Lecture in Training Programme on Cyber Law and Cyber Security for Judicial Officers on 10th April,2010 organized by Institute of Management in Government, Thiruvananthapuram, Kerala at IMG Main Campus, Thiruvananthapuram, Kerala

By

Justice Rajesh Tandon,
Chairperson,
Cyber Appellate Tribunal
Ministry of Communications & Information Technology Department of Information Technology,
Jeevan Bharti (LIC) Building, Connaught Place,
New Delhi.

Subject

ROLE OF JUDGES AND PROSECUTORS IN COMBATING WITH CYBER CRIMES

The Information Technology Act,2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October, 2009.The definition of the Information Technology Act provides as under:

(a) "Act" means Information Technology Act,2000 (21 of 2000)

(b) "Communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication"

(c) "Communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource.

The Information Technology Act,2000 was introduced on 9th June,2000. Mitigation that has led to the introduction of the Information Technology Act,2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No.51 of 162 dated 30th January,1997 which has recommended that all the States should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication. The preamble of Act 21 of 2000 provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act,1872, the Banker's Books Evidence Act,1891 and the Reserve Bank of India Act,1934 and for matters connected therewith or incidental thereto;

Whereas the General Assembly of the United Nations by resolution A/RES/51/162 dated 30th January,1997 has adopted the Model

Law on Electronic Commerce adopted by the United Nations Commission on International Trade law;

And whereas the said resolution recommends, inter alia, that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information."

Gradually the Act was amended on 5th February,2009 being the Amendment No.10 of 2009 which has introduced the world digital signature instead of electronic signature as provided under Chapter II of Section 3 of the Act. In Section 2, Clause (ha) was introduced after the word (h) which provides the Communication device. It reads as under:

"Communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;"

The Information Technology Act,2000 came into force on 17th October, 2000. It has 94 sections divided into 13 chapters. This Act was amended vide notification dated 27th October,2009.

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd edition 2005 has defined the same in the word of `Cyberspace". It has used a term as a `floating' in an electronic environment, which is accessible internationally. Then the Author has also defined the `Cyber theft' known as the act of using an online computer service.

In this dictionary `Cyber law' is defined as under:-

> "The field of law dealing with computers and the Internet including such issues as intellectual property rights, freedom of expression, and free access to information."

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd Edition 2005 has defined **`Cyber theft'** known as the act of using an online computer service.

In this dictionary **`Cyber law'** is defined as under**: -**

> "The field of law dealing with computers and the Internet, including such issues as intellectual property rights, freedom of expression, and free access to information."

The definition of the Information Technology Act provides as under:

"Computer" means any electronic, magnetic, optical or other high speed date processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

JURISDICTION

Section 1(2) of the Information Technology Act,2000 reads as under:-

> "1(2) "It shall extend to the whole of India and, save as otherwise provide din this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

Section 3 provides with regard to Digital signature and the Authentication of electronic records.

Section 4 provides the legal recognition of electronic governance. For short known as E. governance.

The use of **Information and communication technology** in judicial sector and in Administration of Justice had been probably one of the promising examples of e-governance through out the world. Democracy is easy to define but very difficult to follow, the strong democratic system for any country depends on their judicial system. The effect of Globalization on the economical and social culture is invoking the need of a strong, transparent and efficient judicial system that should provide a platform to all the stakeholders to get connected. The thrust of basic Information and communication technologies provide this requirement and, therefore, Countries across the world are implementing **Information and Communication technology** to enable judicial system in Administration of justice.

Information Technology (IT) law governs the processing and dissemination of information electronically. These are technology-intensive laws to control and safeguard electronic transactions in the electronic medium. At a very basic level IT laws are dealing with electronic impulses and their transfer from one computer terminal or network to another.

At this point, it is imperative to understand that how this change in culture will be adopted and how it will impact the social culture of developing and under developing countries and how it will be implemented in Administration of Justice.

I, therefore, classify the role of Informations Technology in three parts.

i) IN THE INFORMATION TECHNOLOGY , ROLE OF ADMINISTRATION OF JUSTICE.

ii)WORLD'S SCENARIO ON IMPLEMENTATION OF E-ENABLE

ADMINISTRATION OF JUSTICE SYSTEM GLOCALIZATION.

JURISDICTIONAL ASPECT – ITS ROLE IN THE ADMINISTRATION OF JUSTICE

(i) INFORMATION TECHNOLOGY AND ITS ROLE IN THE ADMINISTRATION OF JUSTICE.

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd Edition 2005 has defined the same in the word of **`Cyberspace'**. It has used a term as a **`floating'** in an electronic environment, which is accessible internationally. Then the Author has also defined the **`Cyber theft'** known as the act of using an online computer service.

In this dictionary **`Cyber law'** is defined as under**: -**

"The field of law dealing with computers and the Internet, including such issues as intellectual property rights, freedom of expression, and free access to information."

The Information Technology Act,2000 (IT Act) came into force on 17 October,2000. According to its preamble, the IT At basically seeks to:

- Provide legal recognition for electronic commerce.
- Facilitate electronic filing of documents with the Government agencies.
- Amend the Indian Penal Code, 1860, the Indian Evidence Act,1872, the Bankers' Books Evidence Act,1891 and the Reserve Bank of India Act,1934.
- Promote efficient delivery of Government services by means of reliable electronic records.
- Give favourable consideration to the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).

"Electronic commerce" or e-commerce includes transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information.

"Electronic Data Interchange" (EDI) is the exchange of standardized business documents from computer to computer. They key to EDI is the fact that all the documents exchanged conform to a common computer-readable format. Instead of sending email messages (which do not follow a set format), EDI allows for structured information to be exchanged. The most important EDI standard is the UN/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce & Transport).

The development of using **Information and Communication technology** in the area of Administration of Justice is not a new thing. In fact, almost the development in this field started almost 2 decades ago. In

this section we will highlight the movements. The points to be highlighted are as under:

(i) Basic Technologies Development.

(ii) Case Management System

(iii) Connecting Judges and third parties.

(iv Tackling the complexity of the sophisticated nature of cyber crime.

i) Basic Technologies Development.

Initially the efforts were started with the objective of exposing the judicial fraternity with the basic **Information and Communication technology** devices like personal computer, some software application for typing the judgments. As a matter of fact some software application for speech to text conversion to make the Process easy had also been introduced but the results were not so convincing. It had been observed in many places that the system provided to the court were hardly unpacked for many years. Upon understanding the root for this problem, the fact that came up was lack of understanding; apprehensions on the reliability of the systems and the target audience were not ready to accept this change in work culture. This had made the policy maker to realize the gap and revealed the area of concern i.e. the change management of the working environment.

ii) Case Management System

The real power of automation had been realized by the judicial fraternity and they started with the initiative of automating few processes like case registration, online listing of cases herein referred as case management system. This initiative had been a great success but had to face a big technical challenge of making the technology work for heterogeneous environment.

In Administration of Justice , it is being used in the following forms:-

- General information
- Information on court activities & organization
- Legal information
- Case information

This concept probably had been the concept of judicial resources planning.

iii) Connecting Judges and third parties:

The potential of the management information system using **Information and Communication technology** was still at **nascent** stage as everything was on **Intranet** domain. The real integration of technology to make an efficient, transparent judicial system without connecting the entire stakeholder like judgment seeking parties, lawyers, judges, Notaries and judicial administration group. This calls for the need to develop a dedicated portal or an application that can have all the view without geographies limitation. It had also been realized that the judges require a lot of case law as a reference to announce their decisions and hence the need to connect a judicial repository system was also envisaged. Not only the judges but all the stakeholders for e.g. the judgment seeking parties will save lot of time and also the physical security of the parties, social stigma in many of the cases due to the cultural set up of that country. The lawyer often had to struggle to manage the status of their cases listing in different courts; this burden may drastically be reduced with having the information of everything in front of them.

iv) Tackling the complexity of the sophisticated nature of crime (cyber crime)

In the judicial system through out the world is struggling with the menace of cyber terrorism. The policy maker are visioning that the in coming years the most devastating impact of cyber terrorism falls to the judicial system as they are now having website presence. The threat of destruction,

disruption or both is just the one side of the coin the other side concerning the judicial fraternity is how to develop a scientific methodology keeping in mind the principles of admissibility of evidence as per the evidence Act of the country. No doubt the initiative to create cyber police stations and investigative agencies are putting all the efforts to pin point the technical intricacies of the nature of the case but still lot have to be done in this direction. Website Platforms are one of the most lucrative platforms for terrorism due to the inherent benefit the user enjoys i.e. anonymity, easy to access, low cost of technology procurement, lack of awareness among users and also the fear of the consequence of negative impact.

In one of the case of search and seizure the police department raided the physical location and seized lot of Floppy Disk, later the constable used a punch to make a hole in the Floppy Disk and tied it up with a string.

Similar matters were also reported at Banglore regarding cyber cases.

ii) WORLD'S SCENARIO ON IMPLEMENTATION OF E-ENABLE ADMINISTRATION OF JUSTICE SYSTEM-GLOCALIZATION.

The growth of globalization is very well realized among the society the consequence of this globalization had made the world a small connected village, wherein any one in fraction of minutes can gather the information of everything they want for e.g. medical related, education related, job related and also law related. The whole process gives a birth to a concept known as glocalization. In this section we will discuss the E-enabled judiciary for some of the biggest democracies of world for e.g. Europe and also the Indian scenario.

The preamble of our constitution says that every citizen shall get justice free from fetters of social, economic and political evils. Therefore, to get speedy justice infusion of Information and Communication Technologies

in Indian judiciary is envisaged. We need to implement Information and Communication Technologies in all four corners of the judiciary in order to achieve its goals in a required and reasonable time. The implementation of Information and Communication Technologies in judiciary is not only for a time factor but also addresses following secondary facets:

i) To help the Judicial Administration in streamlining its day-to-day Activities.

ii) To provide web based information & query counter for the benefit of litigants.

iii) To provide transparency of information.

iv) To cut short delays in all applications.

v) To comply with RTI Requirements.

With the adoption of **Information and Communication Technology** in full fledged manner, the climate in Indian judiciary will change for centuries to come. **Information and Communication Technology** has to implement at three levels i.e. for judges, lawyers and applicants.

Firstly, if judges will adopt **Information and Communication Technology**, they can read the cases to be raked up on next day and refer the precedents for a prudent judgment which they have decided on the same day or earlier on a single platform which can be internet or intended website for it. They can digitally authenticate their judgment, which can give more appropriateness. There are so many cases pending in the higher courts for admission, which can apparently be dismissed because of some trivial flaws electronically, by the judges or persons appointed on his behalf, which can save the precious official time of the judges in the courts. **Information and Communication Technology** will also help the courts to transfer and dispose off the case quickly.

Secondly, if lawyers adapt **Information and Communication Technology**, it will surely become a boon for them. They can see the cause list, latest judgments, courts manual, register their case electronically, refer the latest cases through search engine beneficial for their pleading without going into hectic schedule of reading hard bound journals, will also get other incidental updates happening in the world at one place.

Thirdly, it becomes a requirement for the litigants to give **Information and Communication Technology** in themselves in order to mitigate their sufferings. They are already burdened up with the grievance of their case and perusal of the case increases the intensity of their mental agony. Therefore, following the principles of **Information and Communication Technology**, applicants will be able to see the status of their case at their home, will get receipts for every transaction, complaint easily for any fraud committed, avail the rights enshrined under Right to Information Act, 2005 and encompass many other pains of themselves.

The Indian courts have started implementing **Information and Communication Technology**. Supreme Court and all the High Courts are examples of it.

Information and Communication Technology is very necessary at higher courts just for a reason that they are court of records under Article 215 of the Constitution of India. It means to say if Allahabad High Court had come into existence in 1866, so its duty is to preserve and protect all the documents relating to a particular case with it since then. So they need to maintain their database and for that they need physical space. So if that database is created electronically, it would definitely save the physical space and reduce the burden for searching a file physically, the details of which can easily be taken out though local search engine on an electronic

platform. **Information and Communication Technology** will sooner or later seek an electronic court, which is of utmost importance for the redressal of disputes of the applicants. This will ensure cost effectiveness in imparting justice, transparency, and disbursal of case quickly and getting justice on time.

This judicial system throughout the world is facing with the adoption of the Information and communication technology in the existing judicial process. However, the maturity of the e-enable judicial system in at Phase 4 in many of the developing countries. Therefore we will discuss the challenges related with *"tacking the complexity of the nature of sophisticated cases"*

.

• ***Cyber security to protect the I.T Infrastructure of the Judiciary:*** who knows that the infrastructure that is used to give justice in contrary used for crime i.e. having web identity and presence the infrastructure is prone to many cyber attacks, for e.g. the digital repository that is been used as a reference of similar nature of case is contaminated and a manipulated judgment is uploaded, this will just change the whole meaning of the judicial system and will have catastrophic results.

• **The Judicial Set-up:** every country almost has a similar hierarchy of judicial set-up though the internal processing may be different. When it comes to the implementation of the **Information and Communication Technology** infrastructure the policy maker also need to highlight the topology of the infrastructure i.e. a centralized or decentralized set-up. This will warrant avenue of different need of security and management of the **Information and Communication Technology** infrastructure.

iii) JURISDICTIONAL ASPECT – ADMINISTRATION OF JUSTICE

Cyber space is a world of virtual reality. It is a brand new world. And a brand new world requires brand new laws. Do such laws exist? Or are we seeing rehash of old laws in the new realm? The result is confusion and a sense of betrayal.

Cyberspace requires cyber laws. Physical laws have limitations in the sense that they are one-dimensional in application. They are meant for the physical world which is static, defined and incremental; whereas cyberspace is dynamic, undefined and exponential. It needs dynamic laws, keeping pace with the technological advancement.

Cyberspace is a place where the entry is not bound by geographic boundaries. Any person who lives in this cyberspace is part of the community. He is an unknown entity. He has no fixed geographic coordinates. He traverses cyberspace from one set of coordinates to another.

The Information and Communication technology in judicial system will play an integral role for the society to trust on its judicial process, due to its inherent advantage of fast processing, Trivial retrieval, less human intervention, relatively low cost of development and in some criminal cases where physical presence is an issue this solution is the best one .

Section 78 of I.T.Act empowers Deputy Superintendent of Police to investigate cases under the Act.

Case law

Syed Asifuddin & Ors. V. State of Andhra Pradesh & Anr. (2005) Cri.LJ 4314

Summary of the case.

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisaged by s 65 of the Information Technology Act,2000.

Findings of the court.

- As per s 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

- The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

- A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

- When the person moves from one cell to another cell in the same city, the system, i.e. Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

- All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

- System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

- Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

- Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

- When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

- If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

- When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

- So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

- This is a microprocessor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

- When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indocom.

Now we come to the definition concerning **JURISDICTION** as used under the Information Technology Act,2000.

PROVISIONS RELATING TO JURISDICTION IN CYBER SPACE UNDER THE INFORMATION TECHNOLOGY ACT,2000

Section 1(2) of the Information Technology Act, 2000 reads as under:-

1(2) "It shall extent to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

The aforesaid definition covers the offences or contravention even committed outside India by any person.

Section 75 reads as under:-

75. 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 network located in India.

A perusal of the aforesaid provisions covers up the offences committed outside India by any person irrespective of his nationality. After reading the aforesaid provisions of Sections 13 and 75 of the Act, it is evident that presence of the computer system, computer or computer net working and information received through computer generated by micro fiche being important irrespective of the same having been done outside India irrespective of his nationality. Section 1(2) also is very clear having given coverage to the offences committed outside India by any person.

JURISDICTIONAL ISSUES

The major issues addressed by the IT Act are:

- Authentication of electronic records using digital signatures.

- Legal recognition of electronic records and digital signatures.
- Use of electronic records and digital signatures in Government.
- Retention of electronic records.
- Publication in Electronic Gazette.
- Attribution and acknowledgment of receipt of electronic records.
- Time and place of dispatch and receipt of electronic record.
- Secure electronic record, secure digital signature and security procedure.
- Appointment and functions of Controller and other officers.
- Recognition of foreign Certifying Authorities.
- Functioning and control of Certifying Authorities.
- Digital signature certificates.
- Duties of subscribers such as generating a private-public key pair, acceptance of digital signature certificate and control of private key.
- Penalties for damage to computer and for failure to furnish information.
- Factors to be taken into account by an adjudicating officer.
- Establishment, procedures and functioning of Cyber Appellate Tribunal.
- Offences relating to tampering with source code, hacking, cyber pornography, disobeying Controller's orders, unauthorized access to protected system, misrepresentation, breach of confidentiality and privacy and Digital Signature Certificate frauds.
- Extra-territorial jurisdiction of the IT Act.
- Confiscation of computers, etc. investigation of offences, police powers.
- Liability of Net work Service Providers.
- Overriding effect of the IT Act.
- Protection of action taken in good faith.

- Offences by companies.
- Constitution of Advisory Committee.
- Powers of the Central and State Governments and the Controller to make rules and regulations.
- Amendments to the Indian Penal Code, the Evidence Act, the Reserve Bank of India Act and the bankers' Books Evidence Act.

E-Commerce and the whole Internet are characterized by their internationality. In the case of conflict, the question rises not only about the applicable law but also about jurisdiction as the choice of law not necessary entails the competent court.

Jurisdictional questions are governed by the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial matters of 1968, the Brussels Convention.

Its basic rules determine that, in principle, persons domiciled in a Member State may be sued in the courts of that state, regardless to their nationality (Art.2 of the Convention). In matters relating to a contract, a person domiciled in a Member State may be sued in the courts for the place of performance or the obligation in question. (Art.5 para.1 of the Convention.)

Specific provisions apply to consumer contracts. Therefore, Art.14 para 1 of the Convention stipulates that the consumer has the choice to sue the contracting party in the courts of the Member State where either that party or he himself is domiciled. (Art.14 para.1 of the Convention). In the reverse case, the other party can only sue the consumer in his country (Art.14 para 2 of the Convention). These rules, however, do solely apply to consumers in the cases that are listed in Art. 13 of the Convention. The term "Consumer" has to be understood as a person who concludes contracts for a purpose which can be regarded as being outside his trade or profession (Art.13 para.1 of the Convention).

Important to E-Commerce is especially Art.13 para.3 fig.3 of the Convention, which refers to contracts on services or goods. To establish a specific relation to the consumer's country of residence the consumer must have been the subject to a specific invitation addressed to him or advertising in his state of domicile, and in that state he must have performed a legal act required for the conclusion of the contract. It is not necessary to render the service in the consumer's country of residence.

Appellate consideration

This case presents novel issues arising from the global nature of the Internet, where cyberspace has no territorial boundaries. The crux of the matter involves the US Constitution and whether another nation may regulate freedom of speech – a right which has been long cherished in the United States- by a US resident within the United States on the basis that such speech can be accessed by internet users of another nation.

Basic principles have been essentially geographically based and have therefore been difficult to apply in the context of the Internet. A website can be viewed from any place in the world where there is access to the Internet. As a result, geographical location has less significance than previously in the context of jurisdiction. Information over the Internet passes through a network of networks, some linked to other computers or networks, some not. Not only can messages between and among computers travel along much different routes, but "packet switching" communication protocols allow individual messages to be sub-divided into smaller "packets" which are then sent independently to a destination where they are automatically reassembled by the receiving computer.

The actual location of computers among which information is routed along the Internet is of no consequence to either the providers or recipients of information, hence there is no necessary connection between an Internet

address and a physical jurisdiction. Moreover, websites can be interconnected, regardless of location, by the use of hyperlinks. Information that arrives on a website within a given jurisdiction may flow from a linked sitter entirely outside that jurisdiction. For example, one packet of an e-mail message sent from California may travel via telephone line through several different states and countries on its way to Italy. Part of the "trip" may even go through a satellite in space. Meanwhile, another packet of the same message may travel by fibre-optic cable, arriving in Italy before the first packet, with both transmissions are completed in nanoseconds. Finally, not with standing the Internet's complex structure, the Internet is predominately a passive system; Internet communication only occurs when initiated by a user.

Many disputes involving electronic commerce arise between parties who are bound by a contract determining the terms and conditions upon which they have agreed to interact. Frequently, the contract itself may provide that any dispute concerning it is to be heard in the courts of a specified state ("choice of forum" clause or "forum selection" clause) and is to be determined under the substantive law of a specified state ("choice of law" clause).

Cyber sell is correct in its policy. First, in cyberspace as elsewhere, constitutional due process allows potential defendants to structure their conduct in a way to avoid the forum state. At the same time, to assume that a website operator can entirely avoid a given jurisdiction is unrealistic; because the web overflows all boundaries, the only way to avoid any contact whatsoever with a specific jurisdiction would be to stay off the Internet. For that reason, mere accessibility of a website should not properly be deemed to satisfy the Fourteenth Amendment minimum contacts requirements, and site operators should be able to structure their site use to avoid a given state's jurisdiction. As discussed below, this

reality has been recognized by regulators in the United States under federal securities laws.

As to contractual choice of law and forum, the following three principles should apply between buyers and sellers:

(a) Absent fraud or related abuses, forum selection and choice of law contract provisions could be enforced in business-to-business electronic commerce transactions.

(b) In business-to-consumer contracts, courts should enforce mandatory and non-binding arbitration clauses where sponsors have opted to use them, and should permit the development of a "law merchant," in exchange for:

(i) The sponsor's agreement to permit enforcement of any resulting final award or judgment against it in a state where it has sufficient assets to satisfy that award or judgment; and

(ii) The user's acceptance of an adequately disclosed choice of forum and choice of law clauses.

(e) Jurisdictional choices should be enforced where the consumer demonstrably bargained with the seller, or the choice of the consumer to enter into the contract was based on the use of a programmed consumer's bot deployed by or on behalf of the consumer and whose programming in the extent to which such protections are enforceable and other factors that could determine whether the user should enter into the contract.

Spiritual backing of the electronic media in the Justice System

Internet connection is not only present in the electronic media but the same is also present in our heart. This is called spiritual Internet.

Swami Chidanand Saraswati has said,

"Typically, outbursts of anger and frustration are due to our spiritual batteries being low. We overextend ourselves so much- physically, emotionally and energetically- every day and take such little time for personal replenishment. Just as the body needs many hours of sleep each day in order to be fresh, healthy and productive, so we also need to give time to our spirit to rest, withdraw and re-connect with the source. Meditation, silence, prayer- these are all ways in which our spirit reconnects with the Source and draws energy and inspiration from the infinite, Divine Ocean.

When our mobile phones lose battery charge what happens? The line becomes full of static. We cannot hear each other properly. Mistakes and miscommunications arise. We get "cut off: from each other. In order to solve the problem we have only to reconnect the phone to the charger which is plugged into the electrical outlet. In a short time the batteries will be recharged and our conversation can continue, clearly and uninterrupted.

The same is true in our lives. When our spiritual batteries run low our lives become full of static. We move through each day in an unplanned, unfocused and uncentered way. The connection to our deep Self, to the inner voice, to that sacred will of peace within us gets "cut off" and we wander aimlessly and without direction.

When our spiritual batteries are low we lose touch with the infinite Source of peace and joy; hence small events during the course of each day take on exaggerated importance and our emotional well-being is at the mercy of every person, every phone call and every traffic jam.

How to recharge our batteries? Just plug yourself back into the Source. Get connected again to God. Sometimes people mistakenly say, "God is so far away from me" or "God has left me". No. It is never like that. It is we who have left God, we who have gone astray. The moment we re-connect, the connection is there.

The spiritual corner should be the place where we reconnect to the Divine Source, where we recharge our batteries. When our batteries are charged we can hear not only each other clearly but we can also clearly hear the inner, Divine voice."

In the Bhagwat Gita, Lord Krishna has described meditation as one of the method to reach to Almighty. Thus the Internet facilities were available in the old times also which has been suitably described in the Bhagwat Gita in various chapters.

In Chapter-7 of Bhagwat Geeta, it has been stated as under:

"God is the origin of the whole creation. Wielding His own nature, He brings forth the whole creation. This nature is called the lower Nature (Apara prakrti), while the embodied soul, which is a fragment of God, is called higher nature (para prakrti). The lower nature, is inferior, insentient and changeful while higher nature is superior, sentiment and changeless".

For adjudicating of the dispute under the Information Technology Act, Section 46 was enacted which has given the power for adjudication of the crimes. The power has been given to the Secretary, Information Technology and he has power to adjudge the quantum of compensation under Sections 46 and 47 of the Act. Sections 46 and 47 are quoted below:

46. Power to adjudicate.-

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made hereunder the Central Government shall, subject to the provisions of Sub-section (3),appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer or holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in Sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3)No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4)Where more than one adjudicating officer are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5)Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Sub-Section (2) of Section 58, and-

(a)All proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860)

(b)Shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974)

47. **Factors to be taken into account by the adjudicating officer.** -

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely-

(a)The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.

(b)The amount of loss caused to any person as a result of the default;

(c) The repetitive nature of the default.

Sections 43 and 44 of the Information Technology Act,2000 provides penalties and their Adjudication. It reads as under:

Penalties and Adjudication

43. Penalty for damage to computer to computer, computer system etc.- If the person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-
    - (a) Accesses or secures access to such computer, computer system or computer network;
    - (b) Downloads, copies or extracts any data, computer date-base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
    - (c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
    - (d) damages or causes to be damaged any computer, computer system or computer network, data computer data base or any other programmes residing in such computer, computer system or computer network;
    - (e) disrupts or causes disruption of any computer, computer system or computer network;
    - (f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act. Rules or Regulations made hereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.-For the purposes of this section-

(i)"computer contaminant" means any set of computer instructions that are designed-
(ii)to modify, destroy, record, transmit data or programme residing within a computer system or computer network;
by any means to usurp the normal operation of the computer, computer system or computer network;

(ii) "computer data-base" means a representation of information knowledge, facts, concepts or instructions in text, image, audio, \ video that are being prepared or have been prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or system or computer network and are intended for use in a computer, computer system or computer network.

(iii) "Computer virus" means any computer instruction; information, data or programme that destroys, damages degrades or adversely affects the performance of a computer.

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information, return, etc.- If any person who is required under this Act or any rules or regulations made thereunder to-

(i) furnish any document, return or report to the Controller of the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(j) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(k) maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.- Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty five thousand rupees.

The offences under the Information Technology Act are as under:

Section 65. Tampering computer source documents.-Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.

Section 66 . Computer related offence.- If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
.

Section 66A. Punishment for sending offensive messages through communication service etc. Any person who sends, by means of a computer resource or a communication device.-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently

by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device. – Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C:Punishment for identity theft.-Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D:Punishment for cheating by personation by using computer resource.-Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Punishment for violation of privacy.-Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three yeas or with fine not exceeding two lakh rupees, or with both.

Section 66F. Punishment for cyber terrorism:-

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike

terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70 or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise.

Commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.'

Section 67. Punishment for publishing or transmitting obscene material in electronic form.-Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to

deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B:Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.-Whoever-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuses or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for

a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Provided that provisions of Section 67, Section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form.

Section 67C. Preservation and retention of information by Intermediaries. (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

Section 70. Protected system.-(1)The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub section (1).
(3)Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Section 71.Penalty for misrepresentation.—Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or (Electronic Signature) Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72. Breach of Confidentiality and Privacy.- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without

the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72A Punishment for disclosure of information in breach of lawful contract.—Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Section 73. Penalty for Publishing (Electronic Signature) Certificate false in certain particulars.- (1) No person shall publish a (Electronic Signature) Certificate or otherwise make it available to any other person with the knowledge that-

(a) the Certifying Authority listed in the certificate has not issued it, or
(b) the subscriber listed in the certificate has not accepted it, or
(c) the certificate has been revoked or suspended.,

unless such publication is for the purpose of verifying a (electronic signature) created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

.

Section 78 of I.T. Act empowers Inspector of Police to investigate cases under the Act

JURISDICTION UNDER THE INDIAN PENAL CODE IN RELATION TO CYBER OFFENCES

(i)Sending threatening messages by email Section 503 IPC

(ii)Sending defamatory messages by email Section 499 IPC

(iii)	Forgery of electronic records	Section 463 IPC
(iv)	Bogus websites, cyber frauds	Section 420 IPC
(v)	Email spoofing	Section 463 IPC
(vi)	Web-jacking	Section 383 IPC
(vii)	E-Mail Abuse	Section 500 IPC
(viii)	Online sale of Drugs	NDPS Act
(ix)	Online sale of Arms	Arms Act

For adjudicating the aforesaid crimes, the power has been given to the Adjudicating Officer. After the decision of the Adjudicating Officer, the appeal lies to the Appellate Tribunal under Section 48 of the Information Technology Act,2000. It reads as under:

"48.Establishment of Cyber appellate Tribunal.- (1) The Central Government shall, by notification, establishes one or more appellate tribunals to be known as the Cyber Regulation Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in Sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction."

He exercises the powers contained under Section 58 of the Information Technology Act, which reads as under:-

58. Procedure and powers of the Cyber Appellate Tribunal.-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2)The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are

vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely-
(a)Summoning and enforcing the attendance of any person and examining him on oath;

(b)Requiring the discovery and production of documents or other electronic records;

(c)Receiving evidence on affidavits;

(d) Issuing commissions for the examination of witnesses or documents;

(e) Reviewing its decisions

(f) dismissing an application for default or deciding its ex parte;

(g) any other matter which may be prescribed.

(3)Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228, and for the purposes of Section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure.

Section 61 of the Information Technology Act, 2000 also debars the civil court in respect of the matters which are being tried by the Cyber Tribunal and directly the appeal goes to the High Court against the judgment of the Cyber Appellate Tribunal.

As per report of Deputy Inspector General of Police, Panaji, Goa upto February,2010, there are 22 cases pending and some of the cases are Under Section 66 of the IT Act,2000 and some of the cases are under Section 66A and 67 of the IT Act,2000. Three cases are under Section 420 IPC. Some cases are under Section 43, 43(a)(b) and(h) of the IT Act. As per report, last case was filed on 16.5.2009. All the cases are still pending. When I had a meeting with the Secretary (IT) personnels and police officers at Goa, I had directed them to disposes of these cases promptly.

The following table shows the number of cases reported at Cyber Crime PS, Hyderabad with head wise break up during 2008 & 2009. There is no exclusive designated Court for the Cyber Crime Police Station, CID.

	Source Code Tampering (Sec. 65 IT Act)	Hacking (Sec. 66 IT Act)	Obscene Content (Sec. 67 IT Act)	Nigerian Fraud	Phishing	Credit and Debit Card misuse	Others	Total
2008	-	7	2	2	10	-	1	22
2009	1	4	5	6	7	3	2	28

Since inception the officers and staff of Cyber Crime Police station, CID kept up the expectations and successfully investigated the reported cases. The IPC cases, the investigation of which require computer skills are also investigated at Cyber Crime PS on being specially entrusted by the chief of CID. The case in Crime No. 17/2008 U/s 419,420,468 & 471 IPC requires special mention where in an amount of Rs. 48 Lakhs was siphoned off by two young educated offenders from the ICICI Bank, Khairathabad SB Account. In this case the offenders have exploited the loopholes that prevailed in the Banks and others financial institutions and committed the fraud. One of the accused persons worked in the call centre of ICICI Bank on temporary basis, by which he could gain the critical information of the account having found huge balance. Then he along with co-accused opened false India Bulls trading account and also false AXIS

bank account. They have first transferred the amount from the victim's ICICI Bank SB Account to India Bulls account and from that to fake Axis Bank account, Tarnaka Branch, Hyderabad from where they could withdraw the whole amount. After the detection of the case, a letter was addressed to the Reserve Bank of India mentioning the instances of loopholes in the banking system exploited by the culprits for executing the said fraud and with advice to take necessary corrective steps on the loopholes in the banking system. There are already indications that RBI has moved swiftly and alerted all the banks on this count and directing them to adhere more stringently to the guidelines. Similarly CBI, DOT are also addressed about such system loopholes that have come across while the investigation of cyber offences. In specific addressed letters to DOT with reference shared IP Addresses and to CBI with reference to Bank Frauds, e-mail high jacking, Nigerian frauds.

Institute of Forensic Science

Day by day, law and enforcement agencies find it necessary to regulate the activities that influence our daily lives with the assistance of science. Laws are continually being broadened and revised to counter the increasing crime rates. At the same time they are looking more and more to the scientists for technical support. As a result, the Enforcement agencies as well as forensic laboratories have expanded their investigative functions and methods.

Forensic science plays an important role in criminal justice delivery system. Besides routine work in the laboratory, there is another important dimension to the role that a forensic scientist plays that is participating in the criminal investigation process. A forensic scientist's ability reflects at the crime scene where he is required to give accurate and objective information regarding the sequence of events that have occurred at crime scene. He is not only

required to collect and preserve the physical evidence, but also contributes a highly professional and unique perspective to develop the crime scene reconstruction by the observation and evaluation of physical evidence.

The Central Forensic Science laboratory, Kolkata is a premier Science and Technology Institution which was established in the year 1957 with basic four disciplines of forensic science viz. Ballistics, Biology, Chemistry and Physics divisions under Union Ministry of Home. Later on laboratory was placed in the year 1971 under administrative control of a newly carved out department-BPR&D. In the year 2003, a separate Directorate of Forensic Science was created consisting of three Central Forensic Science Laboratories located at Kolkata, Hyderabad, Shimla, Chandigarh and Allahabad.

The Central Forensic Science Laboratory (CBI) New Delhi was established in the year 1968. The Laboratory at New Delhi is one of the most comprehensive Laboratories in the country

As per report, during the year 2007, the Laboratory scientists gave expert testimony in 261 courts in Delhi and other parts of India and examined 82 Scene(s) of crime at Delhi and outside for scientific investigation of crimes. The services of this forensic science were also provided to Delhi Police, CBI and Judicial courts. Forensic assistance was also provided to Directorate of Revenue Intelligence, Banks, Cabinet Secretariat Board and other public undertakings on regular basis.

In the Kerala State from the year 2005 to April,2009, 135 cases under IPC and Sections 43,65,66,66(2),67 and 72 of the I.T.Act are stated to be under investigation .

As per statistics of Cyber Crime cases registered in Kochi city from the year 2005 to April,2009 , there are 27 cases registered under IPC and Sections 66,67 and 72 of the I.T.Act upto April,2009 which are stated to be under investigation.