Lecture in the Workshop on Cyber Law organized by Asian School of Cyber Laws, Pune under the guidance and supervision of the Cyber Appellate Tribunal, New Delhi on 28th August,2010 at Maharatta Chamber of Commerce, Industries & Agriculture, Pune on the topic of Cyber Law & Adjudication Issues in India.

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

CYBER LAW & ADJUDICATION ISSUES IN INDIA

The topic today i.e. Cyber law & Adjudication Issues in India is a topic which concerns the theme of the Cyber Law. The remedies as well as punishment is contained under the Information Technology Act relating to the Cyber crime. In order to elaborate the theme of cyber law, one has to look to the dictionary meaning where the meaning of cyber law has been defined and the Act from whom it has been borrowed is relevant.

In the Advanced Law Lexicon dictionary, the `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.

The Information Technology Act, 2000 was introduced on 9th June,2000. The Information Technology Act,2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October, 2009.

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 provides 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."

Coming to the definition of the Communication device which has come into force under the amended Act i.e. Section 2 (ha) of the IT Act,2000 which reads as under:-

> (ha) "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;

In the earlier Act of 2000, the word `Computer" has also been defined which reads 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;

According to its preamble, the IT Act basically seeks to:

Provide legal recognition for electronic commerce.

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."

Section 75 of **the Information Technology Act, 2000 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 computer network located in India.

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

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

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

CYBER CRIMES

Cyber crimes have become ubiquitous today. The motive behind most cyber crimes remains the same as that of physical crimes although the technical means to execute them vary. The ingenuity of cyber criminals is becoming obvious when we look at the clever ways in which online frauds are being perpetrated. Phishing, a particularly crafty fraud attack perpetrated by cyber criminals combines elements of forgery, misrepresentation and misplaced trust to obtain sensitive personal data like PIN numbers, credit card details, passwords, etc., of victims. The attackers then rob the victims of their hard earned money by using such personal information.

Other forms of cyber crimes include hacking, unauthorized access to data or resources, alteration of information and electronic mail based offences. These

crimes are universal in nature with scant regard for national boundaries. The anonymity offered by the Internet and the safe haven of foreign jurisdictions make cyber crimes an attractive proposition for prospective cyber criminals.

The Information Technology Act deals with the following cyber crimes along with others:

(i) *Tampering with computer Source Documents:* A person who knowingly or intentionally, conceal (hides or keeps secret), destroys (demolishes or reduces), alters (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law is punishable. For instance, hiding the C.D.ROM in which the source code files are stored, making a C File into a CPP File or removing the read only attributes of a file.

(ii) *Hacking:* Hacking is usually understood to be the unauthorized access of a computer system and network. Originally, the term "hacker" describes any amateur computer programmer who discovered ways to make software run more efficiently. Hackers usually "hack" on a problem until they find a solution, and keep trying to make their equipment work in new and more efficient ways. A hacker can be a Code

Hacker, Cracker or a Cyber Punk. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by means is said to commit hacking.

(iii) *Publishing of Information, which is Obscene in Electronic Form:* A person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it, is liable to punishment. The important ingredients of such an offence are publishing (make generally known or issue copies for sale to public), or transmitting (transfer or be a medium for), or causing to be published (to produced the effect of publishing), pornographic material in the electronic form.

(iv) *Child Pornography:* Child Pornography is a part of cyber pornography but it is such a grave offence that it is individually also recognized as a cyber crime. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The Internet is very fast becoming a household commodity in India. Its explosion has made the children a viable victim to the cyber crime. As more homes have access to Internet, more children would be using the Internet and more are the chances of falling victim to the aggression of pedophiles. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. They even start

contacting children on their e-mail addresses. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object.

(v) *Accessing Protected System* : Any unauthorized person who secures access or attempts to secure access to a protected system is liable to be punished with imprisonment and may also be liable to fine.

(vi) *Breach of Confidentiality and Privacy:* Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable I to be punished under the Information Technology Act.

CYBER CRIMES OTHER THAN THOSE MENTIONED UNDER THE INFORMATION TECHNOLOGY ACT

(i) *Cyber Stalking :* Although there is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behaviour of the cyber criminal towards the victim by using Internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

(ii) *Cyber squatting:* Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different) A trademark owner can prevail in a cyber squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of-pocket expenses.

(iii) *Data Diddling:* This kind of an attack involves altering the raw data just before a computer processes it and then changing it back after the processing is completed. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipts and bank remittances.

(iv) *Cyber Defamation:* Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as liable or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

(v) *Trojan Attack:* A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(vi) *Forgery:* Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. IT is very difficult to control such attacks. For e.g. across the country students buy forged mark sheets for heavy sums to deposit in collage.

(vii) *Financial Crimes:* This would include cheating, credit card frauds, money laundering etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts.

(viii) *Internet Time Theft:* This con notes the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it . This offence is usually covered under IPC and the Indian Telegraph Act.

(ix) *Virus/worm Attack:* Virus is a program that attaches itselves to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

(x) *E-mail spoofing:* It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc. E.g. if A sends email to B's friend containing ill about him by spoofing B's email address, this could result in ending of relations between B and his friends.

(xi) *Email Bombing:* Email bombing means sending large amount of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider.

(xii) *Salami Attack* This is basically related to finance and therefore the main victims of this crime are the financial institutions. This attack has a unique quality that the alternation is so insignificant that in a single case it would go completely unnoticed.

E.g. a bank employee inserts a programme whereby a meager sum of Rs. 3 is deducted from customers account. Such a small amount will not be noticeable at all.

(xiii) *Web lacking:* This terms has been taken from the word hijacking. Once a website is web jacked the owner of the site loose all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site.

Coming to the crime factors, in nut shell the same are defined as under:

Section	**Offence**	**Punishment**
43	Damage to Computer, Computer system etc.	Compensation to the tune of Rs.1 crore to the affected person.
44(a)	For failing to furnish any document, return on report to the Controller or the Certifying Authority.	Penalty not exceeding one lakh and fifty thousand rupees for each such failure.
44(b)	For failing to file any return or furnish any information or other document within the prescribed time.	Penalty not exceeding five thousand rupees for every day during which such failure continues.
44(c)	For not maintaining books of account or records.	Penalty not exceeding ten thousand rupees for every day during which the failure continues.
45	Offences for which no penalty is separately provided.	Compensation not exceeding twenty five thousand rupees to the affected person or a penalty not exceeding twenty five thousand rupees.
65	Tampering with computer source documents.	Imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.
66	Hacking with computer system with the intent or knowledge to cause wrongful loss.	Imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.
66A	For sending offensive messages through communication service etc.	Imprisonment for a term which may extend to three years and with fine.
66B	For dishonestly receiving stolen computer resource or communication device.	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.
66C	For identity theft	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.
66D	For cheating by personation by using computer resource.	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.
66D	For cheating by personation by using computer resource.	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.
66E.	For violation of privacy	Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
66F	For cyber terrorism	Imprisonment which may extend to imprisonment for life.
67	Publication of obscene material in an electronic form.	Imprisonment upto 5 years and with fine which may extend to one lakh rupees on first conviction and its double punishment for second and subsequent convictions.
67A	For publishing or transmitting of material containing sexually explicit act etc. in electronic form.	Imprisonment upto 5 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.
67B	For publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.	Imprisonment upto five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of seven years and also with fine which may extend to ten lakh rupees.
67C	For preserving and retention of information by Intermediaries.	Imprisonment upto three years and also liable to fine.

68	For failing to comply with the directions of the Controller.	Imprisonment upto 3 years and fine upto two lakhs, or both.
69	For failing to extend facilities to decrypt information which is against the interest of sovereignty or integrity of India.	Imprisonment which may extend to seven years.
70	Securing or attempting to secure access to a protected system.	Imprisonment which may extend to 10 years and fine.
71	For misrepresentation or suppression of any material fact from the Controller or the Certifying Authority.	Imprisonment upto 2 years, or fine upto rupees one lakh or with both.
72	For break of confidentiality and privacy	Imprisonment upto two years or fine upto rupees one lakh, or with both.
72A	For disclosure of information in breach of lawful contract.	Imprisonment upto three years or with fine upto five lakh rupees or with both.
73	For publishing digital signature certificate false in certain particulars.	Imprisonment upto two years or with fine which may extend to one lakh rupees or with both.
74.	Publication of Digital Signature Certificate for any fraudulent or unlawful purpose.	Imprisonment upto two years or fine upto rupees one lakh.
76	Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto used for contravention of this Act, rules, orders or regulations made thereunder.	Liable to confiscation.

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
(x)	Pornographic	Section 292 IPC

For adjudicating the aforesaid crimes, the power has been given to the Adjudicating Officer

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-

(a) 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;

(b) 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;

(c) 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.

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

After the decision of the Adjudicating Officer, the appeal lies to the Appellate Tribunal under Section 48 of the Information Technology Act,2000. Section 48 of the IT Act,2000 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."

Cyber Appellate Tribunal 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.

I have also examined the Police and Justice Act,2006 and the Terrorism Act,2000, applicable to the UK.

The Police and Justice Act,2006 establishes a National Policing Improvement Agency for making other provisions and also to amend the Computer Misuse Act,1990, to make provisions about the forfeiture of indecent images of children and to provide for the conferring of functions on the Independent Police Complaints Commission in relation to the exercise of enforcement functions by officials involved with immigration and asylum.

In the Police and Justice Act, 2006, Section 35 states about Unauthorized access to computer material.

Section 36 relates to Unauthorised acts with intent to impair operation of computer etc.

Section 37 relates to Making supplying or obtaining articles for use in computer misuse offences.

Section 39 relates to Forfeiture of indecent photographs of children: England and Wales

Section 40 relates to Forfeiture of indecent photographs of children: Northern Ireland.

Section 44 relates to Transfer of prisoner under international arrangements not requiring his consent

Terrorism Act, 2000 is an Act to make provision about terrorism, and to make temporary provision for Northern Ireland about the prosecution and punishment of certain offences, the preservation of peace and the maintenance of order.

Section 17 of the Act relates to funding arrangements.

Section 18 of the Act relates to Money laundering.

Section 19 of the Act relates to Disclosure of information

In **Bunt v Tilley and others*[1]** 2006 Vol. 3 All England Reports reliance has been placed on the Judgments of:

1. Anderson v New York Telephone Co. (1974) 35 NY 2d 746, NY Ct of Apps
2. Byrne v Deane {1937] 2 All ER 204, [1937] 1 KB 818, CA
3. CBS Songs Ltd. V Amstrad Consumer Electronics plc [1988] 2 All ER 484, [1988] AC 1013, [1988] 2 WLR 1191, HL.
4. Cubby Inc v CompuServe Inc (1991) F Supp 135, Ny Dc.
5. Douglas v Hello! Ltd. [2003] EWHC 55 (Ch), [2003] 1 All ER 1087N.
6. Emmens v Pottle (1885) 16 QBD 354, CA
7. Godfrey v Demon Internet Ltd. [1999] 4 All ER 342, [2001] QB 201, [2000] 3 WLR 1020
8. Jameel (Yousef) v Dow Jones and Co Inc [2005] EWCA Civ 75, [2005] QB 946, [2005] 2 WLR 1614
9. Lunney v Prodigy Services Co (1998) 250 AD 2d 230, NY SC (App Div).
10. MCA Records Inc v Charly Records Ltd. [2001] EWCA Civ 1441, [2003] 1 BCLC 93
11. McLeod v St Aubyn [1899]AC 549, PC

12. Milne v Express Newspapers Ltd. [2004] EWCA Civ 664, [2005] 1 All ER 1021, [2005] 1 WLR 772
13. PLG Research Ltd. V Ardon International Ltd. [1993] FSR 197, Patent Ct.
14. Schellenberg v BBC [2000] EMLR 296
15. Stratton Oakmont Inc Prodigy Services Co (1995) 23 Media L Rep 1794, NY SC
16. Totalise Plc v Motley Fool Ltd. [2001] EWCA Civ 1897. [2003] 2 All ER 872, [2002] 1 WLR 1233
17. Wallis v Valentine [2002] EWCA Cibv 1034, [2003] EMLR 175
18. Zeran v America Online Inc (1997) 129 F 3d 327, US Ct of Apps (4th cir)

Relying upon the above cases, it has been held by the House of Lords,

> "The proceedings in libel in respect of statements posted on websites, the responsibility was attributed the internet service providers. The point in issue before the Court was as to whether an internet service provider could be liable in respect of material which was simply communicated via the services which they provided on the evidence. It was found by the house of lords that the claimant has no realistic prospect of being able to establish tht any of the internet service provider knowingly participated in the relevant publications."

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.

As per report of Deputy Inspector General of Police, Panaji, Goa upto August,2010, there are 23 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.

Some of the instances which are given above relates to the Cyber crime cases which are pending in under investigation.

(i) The Complaint in Cr.No.74/2009 relates to the Section 420 IPC read with Section 66 of the IT Act,2000 where a false e-mail was sent directing the complainant to deposit an amount of Rs.1,69,420/- as he has won the COCO COLA contest of one lakh Pounds. On the investigation he was arrested at Imphal East Manipal. This case is still under investigation.

(ii) Similar complaint under Section 420 IPC read with Section 66 of IT Act,2000 was filed for depositing a sum of Rs.35000/- towards custom charges to Elite Creative with PAN No.AMGPA2286A, ICICI Bank branch New Delhi. This case is still under investigation.

(iii)In the another complaint under Section 67 IT Act,2000, the complaint was lodged when husband has transmitted SMS having vulgar and malicious text on his wife's mobile and the husband was arrested and was released on bail. This case is still under investigation.

(v) In a case Under Section 66 of the IT Act, a website www.magicmasons.com was lodged for personal gain and he was arrested on 15.12.2009.

Other complaints are also relating to Nigeria fraud.

(vi) Case No.72/2009 is under Section 66 of the IT Act,2000. In this complaint the complainant complained that some unknown accused person gained access without permission to the

computer system of HDFC Bank and purchased tickets for travel worth Rs.30,000/-. This case is still under investigation.

(vii) Case No.99/2008 under Section 66 of the IT Act also relates to purchase of airline tickets in four transactions of Rs.7200/- each and is still under investigation.

(viii) Case No.29/2009 under Section 66(A) of the IT Act is regarding insult to the complainant and hurt the integrity in her individual and professional capacity and is still under investigation.

(ix) Case No.Cr.No.131/10 under Section 379 IPC & 66(c), 66(d), 67(a) of the IT Act is a complaint of hacking, theft and cheating. In this case the accused was arrested on 16.4.2010 and the case is still under investigation.

(x) Case No.Cr.No.126/10 under Section 66(C) of the IT Act is a complaint filed on 6.5.2010 by Ms.Sandhya Pandurang Naik stating that some unknown accused person created false E-mail ID of the complainant lady as Sandhya Naik @Gmau.com and thereby committed theft of e-mail. The case is under investigation.

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, Hyderabad 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.

(i) 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.

(ii)In case No.15/2009 under Sections 66 and 67 IT Act, the accused while at UK pursuing higher studies has created various fictitious e-mail Ids and sent obscene e-mails to the victim woman.

(iii)In case No.19/2009 filed under Sections 66(D), 66(B) of IT Act read with Section 420 IPC, the accused while working in cyber café, installed a special type of software and secured clandestinely critical information of banking accounts of the customers and purchased a mobile phone worth Rs.30,600/- by making online payment.

In Hyderabad most of the cases are phishing frauds by which bank accounts are broken into and transactions made. There are about 18 cyber crime cases including Nigerian Fraud registered at different Police Stations across Andhra Pradesh State.

In the State of Andhra Pradesh incidence and report of Cyber offences is growing year by year and with the enactment and notification of the amended Act,2008 cyber offences is expected to be more at the cyber crime Police stations.

Kerala

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 under investigation .

Kochi city

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 under investigation.

In the Cyber Cell, Kochi City during the year 2008, 82 cyber petitions were filed and during the year 2009, 213 cyber petitions were filed. All the cyber petitions relate to E mail ID Hacking, E mail Abuse, Orkut Abuse, Internet Time Theft, Credit Card Fraud, Online Job fraud, online Lottery scam, online ticket fraud, website defacing, website design copying, financial fraud/E commerce cheating, Mobile abuse through internet, website hacking/blocking, subscription fraud, server hacking, mobile hacking, posting of new Malayalam films in website, lap top lost,

data theft and obscene MMS in Internet. All the cases are under investigation.

During the year 2008, 216 complaints were of abuse, 1694 complaints were of Mobile lost and 216 complaints were of Mobile theft. In the year 2009 complaints of abuse increased to 620, complaints of Mobile lost increased to 3000 and complaints of Mobile theft increased to 568.

West Bengal (Kolkata)

On 12.8.2010, Secretary IT, West Bengal has forwarded a copy of the report in connection with the cases registered under the provisions of the Information Technology Act,2000 received from the Criminal Investigation Department, West Bengal Police.

As per the statement of pending cases, five cases are pending in the **District Howrah** which are still under investigation.

In the **District of Burdwan,** 13 cases are pending .

In the **District of North 24 Pargana,** 16 cases are pending.

In the District of **South 24 Pargana**, 8 cases are pending.

In the **District Jalpaiguri,** 7 cases are pending .

In the **District Hooghly** only one case is pending.

In the **District Nadia**, two cases are pending.

In the **district Medinipur (East)**, only one case is pending.

In the **above Districts**, all the cases are stated to be still under investigation. But in the Districts of Medinipur (West), Purilia, Bankura, Malda, Uttar Dinajpur, Darjeeling, Dakhshi Dinajpur, Cooch Behar, Birbhum and Murshidabad, no cases were registered under the provisions of the Information Technology Act,2000.

In all the above cases, the modus operandi is threatening by e-mail/SMS, defamation, personal gain, data theft, credit card fraud through

internet, publishing obscene materials in electronic form, cheating, sexual harassment through obscene e-mail, threaten of bomb blast, hacking of broadband connection etc.

CYBER SECURITY

Cyber security is very important to protect businesses, governments and general public at large. The same must be a part of the national policy of a nation. Unfortunately, Cyber security in India is an ignored world. The cyber security strategy of India is defective and deficient and is violating the ICT rights of Indian citizens. There are many factors that are ailing cyber security in India. The consequence of the same can be found in the form of recent breach in key MEA computers where several of its computers were infected by malware.

Cyber security actually protects your personal information by responding, detecting and preventing the attack. Cyber security is actually introduced to decrease cyber crimes. All banking institutions and businesses today run their businesses online. Hackers can hack your computer system and misuse your personal information and pictures. Various other dangerous associated with cyber crimes are entry of virus into your system, altering your files, change of password stealing credit card information and make unauthorized purchases.

Security is one of the biggest concerns that affect the world today. Not only in security in the actual world a matter of concern but security in the context of the electronic format and the information stored therein has become a matter of immense concern.

Security is the degree of protection against danger, loss and criminals. Security has to be compared and contrasted with other related concepts; Safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of people attempting to cause destruction.

The word security is derived from the Latin “Se-Cura” and literally translates to “without fear”. `Security’ is, therefore the state of being secure,

or the actions employed to achieve that state i.e. to be secure is to be without fear of harm.

The definition of security provided by the Institute for Security and Open Methodologies (ISECOM) in the Open Source Security Testing Methodology Manual-3 (OSSTMM-3) is geared towards operations and how we interact with security. It states security is:

"A form of protection where a separation is created between the assets and the threat. This includes but is not limited to the elimination of either the asset or the threat. In order to be secure, either the asset is physically removed from the threat or the threat is physically removed from the asset."

It is very often true that people's perception of security is not directly related to actual security. For example, a fear of earthquakes is much more common than a fear of slipping on the bathroom floor; however, the latter kills far more people than the former.

In the corporate world, various aspects of security were historically addressed separately- notable by distinct and often non-communicating departments for IT security, physical security, and fraud prevention. Today there is a greater recognition of the interconnected nature of security requirements, an approach variously known as holistic security, "al hazards" management, and other terms.

As the world is moving towards the information society, it is natural to expect an increase in the emphasis on security.

Security of information and networks are both of tremendous significance. Their significance has further been enhanced due to the onset of Cyber Terrorism in a big way.

In Section 70 of the principal Act, the following sub-section are substituted, namely,

(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.

After sub-section (3), the following sub-section is inserted, namely,

(3) The Central Government shall prescribe the information security practices and procedures for such protected system.

After Section 70 of the principal Act, the following sections are inserted, namely:-

70A (1) The Central Government may, by notification published in the Official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2)The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.

(3)The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70B. (1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2)The Central Government shall provide the agency referred to in sub-section (1) with a Director-General and such other officers and employees as may be prescribed.

(3)The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security;-

(4) Collection, analysis and dissemination of information on cyber incidents;
(5) Forecast and alerts of cyber security incidents;
(6) emergency measures for handling cyber security incidents;
(7) coordination of cyber incidents response activities;
(8) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
(9) such other functions relating to cyber security as may be prescribed.

CYBER CRIMES IN OTHER COUNTRIES

MALAYSIA

Before analyzing the cyber crime related laws in Malaysia, it is important to have a basic understanding about the foundation of the Malaysian legal system.The Constitution of Malaysia provides for a dual justice system – the secular laws (criminal and civil) and sharia laws (applicable for Muslims in personal law matters e.g. marriage, inheritance etc).

Federal laws enacted by the Parliament of Malaysia apply throughout the country while state laws enacted by the State Legislative Assemblies apply to the particular state.

The application of English law or common law is specified in the statutes. Section 5 of the Criminal Procedure Code states that English law shall be applied in cases where no specific legislation has been enacted. Similarly, in the context of civil law, Sections 3 and 5 of the Civil Law Act allows for the application of English common law, equity rules, and statutes in Malaysian civil cases where no specific laws have been made.

The investigation of crimes comes under enforcement agencies like the Royal Malaysian Police, Anti Corruption Agency, Royal Customs and Excise, Securities Commission etc. The prosecution is under the Attorney General.

SINGAPORE

Before analyzing the cyber crime related laws in Singapore, it is important to have a basic understanding about the foundation of the Singapore legal system. According to the Singapore Ministry of Law website: Singapore is a republic with a parliamentary system of Government.

The roots of Singapore’s legal system can be traced back to the English legal system and it has evolved over the years. The sources of law are derived from our Constitution, legislation, subsidiary legislation (e.g. Rules and Regulations etc) and judge-made law.

The Constitution is the supreme law of the land and lays down the basic framework for the three organs of state, namely, the Executive, the Legislature and the Judiciary.

The Executive includes the Elected President, the Cabinet and the Attorney-General. The President is elected by the people and is empowered to veto government budgets and appointments to public office. The Cabinet comprises of the Prime Minister and Ministers appointed from among the Members of Parliament and is responsible for the general direction and control of the Government and is accountable to Parliament. The Attorney-General is the principal legal advisor to the government and has the power and discretion to prosecute offenders.

The Legislature comprises the President and parliament and is the legislative authority responsible for enacting legislation. Parliament is made up of elected, non-constituency and nominated Members of Parliament. The President's assent is required for all bills passed by Parliament and he may in his discretion withhold assent to certain bills.

The Judiciary consists of the Supreme Court and the Subordinate Courts and the head of the Judiciary is the Chief Justice. Judicial power in Singapore is vested in the Supreme Court and in such subordinate courts as may be provided for by any written law for the time being in force.According to the Supreme Court website:

Although Singapore became independent on 9 August 1965, the ties between the judicial systems of Singapore and Malaysia were not severed until 1969. The Supreme Court of Judicature Act 1969, re-established the supreme Court of Singapore, comprising the High Court, the Court of Appeal and the Court of Criminal Appeal.

Jury trials were abolished in 1969. The next important milestone for Singapore's judicial system was the introduction of judicial Commissioners to the Supreme Court Bench, with the first Judicial Commissioner being appointed on 1 July, 1986. A Judicial Commissioner is appointed for specific

periods of time and may exercise the powers and perform the functions of a Judge. In this capacity, he enjoys the same immunities as a Judge.