Regulating Cyberspace: The Emerging Problems and Challenges

K. Vishnu Konoorayar*

The term ‘cyberspace’ was coined by the science fiction writer William Gibson in his short stories and novels to denote the separate space created by Internet¹. Internet² was developed in the 1960s by United States of America for its military purposes. Their main intention was to avoid any loss of military information. With its decentralized nature, if any part of the network is destroyed, the information already stored into other parts of the networks can easily be saved³. By the beginning of 1970s the universities and academic institutions in United States had begun to use this network of computers. Later on, when the business community understood the real potential of this network in the area of communication, they also began to use the Internet. For them it was the fastest and cheapest way of communication. In the beginning of 1990s, the Internet turned into a virtual super market. Every type of goods and services were available on the net, on different terms and conditions. Gradually with the advent of e-commerce, e-advertisement, and e-banking, the notion of the competition that grasped the physical world affected the Internet also. Many websites were hacked and destroyed, pornographic and other illicit information were flown freely, many highly reputed persons were defamed by anonymous persons, and thus trademarks and copyrights were grossly

* LL.M. (Cochin); Guest Lecturer, Centre for Legal Studies, Kannur University, Palayad, Thalassery, Kerala.


2. Internet is defined as a “vast web of interconnected networks with each network being connected to many different computers, including home computers via telephone lines and modems.” Matthew Oetkar, “Personal Jurisdiction and the Internet,” 47 Drake Law Review 613, 619 (1999).

infringed. As a result, the consumers of e-commerce were searching in darkness to find out appropriate forum to get damages.

The term ‘cyberspace’ entered into the arena of law, when the American Supreme Court, compared the breach of law in cyber space to the breach of law in real space. The Court applied the laws of the real world to the cyber space. After this judgment the jurists of the cyber space were divided into two groups. One group argues that the laws of the real world can be extended to the cyberspace. The other group says that the territory based traditional laws cannot be applied to Internet. This study intends to analyse these two lines of arguments and examine the emerging problems and challenges which are to be addressed by the law and its techniques.

To understand these conflicting issues it is necessary to look into certain fundamental characteristics of the Internet and how Internet differs from other methods of modern communication.

**Absence of Geographical Boundaries and the Problem of Anonymity**

The cyber space has no real connection with the real space. It cannot be divided on the basis of physical boundaries. Beyond the cables, telephone lines, satellites and computers that are known as ‘backbones’, the internet has no connection with the real world. Away from these backbones, the Internet creates a separate world, which is built of passwords and electronic data. The place of the residence of the defendant or the cause of action of the suit, which are the traditional basis for fixing jurisdiction, cannot be established with certainty in the Internet. Even a childish act can create a confusing issue of jurisdiction on the net.

---

5. They are spread out everywhere, in land, sea and space, which may or may not come within the control of any legal system. These are owned by different entities under state and private control.
6. For example consider a case where ‘A’ in India, decides to download an article from a website and pays money for it through a credit card. He may not be able to perform the download because of the fault of the server. The (f.n. contd. on next page)
In the Internet, the sender of an information cannot necessarily be presumed to be who he or she is. It is also not always possible for the sender to know the recipient’s true identity. Graham Greenleaf explains the problem of anonymity in cyberspace with the help of a cartoon, which appeared in the New York Magazine. In this cartoon, two dogs are sitting in front of a computer. One dog says to the other: “On the internet no one knows that you are a dog”. This interesting cartoon shows the difficulties in bringing Internet activities within the clasp of present legal system. So it has been rightly pointed out that ‘a user’s digital identity has no connection with his physical world identity.’

In some cases, this uncertainty as to identity do not raise problems. But when the dealings are having legal consequences and financial effects, the party cannot be satisfied of having merely an e-mail address as to the identity of the opposite party. The existing identification tools become a failure here. As it is aptly observed that the technology is creating new

money is already withdrawn from the bank by the website owners. He may desire to sue the owner of the site. But the owner is in England and the site is based in USA. This would create practical difficulties in applying the traditional legal principles to the Internet.

7. With the use of cyberspace architecture such as cookies, it may be possible for him to identify the user’s computers in some way, but the user may be browsing the net from the Internet cafe. It is also not possible to identify persons behind a domain name. The domain name might be abc.com, which offers to sell some valuable material, if credit card number is given. This address of the firm could be fictitious. Don Gosselin, Java Script, Vikas Publishing House, Delhi (2000), p.406.


10. For example when a man is simply browsing the Internet to hear some music, which is free, he is not interested in the website’s physical address. The website is also not interested in the users true identity.

11. One method of identifying a correspondent is to use the identity information supplied by that person. If a user is viewing a website, a form can be used which requires the user to input identification details. The drawback of this (f.n. contd. on next page)
areas in law. When the new technologies converge, the legal principles are either absent or imperfect. The application of the law to the new emerging situation provides many loopholes through which the culprits can easily escape.

The development and enforcement of legal rules are logically based upon a number of related considerations like power, effects, legitimacy and notice. If any single state makes any law for the Internet, system is that it requires the information provided by the user to be taken on trust. Even when it is trustworthy, or can be considered as trustworthy, the question of proving it in a court of law is a major hindrance. Most of the legal systems, with the help of advanced technology are trying to solve this problem at least in commercial transactions. Many legal systems have given validity to identification tools such as electronic signature and ID certificates. E.g., see the Singapore Electronic Transaction Act, 1998; The (US) Uniform Computer Information Transaction Act, 1998; The (Indian) Information Technology Act, 2000.


14. Control over physical space, the people and things located in that space is an attribute of sovereignty and statehood.

15. Law makes some mechanism for its enforcement, which include the ability to exercise physical control over and to impose coercive sanction on law violators. One country cannot and should not have law enforcement machinery in another country.

16. The Indian law making bodies do not have the legitimacy to adopt laws for another country. In Internet cases the courts may need legitimacy for their decision in other country also. The absence of legitimacy makes the enforcement of the decision difficult.

17. In real space, if a person travels from one country to another, he knows that he should obey the laws of the host country and not that of his own country. In the cyber world no one gives any warning, as to the area, which he is travelling. He does not see any signal board and no one gives him any notice. When he is browsing the net, he normally does not understand the legal system of the host website. He may be browsing two or more similar websites at the same time, and does similar activity in all those websites. But with regard to all those websites his rights and duties are different, even though, he has no notice of the same.
the concept of sovereignty is lost. According to Johnson and Post, ‘the correspondence between physical boundaries in law space reflects a deeply rooted relationship between physical proximity and the effects of any particular behaviour’\(^\text{18}\). Elizabeth Longworth, says that, ‘the ability to impose sanction on law violator is fundamentally constrained by the need of physical proximity and physical control.’\(^\text{19}\) Johnson and Post describe these difficulties in the following words:

“While these electronic communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the real world of atoms emerges. This new boundary defines a distinct cyberspace that needs and can create new legal institutions of its own. Territorially based law making and law enforcing find this new environment deeply threatening.”\(^\text{20}\)

Absence of physical boundaries in cyber space may lead to a situation where the basis of morality and culture will be shaken in a society. The morals of a society could vary from the morals of another society. The Internet being a global communication media can encroach upon the morality of a society. An example is the publication of obscene materials on the Internet. The Indian law makes the sale of obscene materials punishable\(^\text{21}\). With the advent of Internet, people can view and download obscene materials irrespective of their age. Even if the true address of the host website is known, an Indian court cannot punish the offenders who are in a foreign country. The publication of obscene materials may not be an offence in the country where the server of the host web site is situated. The criterion for punishment varies from countries to countries. For instance

---

in USA the obscenity test is based on the ‘contemporary community standards’ of the nation. There is no barrier to publish any material which matches their contemporary community standards.

These peculiar characteristics of the Internet make the problem much complicated to the legal systems, especially on jurisdictional issues.

**Jurisdiction of Internet Cases**

The effectiveness of a judicial system rests on bedrock of regulations. Regulations define every aspect of a judicial system’s functioning. But a court must have jurisdiction, venue and appropriate service or process in order to hear a case and render an effective judgment. The many issues on Internet cannot be managed by the existing principles of jurisdiction. The courts all over the world are facing the difficulty in finding out solutions to the Internet litigations. The most difficult question is with regard to the jurisdiction. In the physical world the principles for establishing applicable law and deciding jurisdiction in cross-border litigations were established many years ago. But because of the special characteristics of the Internet, these rules cannot be applied in fixing jurisdiction of Internet cases.

---


24. Principles of private international law decided these matters by deciding in which geographically limited jurisdiction the relevant element of transaction can be included. Cases like *Pennoyer v. Neff* 95 U.S.714 (1877), *International Shoe Company v. State of Washington*, 326 U.S.310, *Helicopters Nationals De Columbia v. Hall*, 466 U.S.408 (1984), *Burger King Corporation v. Rudzewics*, 471 U.S.462, the judiciary have brought the concepts of physical presence and minimum contact. Almost all the statutes of the developed legal systems base the provisions of jurisdiction upon the residence of the defendant or the place of cause of action. So from judicial decisions as well as statutory law it is clear that the wrong doer must have some physical contact with the real world to establish jurisdiction.
a) *Jurisdiction in Civil matters*

The problem of jurisdiction in contractual obligation is an important aspect to be looked into. In the Internet contract, if the parties can be properly identified and they chose a particular national law by which they would be governed, the forum will be that particular State. Hence in *Compu Serve v. Patterson*<sup>26</sup>, the parties decided to be governed by the law of State of Ohio. The Court in Ohio did not hesitate to decide that particular case. But the laws with regard to the jurisdiction when the parties do not choose a forum state are still unclear. Indian jurisprudence with regard to the jurisdiction over the Internet is almost non-existent.<sup>27</sup>

In India except, on a few occasions, foreign judgments are binding on Indian courts. This position of law assumes importance when a foreign judgment in Internet case is to be enforced. The main argument on the behalf of the defendant would be that a foreign court has no jurisdiction to try the matter. He might argue that the judgment was arrived at in his absence and the judgment is not enforceable. However, the Indian judiciary in such an instance has held that these reasons are not valid.<sup>28</sup> On the

---

25. Under the traditional law, where both the parties are located within the territory of the same state, the contract law of that country will govern the issue. If the parties are located in different jurisdictions, there is choice of law rules that govern which law would properly apply to the dispute. When the parties include in their contract the choice of law, then it is applied. When the parties keep silence as to the place of jurisdiction in their contract, the court normally consider factors such as the law of the country, which is having 'closest connection with the contract'.


27. The reasons for this seem to be existence of the strong unitary characteristics of the Government in India. This makes the application of private international law useless. Once a judgment is arrived in any of the state in India, the enforcement is determined based on the procedural laws like the Code of Civil Procedure, 1908, and the Code of Criminal Procedure, 1973. Unlike in America the application of law is not based on the principles of private international law. The above said statutes in India have the provisions with regard to jurisdiction.

basis of this principle, the courts in India would not have any hesitancy to enforce any foreign judgment. In India a suit in respect of immovable property or in respect of movable property that is actually under attachment, is required to be instituted in the court within whose local jurisdiction, the subject matter is situated.29 In an Internet case when the property is situated in a foreign country, this provision becomes irrelevant. Another provision says that a suit for the compensation of the wrong done to person or to movable property, may be instituted either at the place of residence of the defendant or at the place where the wrong was committed.30 Has this provision got any relevance in the overwhelming Internet cases?

b) Jurisdiction in Criminal matters

Since Internet is everywhere, the commission of a crime can take place anywhere on the Internet, due to which the Internet user finds, the subject matter of the jurisdiction of many countries for a single act. Occasionally this may lead to a situation where a person is subject of an extradition request from many countries. Ordinarily the jurisdiction of a court relates to the place where the offence is committed.31 This is based on the English common law position that all crimes are local and should be tried only by the local courts within whose jurisdiction the act was committed. When there is uncertainty as to the local area within which the crime was committed, the courts within whose jurisdiction even a part of the offence was committed have jurisdiction to try the matter. This will result in a situation, where the prosecutors of many jurisdictions have a choice of forum as to the trial of offences.

Computer Crime, Cyber Crime and Internet Crime

The criminals can commit a crime in the cyber space and have its impact in the real world with less expense and with less manpower
compared to the real world.\textsuperscript{32} The statistics show that the crime on the net is exploding at 4.2\% every week.\textsuperscript{33} Nowadays India is also a victim of the crime committed in the cyberspace.\textsuperscript{34}

There are three words that are used by authors synonymously—cyber crime, computer crime, and Internet crime.\textsuperscript{35} If a computer is stolen from

\begin{itemize}
\item[35.] Marc M. Goodman says that a ‘computer crime’ can be classified into three broad categories as crimes where the computer is the target, crimes where the computer is a tool of the crime and crimes where the computer is incidental. In the first category, a perpetrator intentionally attacks an innocent party’s computer. In the second category, the computer is used to commit a traditional crime in a high tech way. The third one is, where a computer is mere incidental, in the sense, the perpetrator might have committed the crime even if there was no computer. After classifying in this manner he interchangeably uses the term ‘cyber crime’ and ‘computer crime’ to deal with these problems. Marc M. Goodman, “Why The Police Don’t Care About Computer Crime”, 10 Harvard Journal of Law and Technology 468 (1997); Nandan Kamath says that “since the Internet is composed of computers, crimes occurring on the Internet are computer crimes”. He also says that “a computer can be the subject of a crime by being stolen or damaged; it can be the site of a crime such as fraud or copy right infringement; or it can be the instrument of a crime, such as when it is used to access other machines or store information illegally. These are all computer crimes in the sense that a computer is involved”. He there after uses the words ‘computer crime’ and ‘Internet crime’ synonymously. Nandan Kamath, Law Relating to Computers, Internet, and E-Commerce, Universal Law Publishing Co.Pvt Ltd, New Delhi (2000), p.22. Suresh T. Vishwanathan defines computer crime as : “(1) any illegal action in which a computer is a tool or object of the crime; in other words any crime, the means or purpose of which is to influence the function of computer (2) any incident associated with computer technology in which a perpetrator, by intention, made or could have made a gain and (3) computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data”. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House, New Delhi (2000), p.13.
\end{itemize}
a house, it is not a computer crime or a cyber crime. It is just like stealing gold ornaments or a television set from the house. It is a crime in the traditional sense, which can be dealt by traditional laws. When a crime is committed to or by a computer, without using the Internet it is just a computer crime and not a cyber crime.

A cyber crime can be understood as any crime committed with the help of Internet, abusing the special characteristics of the Internet such as anonymity, absence of geographical boundaries and speed. Once committed, it would be difficult for the law enforcing and the adjudicating agencies to deal with the situation and find out a remedy. In some situations there will be only cyber crime, and in some other situations it stands along with a traditional crime.

The cyber crime can be classified broadly into four categories namely, cyber theft, cyber trespass, cyber violence and cyber


37. For example in a conspiracy to commit a murder in India, apart from the person who really commits the murder, all other conspirators may be in some other countries, but not identified where. They might have planned the murder through the use of Internet. Here, even the person who commits the murder is unaware of the other persons. If the conspiracy was through postal service, other persons can be found looking to the postal address. If it was through telephone line, the person can be identified, or at least tracing the telephone networks can identify the location.


39. If any one dishonestly moves any movable property without the owners consent, it is a theft. Here the perpetrator moves the property without the owner's or possessor's consent. For example by breaking into the computer (f.n. contd. on next page)
obscenity. When one deals with these issues, a complex of moral, political or legal values arise, and they are so intertwined that it cannot be restricted by any particular individual, social group or country.

Governments all over the world are now trying to find methods to regulate cyber crimes. These nations try to do it by either applying an Internet specific law or by extending the application of the existing criminal laws. No state has the power and legitimacy to make laws for an area, which does not have any physical or geographical boundary. In Reno v. American Civil Liberties Union, it was held that no single entity control the Internet. In Blumenthal v. Drudge the Court said that ‘the internet is actually nowhere and everywhere.’ No single state can make laws to

40. The information stored in the Internet might be restricted using passwords. These passwords are the fence. Breaking a fence and entering into some one else’s property is punishable.

41. If the impacts of the cyber activity of a person or group of persons have violent effects upon another person, or social group, or a country, then it can be called as cyber violence. These types of activities do not have a direct physical impact; nevertheless, the victim feels the violence of the act. This can lead to long-term psychological impact on the victim.

42. This means the trade of obscene materials within the cyber space. This is by the extension of the principles, punishable under Sections 292 and 293 of the Indian Penal Code. But these sections are helpless because of the special natures of the Internet.

43. E.g., see the (Indian) Information Technology Act, 2000, The (US) Computer Fraud and Abuse Act, 1997 and The (Canadian) Criminal Code. After defining the various offences the Indian law tries to bring the jurisdiction of these offences to Indian courts, even if committed outside India and authorizes the Indian law enforcement agencies to take action according to the Act. But while applying these provisions both theoretical as well as practical difficulty will arise.

44. Supra n.4.

control an area which is not controlled by them. Regulations of crime at national level are determined by the legal system of each country. They are well settled and confront no problems. With the use of these provisions and the procedures under the Extradition Act, 1962 and different extradition treaties entered by India with different countries, no complex problems arose till the advent of Internet.

After the wide-spread use of Internet, crimes of extra-territorial nature have become more common. There are many practical difficulties, which would arise when a particular state is trying to regulate the cyber crime and fix the jurisdiction in the local area, where the offence is committed. They are problems of legislation, policing, adjudication and taking of evidence.

Practical Problems in Extending the Traditional Laws to Cyber Space

The traditional laws cannot deal with the new challenges in the cyberspace. The existing laws and regulation have their bases on physical world activities. In the Internet no physical object is being transferred from one person to another. As Christopher Reed rightly points out:

"Consequence of digitization and automation is that many Internet activities are widely distributed, both among actors and jurisdictions thus making it difficult or impossible to apply existing laws to the Internet analogous of physical world activities." 48

46. When a man commits a crime within India the law makes no difference based upon the nationality of the accused. In Mubarak Ali Ahmed v. State of Bombay, A.I.R.1957 S.C.857, it was held that when an Indian citizen and a foreigner commit the same offence in India, it makes no difference at all. If any Indian citizen goes out of the country and does any act, which is a crime according to the law of India, he can be punished in India.

47. For example, in the physical world the trade and information of products are based upon their transfer in physical nature itself, like a book or a CD-Rom is transferred from one person to another. Existing laws can regulate these transactions.

The major problems and challenges are as follows:

(a) \textit{Multiple Jurisdictions}

Because of anonymity of the Internet user\textsuperscript{49}, absence of geographical boundaries in the cyberspace, and the cross border effect of Internet transactions, all legal systems face legal uncertainty. Due to this, in Internet transactions the national laws become less meaningful and impossible to enforce. There will also be multiplicity of overlapping applicable laws and jurisdictions, which can be “multiple and contradictory regulation or no regulation at all.”\textsuperscript{50}

(b) \textit{Legal Vacuum}

Another difficulty for the legislators is the legal vacuum. The legal draftsman and the legislator have to, in some way, find a solution to the existing problems in cyberspace. But there are no appropriate model laws. For example when the Utah Digital Signature Act, 1996 was passed, it had to be drafted from vacuum. Because of these reasons a legislator feels difficult to enact a law which might be suitable for regulating the Internet.

(c) \textit{Problem of Policing}

Cyber crimes are happening in a world of one’s and zero’s, i.e., a world which is entirely different from the real world. An ordinary person cannot understand the depth of the problem in such circumstances.\textsuperscript{51} David J. Davis, who is a detective inspector of the Fraud Squad of the West Midlands Police says that when the first Internet case involving cyber obscenity came up in the United Kingdom, it was very difficult to convince

\textsuperscript{50} Supra n.19.
the magistrate to issue a search warrant.\textsuperscript{52} The lack of technical knowledge, non co-operation among different police organisation etc., make the problem too difficult to be solved. Moreover, when compared with the conventional crimes, the cyber crimes vastly go unreported or it is not reported to the extent of actual perpetrations.

(d) \textit{Expensive Process}

Another problem is the lack of finance faced by the investigators. Training of law enforcement officers to solve the issue of cyber crime is very expensive. Once he is trained, he has to refresh his knowledge in tune with the technological advancement.\textsuperscript{53} Besides training, the specialized hardware and software required for the forensic examination of cyber crimes are very costly. One such example is digital evidence storage rooms which are “spaces without magnetic interference.”\textsuperscript{54} They must be established to prevent breakdown and destruction of digital evidence. A police department serious about the investigation of high-tech crime must prepare for any eventuality. This is just one such problem. Substantial fund may be required in all aspects of investigation.

(e) \textit{Obtaining Digital Evidence}

Another instance where the policing of cyber crime becomes difficult is with regard to obtaining the digital evidence. Goodman correctly noted that “not only can incriminating clues be hidden encrypted and virus laden, but they can be strewn any where in the world.”\textsuperscript{55} The current Internet specific laws regarding the search and seizure of digital evidence are mostly ambiguous.

When evidence is to be proved in a court, two principal situation have to be considered\textsuperscript{56}. One is whether the offence is mainly by the

\begin{itemize}
\item \textsuperscript{52} \textit{Ibid.}
\item \textsuperscript{53} Marc M. Goodman, supra n. 35.
\item \textsuperscript{54} \textit{Id.}, p.485.
\item \textsuperscript{55} \textit{Id.}, p.483.
\end{itemize}
individual’s use of the Internet. He can do any crime to other individuals, websites, or some other entities. In this case the individual is the culprit. The second situation is whether the remote site holds the evidence of the offence. The examples of such situations are the publication of obscenity in the website or any other situation in which the content of a website is illegal in any country. These perpetrations can be proved from four sources such as individuals’ own computer, his telephone bill, the Internet Service Provider and the remote sites.

(i) Individuals’ own computer

The acquisition of evidence from individual’s own computer and proving it in a court has many problems. The perpetrator who is a technically qualified person does not leave behind any evidence in his own computer. He deletes the memory and all other evidence from the computer.

(ii) Telephone records

The telephone records can be a corroborative evidence in proving a case. It is said that the particular time in which the perpetrator connects to the Internet Service Provider (ISP) will be recorded in the telephone records. If the time of the commission of the offence and his connection with the ISP is one and the same, then it can be a corroborative evidence. This is a situation where the perpetrator connects his computer to the ISP, and uses his own telephone connection. If the person connects to the net from a cyber cafe, it does not make a corroborative evidence. Similarly if the perpetrator is using a prepaid cellular connection taken by a false address to connect to the Internet, the chance of proving the person’s involvement is very less.

57. Id., p.72.
58. Hereinafter referred to as ISP.
59. Supra n.53, p.73.
(iii) Internet Service Provider

In U.S.A the investigating officer can apply to the ISPs to release any such information.\textsuperscript{60} The ISP cannot be held liable for any act of others, if the offence was not committed with their knowledge, or it exercised due diligence to prevent the commission of such offence.\textsuperscript{61} The American Supreme Court in \textit{Cubby Inc and Blanchand v. Compu Serve and Fits Patrick}\textsuperscript{62} supports this idea. In this case the Court said that the ISP is an innocent disseminator of the information, and hence cannot be punished. When the evidence received from the ISP is being used in a court of law, it is very easy for the accused to get the benefit of doubt. One can access to a foreign ISP, using an international call and connect to any site. Here both the ISP as well as the website will be out of the court’s jurisdiction.

(iv) Remote sites

If the country from which the website is hosted allows its content, it is very difficult, to take any action against the site. If in a hacking case, the hard copy or a soft copy of the page hacked is produced, it does not become an evidence before the court of law.\textsuperscript{63} The accused can get the benefit of doubt, that the record produced in the court is a manipulated one. As Sommers aptly says:

“How can they show that data has been obtained from specific computer and nowhere else. Website forgery is not uncommon.”\textsuperscript{64}

Any authentication as to the time and date of occurrence of the incident cannot be given.\textsuperscript{65} In order to prove this, it may require other
forms of evidence such as deposition of witnesses, exhibits indicating ownership of the computer or data. So the question is : can the producing of witnesses give a full and believable explanation of the process by which the file was acquired from the remote computer to the user’s machine to show that the result is accurate, free from contamination and complete?

In order to get acceptance in a court of law, the evidences should be authentic, accurate, and complete. They should form chain. But evidences, acquired from personal computer, telephone connection, ISP and website, may not form a chain, and thus fails to be authentic, accurate and complete evidence in a court of law.

**Regulation of Cyber Transactions**

Due to the Internet, the whole world has turned into a single market place. The business community extended the traditional methods of entering into contract to the Internet and started calling it “online contracts”. Electronic commerce or online contracts can be defined on the basis of the medium upon which they are being entered. Melissa De Zwart defines it as a broad concept that covers any commercial transactions that is affected via electronic means and would include such means as facsimile, telex EDI, Internet and the telephone. If it is defined narrowly it will include only commerce through the Internet. The existing legal systems regulate the problems of commerce through medias other than Internet.

---

66. *Id.*, p.74
67. Electronic Data Interchange.
69. The English as well as Indian law allows the contract to be entered into by writing, orally, or by conduct. In consequence the law has recognized making of contracts using telephone, fax, or any other modern technology. However, the parties should be competent to enter into a contract, and they should give their free consent. Similarly the consideration and object should be lawful. So in the case of Internet commerce or online commerce theoretical impediments are there.
Margaret Jane Radin, points out that in the Internet, only the contract as a product can be seen. This view seems to be incorrect. In the Internet both the contract as consent and contract as product could be seen. The business-to-business contracts are on the basis of contract as consent. These e-contracts are formed as an outcome of bargain. Both the parties make these contracts after the approval of the terms and conditions. The only difference between this and the traditional contract is that Internet is used as a medium of bargaining. Most of the business-to-business contracts are of this type. Here both the parties know each other and they confirm the identity of the parties through the use of digital signatures and time stamp. Usually the Internet does not create any problem in this type of online contract. The parties will be financially stable, they know each other, and the contract is similar to any other ordinary contract. If it is a trans-national contract, it can be resolved through the use of arbitration clause, or any other dispute settlement mechanism, which they choose satisfying the international legal principles regulating trans-national contract.

Where as, the business-to-consumer contracts are on the basis of contract as a product. Here the contract comes along with the product in standard terms. The parties in these types of contract are the main victims. These types of contract are generally termed as click wrap contracts. They are used for the retail sales on the Internet. Once a person enters into a website and wants to purchase some product he has to click on the ‘I Agree’ button. By clicking on this button he automatically agrees with terms of service, or conditions of use which will have some link from the website. The party may or may not note this, but the court has given validity to this contract in Hotmail Corporation v. Van Money

70. For details, see Margaret Jane Radin, “Humans, Computers and Binding Commitment”, 75 Indiana Law Journal 1125 (2000).
72. Supra n.70, p.1128.
73. Suresh T. Vishwanathan, supra n.35 at p.18.
Pie Inc. One such kind is where the products are advertised in a web page, and the party interested to purchase can do so by paying the money through credit card, or any other means.

(a) Invitation to treat and an offer

The invitation to treat is a particular action or statement, which is intended to provoke an offer from another party. If the Internet advertisements are presented to the analogy of an offer and once it is accepted by any party, the website cannot repudiate from the contract. As long as the website does not distinguish between the ‘offer’ and ‘invitation to treat’. This will create difficulty. For example a website has one copy of an old and precious book. If it is considered as an offer, any one can accept it. If it is an invitation to treat, the website owner can accept any of the offer.

(b) Contracts by minors

In cyber space parties will have great difficulty in knowing whether the customer is forty-eight years old or merely eighteen. The online business people may find two difficulties in dealing with minors. First is that the sale of certain goods and contents to minors are unlawful, such as tobacco, alcohol and pornography. Second is that under the English law contracts made by minors for things other than for necessaries are voidable and it

76. An example for this type of contract is the sale books through www.amazon.com. These types of contracts involve the online supply of data, such as software, text or multimedia products.
77. An example for an invitation to treat is the display of goods in a shop window or a supermarket shelves.
binds the minor unless he repudiates. The minor may be under some liability in tort and in restitution. How can this problem be solved in online contract? Even though chance of coercion and undue influence are less on the online transactions, the chance of fraud, misrepresentation and mistake are very high, when compared to ordinary contracts.

In the Internet commerce some of the most common types of online fraud are pyramid schemes, chain letters, bogus business opportunities, credit repair schemes, miracle health and diet products, items paid for but never delivered, investment and security scams, and gambling. None of the states have succeeded in making a law against these types of fraud because of the Internet’s specific characteristics. John Rothchild says that the characteristics of Internet make it difficult for an online seller to structure his online activities.

(c) Online advertisements

Many of the advertisements in the Internet are found to be misrepresentation aiming to induce people to enter into a contract. The laws and regulations for regulating the advertisement vary from country to country. The European Commission Green Paper catalogues the variations among the advertising laws of the European Union member countries. It

79. Mercantile Union Guarantee Co v. Ball, [1937] 3 All E.R 12. It can be found that the basis of the protection to the children as two principles. First is that the law must protect the minors against their inexperience. The second is that the law should not cause unnecessary hardships to minors.


82. Id., p.911.

83. Ibid.

84. Supra n.78, p.18.

says that the rules governing the use of comparative advertising vary greatly from one country to another, as do the rules concerning direct advertising, television and radio advertising. The persons communicating to take online advertisement may not succeed in enforcing their rights due to the variations in law.

(d) **Mistake of law and mistake of fact**

The conventional contract principles give much emphasis on the mistake of law and mistake fact. The mistake of law of a foreign country is considered to be a mistake of fact. But this distinction does not have any significance in the Internet. In the online contracts, as pointed out earlier, geographical boundaries between the states have no role. The relevance of the distinction between foreign law and domestic law ends here.

(e) **Problem of enforcement**

Even if the party could establish jurisdiction to try a case, and the court delivers a judgment the next question is as to its enforcement. In the absence of a treaty, it will not be possible to enforce the injunctive provisions of an order in the court of a different sovereign. Under International Law, if a state pursues public claims outside the confines of its own territory, is attempting to invoke its sovereign rights within the territory of the forum state. According to F.A. Mann, in the absence of the consent of the sovereign of the forum state, this assertion involves the infringement of domestic jurisdiction of sovereignty. So the plaintiff, even if determined to enforce the judgment against defendant in a foreign state, may not succeed unless there is a treaty between the states.

86. *Supra*, n. 81, p. 911.
87. The Indian Contract Act, 1872, Ss. 20-22.
88. *Supra* n.81, p. 919.
(f) **Problem of being cost effective**

To start a business through Internet the cost is very less.91 If the order of the court is to attach the assets of the defendant to recover money, it might not succeed because either the defendant does not have much assets or he might have sold or transferred the assets. Once the assets of the defendant are attached before judgment, the defendant cannot transfer the property so attached. But the nature of the order is very weak even in ordinary transnational civil litigations. In countries belonging to the British Commonwealth, a procedure known as the ‘mareva injunction’ is available. A mareva injunction is an exparte interlocutory measure intended to freeze a defendant’s assets prior to judgement in order to prevent the removal of those assets from the jurisdiction of the court. The Brussels Convention, 1968, extends the principle of mareva injunction to the European Union. Even countries, which do not have the system of mareva injunction, do have similar systems. In the online context, the problem is that such a system can be used only if the assets of the defendant can be identified. But due to the very nature of the Internet, these assets may not be identified. To enforce a mareva injunction, a foreign counsel has to be engaged. This is a very expensive procedure. Most of the online consumers may not be in a position to have such a high amount.

**Conclusion**

In the foregoing analysis it can be seen that the cyberspace is not an area, which the present territory based legal systems can easily accommodate. The standardization of law in cyberspace needs to be arrived at.92 This would need a separate International Cyberspace

---

91. *Supra* n.81, p.926.

92. The actors who have initiated this process include the United Nations Commission on International Trade Law, which had drafted a model law on electronic commerce. The European Union, the International Chamber of Commerce, the World Trade Organization and the World Intellectual Property Organization have drafted common standards for the e-commerce. The UNCITRAL Model Law on Electronic Commerce, which was drafted in 1996 and adopted in 1998, is intended to be a guideline for the states that wish to enact a separate legislation for electronic commerce or update their current laws regarding cyber space.
Convention and enforcement machinery. The group of nations, by entering into a convention should set standards. The standard shall be made broadly so as to include cultures, customs and values of different population. Recently, the European Union has drafted a Convention on Cyber Crime and has tried to arrive at a standard setting process.93 The Convention is successful in attaining standards among the European countries. At the global level, it could be still difficult. The Convention on Cyber Crime, stipulates for standardization of cyber crimes, through which the crimes can be punishable any where in Europe. Each state party shall have jurisdiction to try the case if the offence is committed in that country. The Convention also provides for the encouragement of creating cyberspace morals among the users.

Similar to the European Convention, the world community may try to standardize the laws on cyber crime. Once these standards are set, a Commission on Cyberspace can be constituted, which shall enforc these norms at the international level. Each state party who are members to the Commission shall file yearly reports to the Commission regarding the measures taken by them in the regulation of cyber crime. The Commission can send special reporters to these nations for studying how far these countries have become successful in adopting the convention. If the Commission is not satisfied with the report, it can give directions to the state to comply with the convention. Once they do not comply with the convention within the stipulated time, the Internet flow to that country can be blocked.