CYBERSPACE AND JURISDICTION

Miss Prevy Parekh[1] *& Miss Tarunya Rao*[2]

INTRODUCTION

The present government is promoting digitalization in full force which is a great step towards the future and transparency. As a part of 'Digital India' the government emphasizes on getting every place in India Internet enabled which will open up tonnes of opportunities, empower E-governance, employment and ease of doing business across the globe from any remote corner. 'Digital India' is where the technology ensures the citizen-government interface is incorruptible. This is vision of every youngster in our country. The world today looks at India for the next big idea. Digital technologies have been increasingly used in everyday life from retail stores to government offices. They help us connect with each other and also share information. One side as a nation we are striving to achieve a 'Digital India', on the other side the scope of crime in cyber space increases. Before stepping into "Digital India" it is important to get policies that would deal with any cyberspace related crimes ready for the future.

Today internet has revolutionised, its reach is far more than any other of communication. But with this novelty also comes great risks where this boon called the internet can also be misused and hence giving rise to many criminal activities and instances of abetment of criminal activities which have to be regulated. The basic nature of the internet is that it is endless and has no boundaries. This is a primary characteristic of the internet and poses as a severe problem when one speaks of the issue of jurisdictions.

Jurisdiction is the concept where by in any legal system, the power to hear or determine a case is vested with the appropriate court. The main problem of cyber law jurisdiction is the presence of multiple parties in various parts of the world who have only virtual nexus with each other. Then the problem of place is raised that where the party wants to sue and what remedy is available to him?

[1] 3rd Year BBA LLB , SLS, Pune

[2] 3rd Year BBA LLB , SLS, Pune

Now cyber security has become an integral part of national security. Today computers play a major role in almost every crime that is committed. The applicability and effectiveness of our existing laws need to be constantly reviewed so that we can ably face the risks at present. Currently in India we have the Information Technology Act, 2000 (also called, IT Act, 2000) which is an enabling provision for regulating the activities that take place in cyberspace.

Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet. As such, a single transaction may involve the laws of at least three jurisdictions:

- The laws of the state/nation in which the user resides,
- The laws of the state/nation that apply where the server hosting the transaction is located, and
- The laws of the state/nation which apply to the person or business with whom the transaction takes place. So a user in one of the states in USA conducting a transaction with another user in Australia through a server in Chennai could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Jurisdiction is an aspect of state sovereignty and it refers to judicial, legislative and administrative competence. State sovereignty as defined by the Merriam-Webster dictionary is the "a country's independent authority and the right to govern itself"[3]. Although jurisdiction is an aspect of sovereignty, it is not coextensive with it. Just because a country has its sovereignty (both internal and external) intact does not mean it has unlimited jurisdiction over all sorts of issues. International law limits a state's right to exercise jurisdiction.

The internet today is making a complete mockery of the law not just the traditional laws but even the so-called modern laws. The very basis of any justice delivery system, the jurisdiction, which gives powers to a particular court to accommodate a particular case, is itself being threatened over the internet; leave alone the other traditional laws.[4] The paper aims at how the challenge of jurisdiction (national and international) is to be combated with

[3] Simple dictionary meaning of Sovereignty as per the Merriam-Webster Dictionary.
[4] Yashraj Vakil, "Jurisdictional Challenges – Cyber Crime Prosecutions", The Lawyers Collective, February, 2005, p. 29

regard to cyber law in India. The paper also aims at discussing the plausible alternatives of dealing with issues regarding cybercrime like arbitration.

INFORMATION TECHNOLOGY ACT, 2000

Through the Fifty First Amendment the Indian Parliament has enacted an Act called the Information Technology Act 2000.[5] The primary aim of the parliament in making this law was to recognize e-commerce and growing use of internet. The act aimed at meeting with future legal problems that might arise due to the rapid increase in use of the internet. The Indian Parliament captured the spirit of the General Assembly's recommendations dated 30 January 1997 in the **United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model)** in the form of The IT Act 2000[6]. The basic principles of the Model Law were:

- To facilitate rather than regulate electronic commerce.
- To adapt existing legal requirements.
- To provide basic legal validity and raise legal certainty.

The Act facilitates international trade and acts as alternative to paper-based methods of communication and storage information as it facilitates E-commerce and E-governance in the country. It establishes a regulatory framework in the country also lays down punishment regimes for different cybercrimes and offences.

The extent of the application of this act is stated in Section 1(2). **Section 1(2)**[7] of IT Act 2006 states:

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

It can be understood that the act applies to any offence or contravention committed thereunder outside India by any person. It can be seen that sub-section (2) highlights the extra-territorial jurisdictional power of the nation over the wrong doer, irrespective of his

[5] It received the presidents consent on 9th June 2000
[6] B.M.Gandhi. Indian Penal Code. India: Eastern Book Company. p. 41. ISBN 9788170128922.
[7] Information Technology Act, 2000

nationality, domicile, status etc. But to completely understand Sub-section 2, one should read it with Section 75. **Section 75**[8], IT Act, 2000 reads:

Act to apply for offence or contravention committed outside India.-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an 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.

Therefore, Section 75 of the IT Act, 2000 states that the act applies to any offence or contravention committed outside India by any person irrespective of his nationality [S.1(2)], if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India[9]. For domestic suits and cases the act established a Cyber Appellate Tribunal, which is defined in Section 2(1)(n). This Tribunal has been established under Section 48(1).

The relevant clauses of **Section 2(1)**[10] read:

(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48.

(na) "Cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

(nb) “Cyber Security" means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Section 48(1)[11] reads:

Establishment of Cyber Appellate Tribunal. – (1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

[8] Information Technology Act, 2000
[9] Information Technology Law and Pratice , vakul Sharma III Edition (2011)
[10] *Ibid*
[11] *Ibid*

Jurisdiction may be defined to be the power or authority of a court to hear and determine a cause so that they can adjudicate and exercise any judicial power in relation to it. In other words, jurisdiction means the authority which the court with regard to deciding of matters that are litigated before it or to take cognizance of matters presented in a formal way for its decision.

Hence, the IT Act, 2000 makes provisions for a person to protect his cyber rights by the creation of the Tribunal. Like mentioned earlier, the act in its inception was made with a futuristic approach, but it failed due to the unforeseen rapid growth of the internet. The rise of online marketing, e-commerce, e-banking and other such online portal have given a gateway for a new array of crimes, cybercrimes. The question is whether the prevalent laws are capable enough to deal with the basic complexities of the cyberspace like jurisdiction.

JURISDICTION AND CYBERSPACE

Traditionally where the cause of action arises is where the jurisdiction lies, but how to determine when there are multiple parties involved in varied parts of the world. There are three parties to a transaction that takes place in cyberspace namely, user, service provider and person/business with whom the transaction takes place therefore ideally the most efficient law must address whether a particular event in cyber space is controlled by the laws of the state or country or where the user is located or application of all the other countries' or states' laws.

Unlike in the conventional way, there are three parties to any transaction in the cyber space. The User, the server Host and with whom the transaction is taking place with.[12] The primary issue is, which country's law should apply? Hence, the key issues that can identified are

- When there is cross border interactions on what basis do we decide which country's law applies and which court has jurisdiction?
- What are the basis on which nation can claim to apply laws and regulations if the internet activity originate from different jurisdiction.[13]

[12] Anupa P kumar, "Cyber laws" , Mr.Anupa Kumar Patri, 2009
[13] Chris Reed, "internet law test and materials" Universal publishing Co.Pvt.Ltd 2005 p.217

Therefore Matters of jurisdiction is subject of state and International law when the contracting parties or parties in dispute are of different nationals. Under international law the state is subjected to application of its law when there are international parties to dispute.

There three kinds of jurisdiction that exists in matters of determining a country's jurisdiction under international law. These are, prescriptive jurisdiction, jurisdiction to adjudicate, jurisdiction to enforce.

- **Prescriptive jurisdiction**

It is the jurisdiction of the state to make laws applicable to person and certain circumstances, however international laws exercises limitation on states authority to prescribe laws if there is a conflict of interest with another state.

- **Jurisdiction to Adjudicate**

It is the power of the state to subject a person or things to courts or administrative tribunals either civil or criminal, whether or not the state is party to the proceedings. If there exists sufficient relationship between the state and the person.

- **Jurisdiction to Enforce**

Is the power of state to induce or punish for noncompliance with laws and regulations. However a state's law can be enforced by the officers with due permission of the state officials concerned. From arrest to producing documents and police arrest cannot be conducted without consent. However there may be circumstances where the state may have jurisdiction to prescribe but jurisdiction to adjudicate is absent. In criminal cases especially jurisdiction to adjudicate does not exists without jurisdiction to adjudicate because courts do not apply criminal laws of other states.

Personal jurisdiction is jurisdiction over the persons or entities involved in the lawsuit. One way to think about personal jurisdiction is to ask the following question: "What right does a court have to determine the rights of the parties involved in the action?" In other words, the question of whether a court has personal jurisdiction over a person involves the question as to whether it would be fair for the court to issue a judgment against that person. The element

that must be satisfied for a court to have personal jurisdiction is the law that governs the court must give it authority to assert jurisdiction over the parties to the case.[14]

India, like the US follows the principle of the 'Long Arm Statute' to decide in matters of personal jurisdiction on the international front. Further we will discuss the concepts of Long Arm Statute, Minimal Contact in regard to personal jurisdiction for disputes based on cybercrime. Though India is not one of the signatories to the cybercrime convention, which will be explained later, but it has adopted principle of universal jurisdiction to cover both the cyber contraventions and cyber offences under the Act. It has been argued that from the point of view of application, it would be extremely difficult to enforce the jurisdiction of Indian Courts on cyber criminals belonging to different nationalities. Moreover, the Extradition Treaties, which India has signed so far, do not cover 'cybercrime' as an extraditable offence.[15]

LONG ARM STATUTE & MINIMUM CONTACT

What makes for minimum contact? Minimum contact rule establishes that so long as a corporation had a degree of contact within the state bringing suit, they are subject to the laws of the state and can be sued by and within the forum[16] state in court. This is not exactly black and white. The law says minimal, or very few contacts, are enough to establish contact. But there is also a right to fair play and substantial justice, which sets three distinct factors needed to extend long arm statute jurisdiction to bring a defendant corporation to court:

- Closeness of the relationship between the claim and the contact
- Convenience of bringing the defendant corporation to the forum state
- State has an interest in protecting the rights of its citizens

To put this all together, minimum contact rule may apply so long as it does not interfere with fair play and substantial justice. This method is often used as a method to decide whether the long arm statute can be used to award personal jurisdiction to a certain state for disputes in the international front. This concept is now being followed by India too as the prevalent laws are not enough to define and clarify the jurisdiction issue when it comes to cybercrimes

[14] Available at http://nationalparalegal.edu/public_documents/courseware_asp_files/researchLitigation/Jurisdiction/PersonalJurisdiction.asp (Last accessed on 26/06/2016)

[15] 'Cyberspace Jurisdiction and Courts in India' by Dr. Ravishankar K. Mor, Asst. Prof., Dept. of Law, Yeshwant Mahavidyalaya, Wardha

[16] Particular court or jurisdiction which has rightful jurisdiction

alone. The provisions of Section 1(2) when read along with Section 75 empower the court with the long arm jurisdiction which is absolutely necessary.

But what is this 'Long Arm Statute'? In the simplest of words it refers to the jurisdiction a court has over out-of-state defendant corporations. **International Shoe v. Washington**[17] was a landmark case that set precedent for establishing the right for government to use the long arm statute to bring an action against a defendant corporation. Long-arm statute went a step ahead of 'minimum contacts' to look into whether the contacts were sufficient to establish "purposeful benefit", like:

- Purposefully and successfully solicitation of business from forum state residents
- Establishment of contract with the forum state residents
- Associated with other forum state related activity
- Substantial enough connection with the forum state [18]

Once the court determined that sufficient 'minimum contacts' existed to exercise specific jurisdiction over the defendant, the court then would have to consider whether it was reasonable to subject the non-resident defendant to the personal jurisdiction of the forum to the extent that federal constitutional requirements of due process will allow. The importance of the International Shoe Company's case is that it established for the first time that personal jurisdiction might exist even though the defendant had no physical presence in the forum state. It acted as a precursor to the state's long-arm statutes. Later, with the advent of e-commerce, this judgment has been used by the courts all over the United States as an established law in identifying "minimum contacts" to claim personal jurisdiction over a non-resident.

If a corporation or party located in one state/country does business in another state and employs people in yet another state/country, they just may fall under the long arm statue. Therefore the long arm statute basically allows a state to exercise jurisdiction over out-of-state defendants, provided that the government can prove that the defendant has at least minimum contacts in the affected or forum state. This means, if a corporation was to be sued in a country that they do not actually do business or use the cyber services in, in this case, but have a connection to the state(affected the computer systems of that state) the party is

[17] 326 310 (1945; 1945 U.S. Lexis 345)
[18] International Shoe Co. v. State of Washington, Office of unemployment Compensation and Placement et al, 326 U.S. 310, 316 (1945); See also Hess v. Pawloski, 274 US 352 (1927)

considered to have minimum contact sufficient enough to be sued within the forum state. However, in **Cybersell, Inc. V Cybersell, Inc.**[19], a case is related with the service mark dispute between two corporations, one at Florida and another at Arizona. The court held that the effect test does not apply with the same force to a corporation as it does to an individual "because a corporation does not suffer harm in a particular geographical location in the same sense that an individual does.

Yahoo Inc. *vs* Laligue contre Le Racism EL, Antisemitisme[20] popularly known as the Yahoo case which highlights the jurisdictional issues in cyberspace is another landmark issue in this subject. The facts of the case were on the lines that the union of French students and International League against Racism and Anti-Semitism filed a suit against yahoo for hosting auctions that displayed and sold Nazi propaganda. Yahoo argued that the French court did not have jurisdiction. However this was denied and yahoo did not go for an appeal rather challenged the enforcement of the order in United States. In mean time the French courts claimed for dismiss of declaratory judgement, the U.S court however ruled that jurisdiction existed based on the Effect Theory. The effects theory is in simple words, A doctrine, developed mainly by the American courts in anti-trust cases, asserting jurisdiction over acts of foreign nationals committed abroad but having effects in the American marketplace; an extended form of the objective territorial principle.[21]

A state can only enforce Laws in a forum where the defendant can be found or where assets of the defendant belonging to him can be found. Enforcement of judgement rendered by another court requires recognition by another court to enforce it. In United States a Principle of Comity is followed. Comity is the recognition which one nation allows within its territory to the legislative, judicial and executive acts of the other state. However procedures may vary widely across the globe. The principle of comity is followed unless there is a violation of due process, personal jurisdiction and public policy. In simpler words, the principle that one sovereign nation voluntarily adopts or enforces the laws of another sovereign nation out of deference, mutuality, and respect is what the Principle of Comity is. For example if India uses a judgement passed in the US regarding a matter of cybercrime it follows the Principle of Comity. India is not constitutionally bound to follow the US, but it does so out of deference, mutuality, and respect.

[19] (1997)130 F.3d 414
[20] 169 F.Supp 2d 1181,2001
[21] Irwin Law Inc, May, 2008, 634 pp, Public International Law 2/e, By John H. Currie

POSITION IN EUROPEAN COUNTRIES

The **Brussels Convention**[22] does not require minimum contact between the state and the defendant. The convention permits assertion of jurisdiction if the plaintiff suffers from tort injury within the forum.

POSITION IN INDIA

Unfortunately, only a very few cases concerning personal jurisdiction in cyberspace have been decided by the superior courts in India. The reason perhaps is that residents in India have not yet accepted or adapted themselves to this new technology as a fit mechanism to undertake legal obligations (coupled with an extremely slow justice delivery system). The approach adopted is similar to the ‘‘minimum contacts’’ approach of the United States coupled with the compliance of the proximity test of the Procedural Codes in India.

The term *‘Lex Fori’* literally means the law of the forum or the law of the jurisdiction where the case is pending. The exercise of jurisdiction is regulated by the procedural laws. Procedure is the judicial process for enforcing rights and duties recognized by substantive law and for justly administering redress for infractions. Procedure involves all aspects such filing of suit, collection of evidences, enforcing of judgements.

Jurisdiction under Indian laws is dealt with through the civil law, Civil Procedure Code, 1908. The sections that deal with jurisdiction involve Section 6 of the CPC which deals with pecuniary jurisdiction, while Section 16 states subject matter jurisdiction. Section 19 deals with suits for movable property and Section 20 states where the defendant resides or cause of action arises, in other words territorial jurisdiction.

In the case of **Rajasthan High Court Advocates Association vs Union of India**[23]**,** the Supreme Court defined cause of action as every fact which is necessary for plaintiff to prove, if traversed in order to support his right to the judgement of the court. If, for instance due to a transaction cause of action has arisen in Hyderabad wholly or partly the courts would have jurisdiction if the defendants reside in India or anywhere else.

The problems that arise with respect to Section 20, which talks about territorial jurisdiction is when parties are located in different jurisdictions, medium of communication is in different

[22] 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters.
[23] 2001 2 SCC 294

country, or also when under certain jurisdiction of a country certain act is an offence while in another country it is not.

Section 20 of CPC[24] states:

Other suits to be instituted where defendants reside or cause of action arise.- Subject to the limitations aforesaid, every suit shall be instituted in a Court within the local limits of whose jurisdiction—

(a) The defendant, or each of the defendants where there are more than one, at the time of the commencement of the Suit, actually and voluntarily resides, or carries on business, or personally works for gain; or

(b) any of the defendants, where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case either the leave of the Court is given, or the defendants who do not reside, or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution; or

(c) The cause of action, wholly or in part, arises

Another way to decide jurisdiction is agreement between parties, parties by agreement can confer to one jurisdiction and exclude the rest. The Indian law recognises and give effect to the autonomy of parties.

JURISDICTION OF INDIAN COURTS OVER FOREIGN CITIZENS OR PERSONS

Section 16 of the code[25] states that:

"Subject to the pecuniary or other limitations prescribed by any law, suits-

(a) For the recovery of immovable property with or without rent or profits,

(b) For the partition of immovable property,

(c) For foreclosure, sale or redemption in the case of a mortgage of or charge upon immovable property,

[24] Civil Procedure Code, 1908
[25] *Ibid*

(d) For the determination of any other right to or interest in immovable property,

(e) For compensation for wrong to immovable property,

(f) For the recovery of movable property actually under distraint or attachment, shall be instituted in the Court within the local limits of whose jurisdiction the property is situate:

Provided that a suit to obtain relief respecting, or compensation for wrong to, immovable property held by or on behalf of the defendant, may where the relief sought can be entirely obtained through his personal obedience be instituted either in the Court within the local limits of whose jurisdiction the property is situate, or in the Court within the local limits of whose jurisdiction the defendant actually and voluntarily resides, or carries on business, or personally works for gain."

Therefore Indian courts cannot assume jurisdiction over immovable property located in foreign countries.

Section 19 of the code[26] states that

"Where a suit is for compensation for wrong done to the person or to movable property, if the wrong was done within the local limits of the jurisdiction of one Court and the defendant resides, or carries on business, or personally works for gain, within the local limits of the jurisdiction of another Court, the suit may be instituted at the option of the plaintiff in either of the said Courts."

ENFORCEMENT OF FOREIGN JUDGEMENT

In India foreign judgement can be enforced in two ways

- Reciprocating Territories
- Non-reciprocating Territories

Reciprocating Territories

If it is a reciprocating territory it can directly enforced by filing for an executive decree. Reciprocating territory" means any country or territory outside India which the Central

[26] *Ibid*

Government may, by notification in the Official Gazette, declare to be a reciprocating territory for the purposes of this section; and "superior Courts", with reference to any such territory, means such Courts as may be specified in the said notification.[27] Countries like Canada and UK are reciprocatory countries.

Non Reciprocatory Countries

Judgements from a non reciprocatory country can be enforced in Indian courts only by filing a law suit. The foreign judgement is considered as evidence.

CONVENTION OF CYBER CRIMES

As already analysed different countries have different laws governing them when it comes to Cybercrimes. Different techniques followed all around the world do not help dealing with these transnational crimes at all. Hence another attempt to solve this jurisdictional issue was made in 2001 in Budapest when the Convention on Cybercrime[28] was adopted by the Council of Europe and other non-member countries. The Council of Europe, which is not an organ of the European Union, was founded in 1949 to promote human rights, democracy and the rule of law in Europe[29] The signatories to this convention include major non- member countries such as the US and Canada who have ratified the convention.

The convention of Cybercrimes was adopted by the council of Europe in 2001; it came into force in the year 2004. It is the first and only International treaty to deal with breaches of law over the Internet and other information technology related crimes. The convention aims at protecting the confidentiality, integrity and preventing misuse of computer systems, networks and data.[30]Since several the big nations across the globe are members to this convention and it is the only convention on cybercrimes there is a need for India to ratify this convention as this is the closest that there is to a legal framework that could probably be considered a global standard. On the hind side Russia, China and India are not signatories to this convention as it threatens the absolute sovereignty of countries. Russia has out right claimed this to be their

[27] Civil Procedure Code, 1908, Sec.44A
[28] Convention on Cybercrime, Budapest, 23/11/2001, CETS No.185
[29] A Global Convention on Cybercrime? by Brian Harley, March 23, 2010. Published in The Columbia Science and Technology Law Review.
[30] Preamble, Convention on Cybercrime, Budapest, 23/11/2001, CETS No.185

reason for not signing the treaty and said declared its non-cooperation for any law enforcement investigations relating to cybercrime.

CONCLUSION

International jurisdiction is an ever persistent issue that has been prevalent not only in cyber law but in several legs of law. It is unavoidable and extremely sensitive an issue because of the simple reason of world politics and diplomacy. There is not much anybody or country can do as there is such a great irreconcilable difference in each country's stand. Cooperation by countries is the basis for any of the current methods of tackling jurisdiction will work. What the flaw with these is that they all depend heavily on country cooperation. Hence the authors of this paper suggest creation of a separate dispute resolution body that specially deals with cybercrime. The decision of this body should be binding on the parties that approach it. The dispute resolution should work on basis of the guidelines that have already been provided by the UNCITRAL rules. It is extremely important that a strong body similar to the WTO (World Trade Organization) is made so that a permanent solution is found to this issue of problem of jurisdiction and international cooperation. The UNCITRAL rules in accordance with the rules of the Cybercrime Convention together should act as a strong guideline for the making of such a body.

This solution will also allow the countries to do away with problem of extradictory crimes. Even if the present state of knowledge and understanding of cyberspace and legal issues related thereto does not permit a detailed law on this subject of jurisdiction, for aspects on which no consensus may be reached, an international monitoring or regulatory body with some binding authority may be assigned the task of analysing, etc. rules of cyber jurisdiction. Such a body may, on the lines of UNCITRAL etc.[31] may propose and adopt certain model laws for the states to base their domestic legislations on, Still other aspects may have to be inevitably left to the domestic courts to rule upon since it is only in a real factual situation that issues which could not be contemplated will arise, requiring courts to adjudicate upon the legitimate interests of the parties. Expecting a comprehensive treaty based solution on all possible issues is unrealistic and also undesired for cyberspace is only a few decades old and a number of more complex issues are yet to surface. And, to decline to act merely because a

[31] The UNCITRAL Model Law on Arbitration sets a valuable precedent as it forms the basis for domestic legislations in a number of states, including India.

comprehensive agreement looks difficult is to act contrary to the collected wisdom from the past.

SUGGESTIONS

- An impartial body that acts as a dispute resolution body to deal with the cyberspace disputes that take place between people from different countries.
- All domestic cyber disputes should be tackled by the domestic courts of the various countries in accordance with their own laws.
- An international monitoring or regulatory body with some binding authority may be assigned the task of analysing, etc. rules of cyber jurisdiction should be made that has binding control over the countries.

On a concluding note, the internet is big, vast, complex and here to stay. Our traditional methods of legal systems have miserably failed in front of technology. Instead of altering our current systems and trying to find a method that is new, innovative and a kind where all have to compromise a little so that the compromise can be used for a greater good of justice and equity.

Coming back to how we started off, the 'Modi Government' has been propagating the use of internet and making the government's resources and documentation all online and easily accessible by all. As brilliant and forward as this idea is, it can become equally dangerous and a potential inspiration for greater cybercrime. While it is a great step towards becoming a more transparent and greater democracy it also invites and makes it easier for cyber terrorism, this calls for greater cyber security. Several unforeseeable cybercrimes will come to rise which will need immediate attention which they come and at that moment solving issues like jurisdiction will only slower the process and create a snowball effect making things worse. If digitally advancing countries, such as India, fail to establish an efficient legal framework, then the jurisdictional problem of cybercrime legislation will continue to threaten state sovereignty.