case:

***Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy and Anr.* (2009)**

The Hon'ble Court further went on to say that the Plaintiff will have to show prima facie that the said website, whether euphemistically termed as "passive plus" or "interactive", was specifically targeted at viewers in the forum state for commercial transactions.". The most striking peculiarity of the case was that neither of the parties was located within the territorial jurisdiction of the Court.[16]

3. **Passive:** A passive website merely provides information and no contact or nexus is formed with the relevant forum and any indicted activity is merely incidental.

Case:

***Cybersell v. Cybersell* (1997)**

The court used the Zippo framework to determine that the defendant's website was merely passive on a sliding scale because the interactivity of their website was limited to the name and address of the browser. The only link between the defendant's website and the forum was the accidental access i.e. “hit” by the plaintiff on the site. [17]

This characterization provides the court with a conclusion as to whether or not the defendant purposely availed itself of the benefits of the forum state. This approach is therefore often considered as a seminal authority to establish minimum contact.

V. INTERMEDIARY APPROACH

Premise: Ongoing Business Transactions

Where websites are not owned by out-of-state defendants but are used as intermediary vessels for sales, the issue of personal jurisdiction pertains to the individual rather than the intermediary website. In order to evoke jurisdiction some “ongoing obligations” need to be identified.

[16] Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy and Anr.,(2008),CS (OS) No.894/2008

[17] Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414, 418 (9th Cir. 1997).

Isolated or single business transactions do not suffice to evoke personal jurisdiction by the form state.

Case:

- ***Boschetto v. Hansing* (2008)**

The court concluded that a single transaction cannot be purported to imply that the defendant purposefully availed the business of the forum state through an intermediary website. Therefore, the contract of sale of goods was insufficient to create a substantial connection to the forum state. [18]

C. CHALLENGES TO "EFFECT" APPROACHES

Though technological innovations are viewed as a nemesis of law enforcement, they are a medium to impose liabilities in the virtual world itself to effectively screen and filter the effects of impugned virtual activities that do not comply with local rules. Technology can empower sovereign states to enforce local laws in the absence of the tangibility of the assets of internet participants. Various tools like filters, packet interceptors, hacker tools, electronic blockades equip the states to prevent offenders from operating outside the borders of their jurisdiction or restrict their access to the place of "effect".

As aforementioned, courts fall prey to erroneous interpretation of statutes where intricate nuances of foreign judgments on account of vernacular and legal differences. Vernacular differences, on one hand, are characterized by distorted translation tactics employed by defendants creates a false implication that is not reflected in the original text of the statute. For example, in the Yahoo! case, the company submitted a misleading interpretation of the French Statute omitting the qualifying phraseology. It created an implication that was not aligned with the original text and connoted that the activity undertaken by the company was within legal boundaries. Legal differences across jurisdictions, on the other hand, encourage participants in illicit activities to indulge in forum shopping by operating from states that provide a "legal safe haven". For example, the blanket denial of personal jurisdiction by routing virtual activities

[18] Boschetto v. Hansing (2008) 539 F.3d 1011, 1018 (9th Cir. 2008).

around restrictive laws by locating and conducting such activities within legal safe havens where such activity is permitted. Nonetheless, the sovereign authority has been seen to bring offenders within legal enforcement mechanisms as discussed above.

Apart from the offenders, adherence to the law and due process applies to the state authorities and this restricted leverage of operations often impedes authorities from transgressing legal processes that the offenders have been witnessed to flout. Technological enforcement instruments necessitate legal authorization within the threshold of traditional enforcement instruments. Moreover, the collateral implications/damages are weighed. As technology enables noxious behaviour online, states need mechanisms to sanction virtual activities that violate the citizen's politically chosen rights i.e. chosen rules of law. Therefore, the implications or restrictions on legitimate civilian access should necessarily be least intrusive taking into account the magnitude and urgency of the imminent threat to public order. For example, police searches through faulty search warrants enable the victim to claim redressal for erroneously deploying technological enforcement instruments.

Moreover, counterintuitive efforts taken by the state to combat technological assaults in the virtual realm through technologically-based compliance services and products like filtering technologies or customized security zones that support public values are hindered by the notion that such efforts ultimately are a constitutional challenge. For example, in *Center for Democracy & Technology v. Pappert (2004)* the court concluded that the Pennsylvania statute that enabled web filtering cannot be enforced without violating the First Amendment which guarantees free speech and was ultimately declared unconstitutional.[19]Such technological developments provide little incentive for compliance with state laws without encroaching on data privacy. Ironically, as a result, technologically enforced public policy often faces traction by the public itself which seems to flout ethical internet practices and argues for technical solutions rather than legal solutions to virtual problems like music and film piracy, gambling, hate speech or trolling, etc.

Even the international conventions on the recognition of foreign judgments provide an exception to enforcement when there is a conflict with the public order of the enforcing state. For example, in Antigua's case against the United States, an Antiguan filed a complaint with the WTO alleging that the restrictive internet gambling laws enacted by the U.S violated the

[19] Center for Democracy & Technology v. Pappert 337 F. Supp. 2d 606 (E.D. Pa. 2004).

trade obligations related to cross border services. This reflects that the constraints on the use of electronic borders for enforcement will affect the legitimacy of the rules themselves rather than the mechanism involved.[20]Adherence to customary international laws often undermine and overstep National Internet Policy. Moreover, "communication requirements and preventive obligations" on one hand uphold cooperation but also restrict corrective action.

D. CONCLUSION.

Granular technologies and virtual architecture virtual private networks requiring geographic localization help create jurisdictional safe zones. Technological innovations which create an incentive for internet participants by giving them the discretion to participate in a network and choose permissible network activities by agreeing to take part in contacts to which personal jurisdiction can be exercised. For example, the French Law for Trust in the Digital Economy requires making the clients abreast of filtering technologies and enabling them to report unauthorized content. The revolutionary General Data Protection Regulation (GDPR) is a major step towards winning the battle for jurisdiction. Content filtering technologies like NET Passport prohibits circumvention of technological protections.[21]

Although, as aforementioned such protective mechanisms can combat the blatant disregard for the responsibility of offending virtual acts, the very idea of upholding traditional public policy instruments over technological determinism is the root of apprehension from state authorities to deploy "effect approaches" or technological ammunition. More often than not, judicial ambiguity, differences and inefficacy hinder the employment of safeguards. The judicial effort across the globe can only elusively bridge internet separatism in the absence of a uniform international effort.

[20] WTO Panel Report on U.S. Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/R (Nov. 10, 2004) (ruling on the substantive issue of whether the United States can prohibit offshore gambling), available at http://docsonline.wto.org/DDFDocuments/t/WT/DS/285R-00.doc.

[21] Article 29 Data Protection Working Party, Working Document On On-line Authentication Services, At 4, E.U. Doc. 10054/03/EN WP 68 (Jan. 29, 2003) ("As a result of this very open and fruitful dialogue Microsoft has committed itself to make changes to the system delivering improvements from the data protection perspective."), available at http://europa.eu.int/comm/internal_market/privacy /docs/wpdocs/2003/wp68_en.pdf.