6. **LEGAL CONTROL OF CYBER CRIMES UNDER I.T. ACT.**

In India the issue of cyber crime arose in late 1990s, so only when however there was no law on it in India. Cyber Crime is the new member to the family of crimes and in true sense these crimes were found to be committed in 1990s before which Internet was not accessible to the public. The crimes committed exploiting computer telecommunications in the 1980s and 1990s were telecommunication crimes as the cases of Vladimir Levin, Solar sunrise, Phone master, Rome Lab etc.

But all these were taking place in USA, UK, and Europe, the Western hemisphere of the globe. India became member of cyber world in 1995 through the GIAS, VSAT, and other modern digital networks. To have a legal control of the emerging situation the Information Technology Act 2 was enacted and enforced following UN Model Law and some other national legislations like Singapore, UK, Australia, USA etc. The traditional criminal system along with the basic principles are applied to deal with the Internet related crimes. And a close co-operation and mutual assistance program has been taken to deal with the cross border crimes.

"The Cyber Crimes can be effectively managed with whatever laws are in place provided they can be investigated in a way to gather sufficient evidence for prosecuting criminals. The examination of computers communication equipment and systems for obtaining information for criminal or civil investigations has come to be known as Forensic Computing." *1.

6.1 **CYBER AGE IN INDIA**

The Gateway Internet Access Service (GIAS) gave a new turn to the Information and Communication Technology (ICT) in India. GIAs network passing through Mumbai – Chennai Pune Kolkata and Delhi was opened for the public on 15 August 1995 by Videsh Sanchar Nigam Limited (VSNL). Before this very limited access to the Internet was possible through the ERNFT (Education and Research Network) and Compu Serve (an ISP in America).

The VSAT (Very Small Aperture Terminal) technology based on satellite was also introduced by VSNL in March 1996 through its' Demand Assigned Multiple Access (DAMA) service in March 1996. “Satellite based VSAT is a digital satellite communications network that directly connects geographically dispersed offices / operational locations into an integrated network. The service offers connectivity with multimedia capabilities such as ability to compress text, data files and voice. VSAT was commercially introduced in the USA market during the 1980s.” *2.

The modern communication technology in India is said to have started with the electric telegraph network along railway tracks in the second half of 19th century. And the relevant law the Indian Telegraph Act 1885 is still now in force. The Government exercises general control and governance over the telegraph network through the Department of Telegraph (1885). Then the Telecom Regulatory Authority of India (TRAI) was formed in 1997.

---

In the mid-1990s when GIAS network provided public access to the Internet there was no law in this subject except the Indian Telegraph Act 1885. The relevant provisions under the Telegraph Act 1885. are --- S/3 Telegraph means any appliance used for transmission or reception of signs, signals by wire, electromagnetic & missions, radio waves etc. and S/25 - provides for intentionally damaging or tampering with telegraphs attracting a penalty of imprisonment of three years or fine or both.

In the mean time UN – prepared and published a Model Law in 1998 for electronic commerce, norms for making contracts in the electronic medium as a general guide line to all nations having Internet facility And the Government of India drafted the Electronic Commerce Bill – 1998, but it was left in the mid way and the newly formed the Department of Information Technology prepared another draft and this was then enacted as the Information Technology Act which came into force or 17th October 2000. The IT Act at the same time provided with some relevant changes through amendments in four Acts namely The Indian Penal code – 1860, The Reserve Bank of India Act 1934. The Act also provided for some Rules and guidelines. Such as The Information Technology (Certifying Authorities) Rules – 2000, The Information Technology (IT) Security Guide lines, framed under rule 19(2) of the IT rules – 2000. Some more Rules Orders Regulations are framed in relation to the IT Act. These are * (1) The Information Technology (Certifying Authorities) Regulations – 2001, (2) The Cyber Regulations Appellate Tribunal (Procedure) Rules 2000, (3) The Information Technology (Removal of Difficulties) order – 2002; (4) The Negotiable Instruments (Amendment and Miscellaneous Provisions) Act 2002.


Thus before the enactment of the IT Act in 2000 the Internet related legal issues could not be addressed properly. Hence in the Internet bank account fraud case (Krishan Kumar) in Delhi – S/25-( Intentional damaging and tampering with telegraphs) of Telegraph Act – 1885 was applied. The GOI issued private ISP licenses in May 2000. “The ISP policy of Government of India permits the ISPs to set up International Gateway for Internet …………” * 2A

(Existing Infrastructure And the I. T. Act.)

The crime management infrastructure, as it is prevailing today is a part and parcel of the management of the cyber crime also. In India Modern criminal law was introduced by the then British Government, especially after Government of India Act 1858. Gradually with the finer development of the criminal science in the European and American states, the Substantive Criminal Law ‘The Indian Penal code – 1860, and the procedural criminal law: The Criminal Procedure Code – 1898, The Indian Evidence Act 1872 and others were drafted and enacted by the Governor General in Council. The Government established court system hierarchy of courts, Police and prison. The same system with time to time modernization is prevailing today, at the time of the enactment and enforcement of The Information Technology Act.

And the cyber crime being very much a crime as well, will obviously seek the involvement and assistance of the valuable infrastructure of the existing crime management in India. "................. the country was taken over directly by British Crown in 1858 after the abortive mutiny of 1857. The next few years saw hectic activity in the legislative field and two basic criminal codes, viz. the Indian Penal code and the Criminal Procedure Code which were enacted in 1860 and 1861 respectively." *3. The IT Act itself relates for its' law enforcement activities to the existing Police System, search seizure prosecution evidence and trial.


S/80 Power of police officer and other officers to enter, search etc. (1) Notwithstanding anything contained in the Code of Criminal Procedure – 1973 (2 of 1974)– Any police officer not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a state government authorized by the central Government in this behalf, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Explanation – For the purposes of this sub-section, the expression ‘public place’ includes any public conveyance, any hotel, any shop or any other place intended for use by or accessible to the public.

(2) where any person is arrested under subsection (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having Jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the code of criminal procedure – 1973 (2 of 1974), shall subject to the provisions of this section, apply so, far, as may be, in relation to any entry search or arrest, made under this section.

The British crown soon after dislodging the East India Company in 1858, took elaborate steps for crime management in the country, to recover and ensure faith in the crown. “With the two criminal codes coming into existence, it was imperative to have a police code for the implementation of criminal law in the country. The government therefore appointed a Police Commission in the year 1860 and its recommendations provided the basis for the Police Act in 1861 … Despite the many political changes which have occurred in the last 122 years including the grant of independence to India, the police organization even to day rests largely on the policy laid down in the Act of 1861.”*4. The basic changes thus cancelled the capricious use of government power and established a reasonable and fair procedure on the concept of the Rule of Law.

This basic theme remains unchanged today with further refinement from time to time and naturally is to be continuing in the legal control of cyber – crime.

The e-governance in India is an indivisible part of the governance of the Cyber system of this borderless cyber planet as a whole. So the subject of the cyber governance in India is actually controlled by the different Internet bodies like ICANN, ISOC, IANA, NSI, IETF etc on the one hand and the ICT laws in India such as the IT Act, the IT Rules and Regulations, Security Guidelines /The Indian Penal Code – 1860 The Criminal Procedure Code – 1973, along with the corresponding amendments in the Indian Evidence Act - 1891, the Bankers’ Book Evidence Act – 1891, the RBI Act 1934 etc. and also the Indian Telegraph Act – 1885. And the third prong on e-governance in India is the ICT policy of the Government as has been taken up from time to time. The Information and Communication Technology (ICT) in India is said to have started with the installation of electric telegraph network in 19th century, so the Indian Telegraph Act - 1885 played an important role in the governance of information and communication system network till the end of 20th century.

The early cyber prosecutions were made under this Act “Cyber Theft and India Telegraph Act 1885 The Delhi Police has recently arrested Krishan Kumar for illegally using the Internet account of Col.(Retd) J.S. Bajwa. Krishan Kumar has been remanded to judicial custody for six days........ For violating the provisions of Indian Telegraph Act The said arrest of India’s second cyber theft raises numerous important and crucial law issues .......... S/25 of the Telegraph Act , which has been alleged to have been invoked in India’s first cyber trial, talks of intentionally damaging or tampering with telegraphs .......... Section 378 of IPC defines theft and Section 379 talks of punishment for theft. * 5. The Internet under ARPA of US is said to have come into existence in January 1983 and in a restricted manner it was made available to education and research bodies other than defense activities. India, under this academic program, got an access facility through the ERNET, the Internet could be accessed otherwise through the media company Compu Serve.

But the VSNL (Videsh Sanchar Nigam Limited) was established in 1986 to provide overseas communication through the AT & T for Indian Telecommunication users. On 15th August 1995, the VSNL opened its Internet Access network (GIAS) passing through Mumbai – Delhi – Kolkata and Chennai for common people The DOT (Department of Telecommunication) network also provided Internet access to the people. The Gateway Internet Access Service (GIAS) of VSNL allowed commercial access to the Internet. The VSNL maintained carrier relationship with the AT & T (American Telegraph and Telephone Co.) in overseas telecommunication calls.

And then under new telecom. Policy of the Government, private gateways of Internet Service Providers were allowed in May 2000 when about 72 private ISPs started business in providing Internet Access. The private satellite communication network through VSAT (Very Small Aperture Terminal) Communication points, the physical cabling and network management are looked after by concerned owners of the network. The regulation of mode of enjoyment was generally under the legal control of the state from the early age of Electric Telegraph network i.e. the Indian Telegraph Act – 1885. The first electric telegraph network was established in 1881 connecting Chennai Mumbai Kolkata and Yangon.

In 1985 the Post and Telegraph Department was divided into two separate offices Department of Post (DOP) and Department of Telegraph (DOT).

The general control and regulation of the telecommunication system in the country was reshaped under the new regulatory body TRAI (Telecom Regulatory Authority of India) formed in 1997. "The following are the main features of the National Telecom Policy 1994 Licensing Authority Department of Telecommunications. There will be a Telecom. Regulatory Authority of India (TRAI)." * 6. In February 1996 the TRAI Ordinance was promulgated and it was formed in March 1997. And the government remained to be the sole authority for licensing of all telecom services. The Information and Communication System has been further developed through the introduction of Internet in India. And for this new situation the controlling law has been the Information Technology Act.

Thus the state as a whole governs the use and enjoyment of the cyber - system through the I T Act and relevant portions of the Indian Telegraph Act - 1885. The crime management in this new area also depends upon the traditional legal system and procedure the Criminal Procedure Code 1973 the Indian Evidence Act - 1872 etc. The crime management thus in Cyber India, the subject matter of the present study, is the subject of the state. "A Government of India advertisement revealed that 98.5 percent of organizations surveyed had experienced computer crimes" * 6A. The global cyber space being an indivisible unity the Indian part there of can't have, in true sense, an isolated existence and meaning. So the Indian part of Cyber India can’t be governed in an isolated manner. But a part of global management necessarily falls on Indian people and their government.

In India the cyber crime management involves the traditional crime management system and the relevant provisions in the I C T laws i.e. I. T. Act Rules and guide lines, "India is a signatory to the Model Law and is under an obligation to revise its laws as per the said Model Law. Keeping in view the urgent need to bring suitable amendments in the existing laws to facilitate electronic commerce and with a view to facilitate Electronic Governance, the Information Technology Act was passed." * 7. The UN published the model trade law in 1997 for general guidance of all nations. And the IT Act has observed "New communication systems and digital technology have made dramatic changes ... Business and consumers are increasingly using computers to create, transmit and store information in the electronic form has many advantages ... To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislations."

With a view to facilitate Electronic Governance it is proposed to provide for the use and acceptance of electronic records and digital signatures in the government offices and its agencies," * Statement of object and Reasons IT Act."

The substantial legislations on E-Governance, being the IT Act provides for various items of cyber wrongs U/s. 43 and S/65 – 78 of the Act. "A national seminar on Computer Crime was organized in New Delhi during the last week of February 1999 by the Central Bureau of Investigation (C.B.I). Computer experts from the public sector institutions multinational banks and other financial Institutions, participated in the seminar and tried to gauge the impact of fast spreading computer related crime" * 7(1). Here the C.B.I Director Dr. R.K. Raghavan said that the CBI was preparing to face the new challenges of cyber crime.

6* Sup -2 -----1999-----P--251
6A* Business Standered ( Kol) --- 22.07.2002--- P--2
7* N. Kamath- Universal Law Pub Co Delhi – Cyber Law -2001 –P---624
A Computer Crime Investigation Cell (CCIC) under CBI has been working from 3rd March 2000 (as notified in September 1999) The crime cell under one Superintendent of Police has the nation wide jurisdiction and in the mean time several cyber police stations have been set up in Chennai (Eg more) Bangalore (Lakdikapool), Mumbai (Crawford market) & Kolkata (Lalbazar) The CCIC – CBI – is operating from New Delhi-Lodhi Road- http://cbi.nic.in

Ref: Sites:

3. http://www.cbi.nic.in
5. http://www.cyberpolicebangalore.nic.in


The nature of criminality in cyber – space is somewhat complicated. The high-technology involved in the virtual world has created some critical issues such as the real and legal implications of virtual presence, access and trespass, act or omission, overt act (actus reus), ill-motive (mens rea), transaction in virtual space, evidentiary value of stored computer record and computer generated record and the observance of reasonable doubt etc. "This shift away from the tangible corporeal environment to the information economy made possible by the Internet and telecommunication is an enormous challenge for business government and law enforcement." *8

In determination of criminal liability the two central pillars are namely the actus reus (overt act) and the mens rea (ill-motive). Reconstruction of legal elements in virtual space has become the vital task of the legal science, Government, legal community and Judiciary, the legal system as a whole. The cardinal principle of criminal liability is expressed in the maxim- actus non facit reum nisi mens sit rea-an act by itself is not crime if done without an ill-motive.

An overt act or an act of omission must be present in constituting the crime. The presence of criminal intent alone is not sufficient in that respect. "In this famous phrase, there is a clear distinction between a man’s deed (actus) and his mental processes (mens) at the time when he was engaged in the activity which resulted in the deed. As we have seen, the early Common Law was almost exclusively concerned with the harmful results of a man’s active conduct and it is convenient for brevity to speak of ‘deed’ when discussing general principles. But students should remember that the expression ‘actus reus’ also results or caused by omissions to act in those rare circumstances in which the Common Law imposes a legal duty to take action. *9

Even in statutory offences also, the actus reus is not actionable per se. Case: - Harding V Price (1948) All. E. R. 283 Hada VI- A large motor lorry rolled upon a stationary car and damaged it. But the driver could not feel it due to big noise and thus also did not inform the Police Station as a statutory requirement. "It was laid down that if a statute contains an absolute prohibition against the doing of some act, as a general rule, mens rea is not a constituent of the offence, but there is all the difference between prohibiting an act and imposing a duty to do something on the happening of a certain event. Unless a man knows that the event has happened, how can he carry out the duty imposed? If the duty be to report he can't report something of which he has no knowledge. Even where the statute imposes what is apparently an absolute prohibition, an absence of guilty knowledge may in some cases be a defense. * 10. Thus absolute separation of the state of mind from the actus reus in determining criminal liability is not possible.

As a general rule, the mental element is a crucial factor in imposing liability.

Nathu Lal V. State of MP - AIR 1966 SC43. The Supreme Court of India acquitted the accused on the ground that he had no guilty intention and hence did not contravene, in legal sense, the statutory provision deliberately.

Other than the actus reus and ill motive, the other element required for the purposes of criminal liability is some criminal harm because - crime is defined as an intentional act or omission in violation of criminal law, causing some injury in body mind reputation or property. In the above context of real space criminal liability - the Information Technology Act proceeds to criminalize some acts such as access to material database of the computer, tampering with the computer storage, harassing (Cyber stalking) someone, virus dropping, Internet related pornography, gambling, fraud, etc.

U.K.:-

In this respect, the law of the United Kingdom has been provided in the Computer Misuse Act - 1990. The Act provides for the access as an offence U/s - 1 as follows - S/1 Unauthorized Access to Computer Material

(1) A person is guilty of an offence if -

(a) He causes a computer to perform any function with intent to secure access to any program or data held in any computer.
(b) The access, he intends to secure is unauthorized: and
(c) He knows at the time when he causes the computer to perform the function that is the case

(2) The intent, a person has to commit an offence under this section need not be directed at

(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to fine not exceeding level 5 on the standard scale or to both.

The UK – Act also provides criminal liability U/s. 2 – for Unauthorized access with intent to commit or facilitate commission of further offences.

The section provides that

(1) A person is guilty of an offence under this section if he commits an offence U/s. 1 above (the unauthorized access offence) with intent -

(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person) ; and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences for which the sentence is fixed by law.

(3) It is immaterial whether or not the further offence is committed on the same occasion.

(4) A person may be guilty under this section even though the facts are such that the commission of further offence is impossible.

The law provides – a criminal liability under section – 3 for unauthorized modification of computer material. The section provides –

(1) A person is guilty of an offence if –

(a) he does any act which causes an unauthorized modification of the contents of any computer; and
(b) at the time when he does the act he has the requisite intent and the requisite knowledge (that it is unauthorized).

(2) For the purposes of this section, the requisite intent is an intent to cause a modification of the contents of any computer and by so to impair the operation of any computer, to prevent or hinder access to any program or data held in any computer or to impair the operation of any such program are the reliability of any such program or the reliability of any such data.

It is further mentioned under the sub section (3) that the intent need not be directed at any particular computer, any particular program or data or a program or data of any particular kind, or any particular modification of any – particular kind.
It is also mentioned that it is immaterial whether or not the unauthorized modification (or intended modification) is of permanent or temporary nature.

Thus the Law of UK - under the Computer Misuse Act - provides for a balanced consideration both the ACTUS REUS (overt act) and also the MENS REA (evil intent) for the determination of criminal liability of any person for an act or intended act.

UNITED STATES

The United States law - under the Federal Criminal Code Related to Computer Crime - similarly provides for criminal liability in the cases of act or omission having intention to cause injury or damage of any kind U/s. 1029. 1030.

S/1029 - provides for criminal liability to a person who knowingly and with intent to defraud produces, uses or traffics in one or more counterfeit access devices etc.

S/1030 provides for Fraud and Related Activity as follows: -

S/1030 (a) whoever having knowingly accessed a computer without authorization or exceeding authorized access and having obtained information (related to defense, foreign relations, restricted data) willfully communicates, delivers, transmits or causes to be communicated delivered or transmitted (or attempts to do the same) to any unauthorized person.

The section also provides for criminal liability to the person whoever intentionally accesses a computer without authorization or exceeding authorization - and thereby obtains information of financial institution department or agency of the government or of any protected computer.

The section also provides for criminal liability under subsection five for any person who knowingly causes transmission of a program, information code or command and as a result intentionally causes damage to protected computer.

In the both analysis, thus the US law also provides liability for both ACT and the INTENT.

SINGAPORE

The relevant law of Singapore - The Computer Misuse Act - also provides for intentional act the liability of an offence. S/3 - provides - for the Unauthorized access to computer material -as follows - whoever knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer.

The subsection (3) provides also that it is immaterial whether or not the act is directed at any particular program or data, a program or data of any kind or a program or data held in any particular computer.

The Act - U/s. 4 - provides liability for access with intent to commit or facilitate commission of offence as under.

And S/5 of the Act imposes criminal liability for unauthorized modification of computer material. The law provides that whoever does any act ' which he knows will cause an unauthorized modification of the contents of any computer shall be guilty of an offence.

It is further provided that it is immaterial, whether or not, the act in question is directed at any particular program or data, a program or data of any kind or a program or data held in any particular computer.
The Law – U/S-6 provides for liability in case of “Unauthorized use or interception of computer service. The section states as – "any person who knowingly (a) secures access without authority to any computer for the purpose of obtaining directly or indirectly, any computer services (b) intercepts or causes to be intercepted without authority, directly or indirectly any function of a computer, or uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under (a) or (b) shall be guilty of an offence.

The Act further states U/s. 7 (unauthorized obstruction to use of computer) that any person who knowingly and without authority or lawful excuse interferes with or interrupts or obstructs the lawful use of a computer or impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer shall be guilty of an offense. The Act provides similar liability U/s. 8 to a person making ‘Unauthorized disclosure of access code’ – knowingly and without authority if he does so for any wrongful purpose or knowing that it is likely to cause wrongful loss to others.

The Act U/s. 10 provides similar liability for abetment attempt and preparation to commit or in furtherance of commission of any offence under this Act.

The activities that are per se crime and those culminate in a computer crime are mentioned below;

(.) Alteration of computer data or computer programs – resulting in a crime
(.) Computer espionage – crime per se
(.) Computer forgery -- crime per se
(.) Computer sabotage – crime per se
(.) Computer – related fraud -- crime per se
(.) Damage to computer data or computer programs – resulting in a crime
(.) Unauthorised access------- resulting in a crime
(.) Unauthorised interception-- resulting in a crime
(.) Unauthorised reproduction of a protected computer program----crime per se
(.) Unauthorised use of a computer -------resulting in a crime
(.) Unauthorised use of a protected computer program----crime per se

INDIA

In the above prevailing context ,the rules of determining the Criminal Liability has been scheduled in the Information Technology Act in India.

The IT Act has provided criminal liability for ‘Tampering with Computer source documents – U/s. 65’ ----for ‘hacking with Computer system’ U/s. 66 and for ‘Publishing of information which is obscene in electronic form’ – U/s. 67 and also for securing access or making attempt to secure access to protected system – U/s – 70 all under Chapter – IX of the Act.

S/65 – TAMPERING WITH COMPUTER SOURCE DOCUMENT – 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 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 up to three years or with fine which may extend up to two lakh rupees or with both.
**Explanation**—For the purposes of this section. “Computer source code” means the listing of program, computer commands, design and layout and program analysis of computer resource in any form.

Thus the section distinctly identifies both the ACTUS REUS and MENS REA elements for the purposes of criminal liability.

A) **ACTUS REUS** – whoever conceals destroys or alters or causes another to conceal destroy or alter any computer source code used for a computer, computer program, computer system or computer network.

B) **MENS REA** – whoever knowingly or intentionally conceals destroys or alters... etc.

Thus S/66 provides for both ACTUS REUS (overt act plus injury) and the MENS REA – in both letter – and spirit.

**S/66 – Hacking with Computer system:**

(1) 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 any means, commits hacking. (2) Whoever commits hacking shall be punished with imprisonment up to three years or with fine which may extend up to two lakh rupees or with both.

On analysis

(A) **ACTUS REUS** – Whoever destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(B) **MENS REA** – Whoever with the INTENT to cause or KNOWING that he is likely to cause ---etc.

Thus the liability is based upon both Actus Reus and Mens Rea, and thus not being a strict one.

**S/67 – Publishing of information which is obscene in electronic form** – Whoever publishes or transmits or causes to be published 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 five years and with fine which may extend to one lakh rupees, and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

On close examination, however-

(A) **ACTUS REUS** - (overt act with injury) - whoever publishes or transmits or causes to be published in the electronic form any lascivious material which appeals to the prurient interest or tends to deprave and corrupt persons.

(B) **MENS REA** - (Not Expressed) – The provision however does not expressly exclude ‘mense rea’ hence it is construed by the golden rule of interpretation and the cardinal principle of criminal liability – Actus facit reum nisi mens sit rea.
Publication in the general sense i.e. hard copies or paper copies is different very much from creation storage or transmission in intangible form. In many cases it resembles to close door communication among members holding pass phrase/access code. Hence creation storage and transmission of some graphics of whatever content can’t be actionable per se. And the meaning may be construed as --- “with the intention to make it publicly available if any one creates publishes or transmits or causes to be published in the electronic form any lascivious material.”

S/70 – Protected System – (1) The appropriate Government may by notification in the official gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may by order in writing, authorize the persons who are authorized to access protected system notified under subsection (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of the section shall be punished with imprisonment of either description for a term which may extend to ten years and shall be liable to fine. The provision U/s 70 thus provides for:

(A) ACTUS REUS – Any person who secures access or attempts to secure access to a protected system shall be punished.

AND –

(C) MENS REA – (Not Expressed)

Neither the Act as a whole nor the provision U/s. 70 in question excludes – MENS REA in express terms.

From the above analysis and on the basis of the prevailing views of the jurists, the liability of a person under the IT Act is determined on the basis of the Actus Reus and Mens Rea, both the elements taking at a time.

Case: Dr. Nuker (Anand Khare) and Da Libran (Mahesh Mhatre) of Mumbai intentionally hacked the webpage of Cyber Crime Investigation Cell (Mumbai) in 2001 (July). The CCIC upon investigation tracked their identity and arrested accordingly.

6.3.1 – Development of Technology And Criminal Liability –

With finer and finer development in science and technology, the law faces new challenges in every age. But it is observed by eminent thinkers and jurists that the Internet has raised a very crucial question as to the legal implications of the virtual space, “People are now raising fears and asking questions about the potential for individuals and society at large where those developments take us.”

In various areas the issue has come up requiring solution in a new way yet to be revealed. Some of these are – human cloning, test – tube baby etc. And in cyber – space – the serious debate is going on as to the question of Intellectual Property especially copy – right, trade mark, trade secret and business know how. The other issues are centering around criminal liability in cyber activities i.e. trespass, virtual presence, injury, actus reus, privacy and human rights etc. “The real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record – keeping systems, each of which alone may seem innocuous, even benevolent and wholly justifiable.”

“...... There is nothing special in the fact that Information Technology has brought in cyber crimes too. But the matter of concern is the reach of the technology and the reach of the crimes. The technology is developing fast, so is the cyber crimes. The society and the law enforcement agencies are finding it difficult to catch up with the criminals in this evolution of criminality.”


Various activities and opportunities are being offered by the different technologies like Cookie, blue-tooth, password breaker, sniffer program, MP3, code breaker, search engines, framing etc. But these are questioned in the court of law as to their validity.


Where the defendant was restrained from publishing or distributing - in the US the Playmen magazine. But when one server in Italy opened website containing the same the injunction was extended there too, simply because the intending US - readers got password from the defendant to access the Italian server.

6.4 CYBER CRIMES IN INDIA

With the opening of the Gateway Internet Access Service by VSNL in August 1995, India entered the age of the Internet. And the Securities and the Exchange Board of India (SEBI) granted permission for on-line trade and commerce on 1st January 2000. And by this period, a decade, however, the traditional criminals can't accommodate themselves in the complex technicalities of the virtual space. Nor a technical community culture and liking of Fashion has grown to commit hacking, cracking and other related activities. But the menace as is usual can't be altogether avoided here in India as well. One survey made by PIC - Project India Cracked provided many information in this regard. The survey was conducted during 28.04.2004 to 10.05.02, the survey provides that number of web sites defaced are 780 where the top 5 attackers are AIC (Anti India Crew); G Force Pakistan, Silver Lords, WFD and ISOTK. The survey also revealed that different vital networks like VSNL, AIRTEL websites; ONGC- INDIA, etc were hacked. * 13A. Various hackers groups are active in cyber space. Some of them are Virtual Hell, Web pirate, Red Eye, Shadow Lords, Devil Souls, Dr-Snake, Dr-Evil, Death Team, Delta Force, King 420, Tecno Master, Dr. Hacker, Ghost CR3W etc.

**NO. OF WEBSITES HACKED IN INDIA**

![Graph showing the number of websites hacked in India with data points from 1999 to 2004. The graph shows a steady increase in the number of hacked websites over the years.]}

13A * PIC ---http://www.srijith.net/India...cracked/stats/index.shtml-----download-10.09.2004
And the shadow side of the Internet has started to concentrate from the closing years of the 20th century. Some of these incident reporting are worth mentioning (1) State of Delhi V Krishan Kumar – 2000 in July 2000, one Krishan Kumar misappropriated some money from the Internet banking account of one retired Col. J. S. Bajwa. He was however traced and arrested and prosecuted for violation S/25 Indian Telegraph Act-1885.

S/3 of the Act provides the definition of telegraph to mean any appliance, instrument material or apparatus used or capable of use for transmission or reception of signs, signals, writings, images, sounds or intelligence of any nature by wire, visual or other electromagnetic emissions, Radio waves or Hertzian waves, electric or magnetic means.

And S/25 – provides that if any person intending (a) to prevent or obstruct the transmission or delivery of any message or (b) intercept or to acquaint himself with the content of any message or (c) to commit mischief damage removes, tampers with or touches any battery, machinery, telegraph line post or other thing whatever, being part of or used in the telegraph or in the working thereof, he shall be punished up to three years and/or fine. The relevant IT Act in this matter was passed and enforced only in October 2000 and hence Indian Telegraph Act 1885 was applied to deal with the Internet related fraud. But obviously the telegraph law is not appropriate one. “The definition of telegraph though loosely defined, yet can’t be so much stretched as to include Internet and cyber space within its ambit … This present test case raises a lot of cyber law issues which would have to be unnecessarily addressed in order to achieve the goal of crime free cyber space. All eyes are now on India’s first cyber trial.” 14. Thus the situation in India at the time was really mature to have the right law to deal with issues arising out of the cyber space. And accordingly the Information Technology Act was passed and it was enforced on 17th October 2000.

(2) Illanthirayan and his assistant Umang Dave in September 2001 onwards committed regular hack attacks on various company websites and ISP such as lenet website-www.24online.com www.sachchatroninc.com etc. They sent a threatening e-mail to the department of atomic energy. Analyzing the IP address, the ISP was traced and from its user list the offenders were traced by the LEA;

(3) Dr. Nuker (Anand Khare) hacked CCIC website in 2001, July.

(4) SPAMING (e-mail bombing):
A school dropout (16) son of a teacher in Pondicherry, launched a continuous e-mail bombing targeting a web hosting company in UK and for which the company could not transact any business for about three days at a stretch, in February 2002. The victim company sought for help from CBI in India and the computer crime investigation cell (CCIC) under CBI tracked and traced the accused in a Pondicherry house. The CCIC seized one of the computers containing the ready to use ‘the e-mail bombing programme’ from the possession of the boy. The case against the accused has been filed U/S 507 (criminal intimidation by an anonymous communication), S/509 word, gesture or act intending to insult the modesty of women both of IPC-1860 and also U/S 66 (hacking with computer system) of the IT Act-2k. (5) The project India cracked (PIC) http://www.srijith.net/indiacracked/. Was privately operated and personally owned by Mr. K N Srijith, teaching assistant – the School of Computing – National University of Singapore. The PIC has provided a record of hack attacks on Indian websites for a period from 28/4/2000 to 10/05/2002 (when it was closed). And also identified the hacker groups in some cases such as Virtual Hell, Web Pirate, Shadow Lords, Silver Lords, Devil Souls, Dr. Evil, Death Team, death Symbol king 420, Dr. Snake, Security Team, Delta Force Etc.
Public banks fail to plug infotech security leaks – as has been observed by R.B.Barman, executive director of RBI. He also observed that – “a Govt. of India Advertisement revealed that 98.5% of organization surveyed had experienced computer crimes. * 

The IIT Kharagpur – has opened a study and research center on hacking (help @ bfisecure.com). They noted a record of defaced Indian websites for some months in 2003 some which were – er.railnet.gov.in, hyderabad water.gov.in. They provided the total no. of victim websites as 767 in the first months of the year 2003. * 

New study sees piracy at 70% and rising –
It is observed that “software piracy in the country rose to 70% in 2001-2002 compared to 63% in 2000-2001, according to Business Software Alliance (BSA), an association of software companies fighting piracy … India is the one of the few markets that has seen a rising piracy, says the Business Software Alliance.” * 

NASSCOM observed that 61% of the software sold in India is pirated.

Virus clogs net traffic – Hyderabad January 25 – "a computer worm noticed less than 24 hours back is unleashing terror by stunning computer networks and dramatically slowing down Internet speed.” * 

Anti-virus Firm Symantec.com has updated its’ disc assessment to ‘wild’ this evening and reported close to 30000 infections. Asia is the worst affected with reports of slow down and outages being reported from Japan, South Korea and Cambodia. (The Statesman/26.01.2003/Kol.)

Total Net closure after worm attack-SNS-Hyderabad-Jan-28 - India officially admitted to have under gone total closure of the Internet during over the weekend due to the ‘Slammer’ worm, the worm was exceptionally small-376 bytes due to which it aggressively moved around to cause the worst attack on the Internet in 18th months…” F-Secure an anti-virus company, reported that two lakh computers have been infected and the worm brought down 5 Internet root name servers: * 

Porn CDs Flood Chandni Market - “The familiar scene is that usually foxy looking chaps accosting visitors to Chandni Chawks’s wholesale markets for cassettes and CDs trying to push porn cassettes or CDs or two.” * 

Cyber crime sees first conviction -Chennai - November 6th ---- “In the first ever conviction for cyber crime in the country, the additional Chief Metropolitan Magistrate on Friday sent a man to jail for harassing a woman on the Internet, Suhas Shetty (31) was sentenced for two years for obscenity on electronic media, two years for forging electronic documents and one year for outraging the modesty of a woman.” *
A woman complained that her name had been plastered all over the Internet and her telephone number along with a soliciting message has been put in various adult sites.

State Vs Suhas Shetty:
The law enforcement agency tracking the ISP identified the accused Suhas Shetty and arrested, produced before the court within a month following the complaint.

(13) Court boost to crack down on online lotteries-- legal correspondent. The Calcutta High Court allowed State appeals and set aside trial court restraint order upon it. The state contended that Director, Sikkim Lotteries and officers of Play-win and Smart-win had violated the provisions of the Lotteries Regulation Act-1998

(14) Student deported for Net- sex crime- Houston- Feb 8th. An Indian S. S. Malik(27), a student of University of Texas was found guilty for Internet sex crime for soliciting an underage girl (15). Though however the police officers were posing as a girl in question.-

(15) Caught in the act “the cyber café case in Meerut— where many boys and girls had been arrested in indecent positions has raised many legal issues."

The boys and girls found were arrested for surfing pornographic websites and booked U/S 294 IPC for committing obscene acts in public place. The Meerut administration then demolished the private cabins in the café.

CYBER CRIMES IN INDIA*22A

No. of web sites and computer networks damaged by hackers:----------

<table>
<thead>
<tr>
<th>YEAR</th>
<th>No. of Websites</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999</td>
<td>45</td>
</tr>
<tr>
<td>2000</td>
<td>136</td>
</tr>
<tr>
<td>2001 (up to August)</td>
<td>275</td>
</tr>
</tbody>
</table>

The names of some damaged Websites and Computer Networks: India----:

1. Railway Reservation system
2. National Stock Exchange
3. Reserve Bank Of India-Network
4. NICENET – a Network connection 540 District Towns, 32 Capitals of states and union territories.
5. Indian Financial Network
6. Army, Navy, Air force --Networks
7. ISRO
8. National Information Center-Hyderabad Sector
9. State Web site-Tamilnadu
10. National Information Technology-Promotional Unit-Kolkata
11. Economic Research & Market Intelligence Unit-Delhi
12. 123 India Com.rediff.complanet.net
13. VSNL-Ernakulam
14. South Gujrat University Network

*22 The Statesman Kol:-------- 28-02-2005 ----------p-10
Some computer related cases:---.

(A) State Vs Sanjib Kapoor.
Hare Streer PS Kolkata Case No-776 of 2001
U/S 420/406/467/468/471/ 477A/120B – IPC
FIR date: 05-12-01

(B) Hare Street PS Case No – 391 of 2004
U/S – 120B/420/409/467/468/471 – IPC
FIR Date: 29 -06-2004

One Sanjib Kapoor was arrested by Calcutta police and produced in the city court on the charge of illegal banking business- accepting and in vesting money. The accused was inviting and accepting huge liquid money from the people on the promise of good and quick return but without taking any lawful permission from the concerned authorities. The above two cases were started against him.

The entire business activity was conducted through online communications. The law enforcement authorities find big trouble to collect, preserve and produce necessary evidence of the transactions. This could however be recovered only through computer forensic report. And most probably the computer cell in Calcutta was not equipped with such facilities and trained personnel at the time in question.

6.5. PREVENTIVE AND SECURITY MEASURES UNDER IT ACT.

Management of crime usually includes safety security and preventive measures also. The use of password and encryption provides privacy and at the same time a protection against unauthorized access to the file content. So also a tamperproof log file will give the full record of login and out incidents of accesses to the machine. “The RBI has directed computerized bank branches to put in place an appropriate audit and security infrastructure for their IT systems right from their hardware software, networking, ATM, bank employees their work habits under a computerized environment, which includes confidentiality of passwords, maintenance of control registers, backups and all.” * 23.

The IT Act and the IT Rules have provided a detailed provision for such security and safety measures. So it has been observed that indifference of the sysadmin (system administrator) has invited many hack attacks. Not only the use of appropriate devices like Firewalls, Intrusion Detection system (IDS), Tamper proof log file, encryption, etc. but also the control of the physical access of human individuals is necessary. The information system audit at a regular interval is a legal duty of the sysadmins. Security experts for computer and computer systems advise security testing or circumvention.

The IT Act provides for privacy and also for security U/s. 3 --Authentication of electronic records- subsection (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform at the initial electronic record into another electronic record. The IT Act under CA Rules 19(2) has IT Security Guidelines and (2) Security Guidelines for certifying Authorities to protect the integrity confidentiality and availability of service of certifying Authority (CA).
The IT Security Guideline provides for the implementation and management of IT Security under different sections in thorough details from S/1 to S/26 of the guideline. Some of these are:

1) Advance warning mechanism U/s 20(3) - System must include a mechanism for alerting the Network Administrator of possible breaches in security e.g. unauthorized access, virus infection and hacking.

2) Network isolation system like Firewall U/s. 18 - Network that operate at varying security levels shall be isolated from each other by appropriate firewalls (a screening device software + hardware). The internal network shall be physically and logically isolated from the Internet and any other external connection by a firewall.

3) Proper device (software) to detect virus U/s. 11(2) - Virus detection software must be used to check storage devices both internal and external to the system on a periodic basis. Some more devices like Network Diagnostic tools S/17(7) encryption and password (U/s. 6.3.3) etc. are to be applied as safety measures against crimes.

Other than technical control some more measures are taken to control physical access to the system. Some of which are:

1) Network Administrator 20(2) - Network Administrator shall regularly undertake the review of the network and also take adequate measures to provide physical, logical and procedure safeguards for its security. Appropriate follow-up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

2) Physical and Operational Security U/s. 4.4 - Physical access to the operational site at all times shall be controlled and restricted to authorized personnel only. And all individuals other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

3) Reporting on Security incident U/s. 5.5 - All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence (also U/s. 10.4)

4) Preparation for emergency U/s. 23 - Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

However, it is observed by the informed persons that security is a continuing process requiring a regular check ups and audit. "Installing a network security device is not a substitute for a constant focus on keeping defenses up to date. In a recent survey by the Computer Security Institute, 90 percent of the respondents used antivirus software, but 85 percent were damaged by a virus. Eighty-nine percent had installed computer firewalls and 60 percent had intrusion detection systems, yet 90 percent had their systems penetrated from outside. As these survey numbers indicate, good security practices include not just installing those devices but operating them correctly and keeping them current, including regular patching and virus updates."  

23A * Stanely Theodore -- The Statesman (kol) --28-10-02----------p-10
6.6 ROLE OF ISP UNDER IT ACT.

An Internet Access Provider operates at a very crucial point both in technology and security consideration. All the data coming to and from the users pass through ISP host/server computer. And hence the ISP has reasonable opportunity to monitor and record the data for analysis investigation and study the nature and character of the data used by the group of subscribers.

India's only ISP was VSNL which opened the GIAS (Gateway Internet Access Service) network on 15 August 1995 GIAS passed through Chennai, Delhi, Calcutta, Mumbai, then in May 2000 the Government of India took a new policy and allowed a group of private ISP. And about 75 out of 215 newly licenses ISP started operation on 20th May 2000.

The ISP service as the transit point gives a strategic location for monitoring the criminal activities in the web.

Some of the important Indian ISPs are VSNL, MTNL, Satyam Infoway (p) Ltd. Bharti BT, Data Infosys Ltd, ERNET, M/S. CMC Ltd etc

The information Technology Act – provides for ISP involvement in the law enforcement issues and hold it liable in default of some duties imposed upon it U/s -79 of the Act, ISP liability is the issue of whether an ISP can be held liable for the products and services it provides, the way in which it does business and /or the tools that it uses to conduct that business. *24

The Act provides for ISP liability u/s.79 – Network service providers not to be liable in certain cases. However the Act imposes positive duty upon the ISP to take due care to prevent offence or and also the offence, if any, was committed beyond his knowledge. The Act further provides that “For the purpose of this section---

a) ‘Network service provider’ means an intermediary:

b) ‘Third party information’ means any information dealt with by a network service provider in his capacity as an intermediary”

The relevant Guideline issued by the Government of India provides specific duties on the ISPs as to legal issues involving criminal use of the network.

III-Monitoring Facilities –

a) At each international Gateway location and /or ISP node with a router/switch having an outbound capacity of 2 mbps or more.

1)Every international gateway location and /or the ISP node with a router/switch having a capacity of 2Mpbs or more shall be equipped with a monitoring Center at the cost of the ISP, The details of the monitoring equipment that is required will be specifies by the security agencies through Telecom Authority ... Any other equipment for monitoring may also be put up by the security agencies in the monitoring center.” * 25 The guideline also required that the ISP must arrange for one local exclusive telephone line for this centre and the ISP has to bear all the expenses of this monitoring centre. Thus essential for the purposes of the managment of cyber crimes.

In a case:

AOL v Cyber Promotions Inc 1996.

Cyber promotion a web company of Pennsylvania was directing endless stream of spam e-mail through various networks of AOL targeting AOL subscribers. AOL then blocked the spam mail and redirected these to the different ISPs of the Cyber. It was held that Cyber had no right to send.

25 * Sup ---24------------------------2001-------------------------------p-716
unsolicited e-mail flow through network equipments of AOL, causing a trespass and ‘Cyber’ was restrained from originating allowing spam e-mail

Other case:
- Specht V Netscape & Aol – NY – 2000

Some legal provisions on ISP liability as to criminal activities through the ISP server equipments are:

1) The G7 and G8 Groups published an expert opinion on the subject in Dec. 1997 “.... To define an adequate system of rules for the responsibility of Internet access providers and service providers e.g. by creating a legal system so that in all countries service providers must take reasonable efforts to erase illegal contents on their servers when made aware of these contents. While at the same time, the free flow of data should not be hindered by attempts to block access to other servers and by holding access providers liable.” * 26

The Council of Europe Convention on cyber crime (2001) also provides for similar responsible role of the ISP under A/20(1) - Real time collection of traffic data – Each party shall adopt such legislative and other measures... to compel a service provider.... to collect or record... or to co-operate and assist the competent authorities in the collection or recording of traffic data, in real time, associated with specified communications in its territory transmitted by means of a computer system.

Similar provisions are also found in the Internet Industry- Code of Practice (May, 2002 issued by www.iana.net :)) u's 5 (ISP Obligation in relation to internet access generally) S 6 (ISP Obligation in relation to access to content hosted outside Australia) etc. The cyber crime Code of Practice (www.iana.net :)) issued in July b2003 also provides for similar duty of the ISP U/S 1 4-1.5-1.6-1.7-1.8 where 1.7 says “This code is, in the first instance directed towards ISP/LEA co-operation... provided always that such co-operation is solely directed to the purpose of addressing criminal or terrorist activity occurring on or by means of the Internet and remains within the spirit and letter of relevant privacy legislation and IIA codes.” *27

The cyber crime being essentially a global and borderless issue the co-operation among ISP and LEAS are vital irrespective of any national boundary. The same spirit also holds good for the IT Act.
6.7 --A SPECIAL FEATURE OF THE IT ACT ON THE CONTROL OF CYBER CRIME

The special feature of the IT Act in relation to cyber crime is that the Act makes two groups of crimes. One group of crime as CH-IX U/S. 43 has been kept for a civil control through an adjudicating officer, a government official not below the rank of Director G.O.I./or equivalent State officer U/s.46 (1,3)

And the Cyber Regulation Appellate Tribunal (U/S.48) then takes the appeals from the judgment order or decision of the adjudicating officer and controller of certifying authorities by 45 days. And the second appeal thereafter from judgment order etc. made by the CRAT shall be entertained by the High Court by 60 days U/S. 62 of the Act.

"chapter IX brings a welcome change in the minds of law makers as, may be for the first time, Indian Parliamentarians have come out of their obsession with the idea of criminalization as the sole means of regulating human conduct and upholding societal peace and tranquility and introduced civil liabilities as an alternative."* 28

The chapter IX-S/43 provides for a set of very common cyber wrongs mostly known as crimes in the West. These are unauthorized access, downloading, virus dropping, damage and disruption, denial of access, to facilitate illegal access, divert the charges to innocent use etc. attracting damages up to 1 core.

The Act provides for compounding of offence U/S.63 before the controller or any other officer so appointed. In the 2nd group i.e. the chapter XI thereafter, provides for the crime description in true sense of the term U/S.65 for Tampering with computer source documents with a penalty up to 3 years imprisonment and/or a five up to two lakh rupees.

S/67 for publishing of information which is obscene in electronic form with a punishment of 10 years imprisonment and also with fine up to two lakh rupees.

S/70 for access (also attempting access) a Protected System with a punishment of ten years and also a fine (not specified).

6.8—LEGAL CONTROL UNDER IT ACT

The control of cyber crimes under the IT Act has been attempted in two parts. The first part operates for group offences given U/S.43 through a law of civil nature the Cyber Regulation Appellate Tribunal (CRAT) and adjudication officer.

The other part operates for offences like Tampering (S/65) Hacking (S/66) Obscene publication (S/67) Illegal access (S/70) through the existing crime management laws and procedures like criminal procedure code and police, prison, investigation, search and seizure, evidence, trial and punishment, imprisonment and fine.

6.8(a) SUBSTANTIVE & PROCEDURAL LAW

(1) The Information Technology Act.

The new framework of law has been legislated through the I T Act providing for the criminal liability for tampering with computer source document whoever conceals, destroys or alters any computer command, programme analysis of the ---------the computer, knowingly or intentionally shall be guilty. U/S.65 of the I. T Act (3 years and or fine) The other rule for Hacking is whoever intentionally or knowingly destroys deletes or alters information data resident in a computer resource causing loss damage or likely to cause the
same to. any person or public at large shall be guilty. Of offence U/S.66 of the I.T Act (3 years and or fine)
The Act also provides that when any person publishes or transmits or causes to publish any material in
electronic form which is lascivious and which tend to deprave and corrupt persons is guilty of
offence U/S.67 of the Act with 5 years and a fine upto one lakh but for subsequent conviction it is
10 years and a fine upto two lakh rupees.
The Protected system as notified by the state will have greater security against trespass. And if any
one secures access or even attempts to secure access to it shall be guilty under law (S/70) 10 years
imprisonment and a fine no limit given.-
S/71- Provides for misrepresentation-whoever makes any misrepresentation to or suppresses any
material fact from, the controller or the certifying Authority for obtaining any licence or Digital
signature certificate shall be punished with 2 years and/ or a fine up to one lakh rupees.
S/69- provides for compulsory decryption of any massage in default a penalty of a term up to seven
years of imprisonment. S/72- Penalty for breach of confidentiality and privacy whoever by virtue of
any provision under this Act, secures access to electronic record, book, register or document
without the consent of the person/ owner concerned and then discloses this intercepted or seiued or
recovered data information to any third party shall be guilty. (2 years and / or a fine up to one lakh
rupees).
S/ 73- Penalty for publishing Digital Signature Certificate false in certain particulars- a term up to 2
years and / or a fine up to one lakh rupees.
S/ 74- Publication for fraudulent purpose will be liable for imprisonment up to 2 years and/ or a fine
up to one lakh rupees.
S/ 75- Act to apply for offence or contravention committed out side India -(1) subject to the
provisions of sub-section (2) the provisions of this Act shall apply also to any offence or
contravention committed out side India by any person irrespective of his nationality.
(2)For the purposes of subjection (1). This Act shall apply to an offence or contravention committed
out side India by any person if the act or conduct constituting the offence or contravention involves
a computer system or computer network located in India.
S/85 – Offences by Companies – Incase of a Company – every person who was in charge of and
was responsible to the company at the material point of time, for the conduct of business of the Co.
as well as the Co. shall be guilty and punished accordingly.

(2)The Criminal Procedure Code – 1973 provides for the establishment of the criminal courts,
regulatory rules and working procedu4, these courts are already working for the management and
control of the traditional crimes.
This existing set-up of crime management has been the place for the new cyber crimes also. The
police and prison of the present system are also equally taken help of for the cyber crime
management.
S/78 – provides for the power to investigate offences by a Deputy Superintendent of Police.
S/80- provides for the power of police officer and other officers to enter search a public place etc.
by DSP.
80(3) The provisions of the code of criminal procedure 1973 (2 of 1974) shall subject to the
provisions of this section apply, so far as may be, in relation to any entry, search or arrest, made
under this section.
The Indian Evidence Act - 1872 with some amendments is the basic framework for the rules of evidence trial and witness etc. Some of these are:

- Definition of evidence
- Document to include electronic record - U/s. 59
- Admissibility of electronic record - U/S. 65B
- Presumption as to electronic agreement - U/S. 85A
- Presumption as to electronic gazette - U/S. 81A
- Presumption as to electronic message - U/S. 88A
- Presumption as to electronic records five years old - S/90A

The Indian Evidence Act - 1872 has been amended in various sections to accommodate electronic evidence, and documents in judicial proceedings. The definition of evidence U/s. 3 provides to include all documents including electronic records produced for the inspection of the court. The second schedule of the IT Act - provides for all the changes and inclusions relating to electronic evidence. S/17 provides for admissions, oral or documentary or contained in electronic form. S/22A provides a new rule as to when oral admission as to contents or electronic records are relevant. S/34 provides to include entries in the books of account including those maintained in the electronic form and like other changes have been made under sections- 39, 47A, 59, 65A, 65B, 67A, 73A, 81A, 85A, 85B, 85C, 88A, 90A, 131.

(4) The Indian Penal Code - 1860 as amended in 2000. Various provisions have been suitably amended such as s/29A (inserted) to define "electronic record." To mean the same as provided U/s 2(1) cl. (i) of the IT Act. The changes have been included in the first schedule of the IT Act. The changed provisions and new insertions are:

- s/29A, 167, 172, 173, 175, 192, 204, 463 (forgery), 464 (making a false document), 466 (forgery for record of court or public register), 468 (forgery for purpose of cheating), 469 (forgery for purpose of harming reputation), 470 (forged document or electronic records), 471 (using as genuine a forged document or electronic record), 474 (having possession of document described in sec 466 or 467, knowing it to be forged and intending to use it as genuine), 476 (counterfeiting device or mark used for authenticating documents other than those described in sec 467 or possessing counterfeit marked material), sec. 477A - Talsification of accounts.

(5) The Bankers' books Evidence Act - 1891:

As amended in 2000 in various provisions. The changed and modified position has been provided in the third schedule of the IT Act. Section 2 of the Act-(a) provides for the inclusion of electronic records as print outs of data stored in disc, floppy, tape or any other form of electro magnetic data storage device as Bankers' Books. (b) provides for electronic certified copy or any entry in such books to include a certificate at the foot of such copy that is a true copy of such entry and was made in the usual and ordinary course of business and that such books is still in the custody of the Bank etc. S/2A newly inserted provides for conditions in the print out to accompany a certificate by responsible officer of the Bank.

(6) The Reserve Bank Of The India Act-1934: as amended in 2000 u/s – 58(2)-pp-clause inserted to give the rule on electronic fund transfer between Banks And Financial Institutions.

(7) The Information Technology (Certifying Authority) Rules-2000

(8) The IT Security Guide Lines U/R-19(2)-

(9) The Security Guide Lines For Certifying Authorities [U/R-19(2)]

6.8 (b) ------ Some Special issues relating to Prosecution And Trial -- under IT Act.

The legal process may start with the detection of any security breach or incident. The next stage necessarily goes to be recording and reporting to higher authorities.

Officially however the law-enforcement agencies (L E A) can't start without a written note or complaint or information converted into written form when it comes to the office.

And upon some material information & enquiry the criminal law is set into motion. The police officer (DSP or above in rank) can without warrant enter and search any public place to seize materials connected to an offence or arrest the persons concerned.

And thus the law starts to move and the accused person along with seized articles are taken to the magistrate court when the magistrate takes the cognizance of the offence and registers a case under the IT Act.

6.8.b (1) INVESTIGATION

The timely and efficient investigation on cyber crime issues is a necessity to recover information from the victim computer, to track and trace the accused to employ Intruder Watch, Sniffer program, to monitor and collect traffic data, to employ SATAN, to ascertain nature of attack, extent of loss or injury, to test vulnerabilities, to collect evidence etc. And as in all countries, the law enforcement agencies (LEAs) in India also need the necessary training experience and motivation for ICT offences.

The Computer Crime Investigation Cell (CCIC) under the CBI has been set up in metro cities including Bangalore in India. And CBI – FBI Collaboration has provided for necessary training to the LEA personnel.

In addition to computer forensics, interception, surveillance tamper proof log record etc. the human intelligence network as agent hacker and the like – are also employed in Cyber Crime investigation.

The Indian law enforcement authorities have already reached a strong and confident position to track and trace the online offenders. In 2001 the Mumbai Computer Crime Cell – traced a hacker in a very short time. The Computer Crime Investigation Cell (CCIC) in Mumbai traced and tracked Dr. Nuker (Anand Khare) and Da Libran (Mahesh Mhatre) who hacked the website of the CCIC (www.cccihmumbaiindiain) in July, 2001. The CCIC
analysed the log records of its own server ‘Net 4’ India and traced the IP address of the hackers ‘Server to be DISHNET DSL Ltd, Mumbai which in turn identified the origin to be one Cyber Café ‘Osprey Enterprises’ at Shivaji Park, Dadar.

The CCIC raided the Café and searched and identified the computer used by the hacker and seized these. The café owner gave description of the person hacking the CCIC site. The CCIC – on further analysis of own server log Net 4 India traced more attempts of hacking and traced another – Nexus Cyber Café at Chandan Mansion – where one of the (3) partners disclosed about the activities of Mahes Mahatre and Anand Khare. The IT Act has given wide – powers to the LEA in this regard –


S/80 – Power of Police Officer and other Officers to enter, search etc. – (1) Notwithstanding anything contained in the Code of Criminal Procedure – 1973 (2 Of 1974), any police officer, not below the rank of a Deputy Superintendent of Police or any other Officer.... Authorized in this behalf may enter, any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or being about to commit any offence under this Act.

Explanation – for the purpose of this subsection the expression ‘public place’ – includes any public conveyance, any hotel, any shop or any other place intended for use by or accessible to the public.

S/81 – Act to have overriding effect – The provision of this Act shall have effect not with standing anything inconsistent there with contained in any other law of the time being in force.

Thus the investigation of cyber offences have been made free from the factors contributing loss of time which is fatal for cyber cases. The LEA can easily take the help of ISP – monitoring centers to watch and record the data of some specified item or computer net work.

The investigation officers can also take the help of international counterparts through Network Information Centres and ask for mutual assistance in tracking the routers of the accused, to monitor a foreign ISP and to intercept and collect data there from. “The technical nature of most of the cyber crimes makes it difficult for the traditional law enforcement agencies – top investigate them..... Similarly law enforcement agencies face the continuing problem of the global reach of cyber crime.” * 28A The investigation is further assisted by the power U/s. 69 of the Act – whereby the Controller can direct any agency of the Government to intercept any information transmitted through any computer resource. And the agency can compel also the subscriber to decrypt the message.
A sealing arrangement has been made possible by a software (True Back). This has been developed by Centre for Development of Advanced Computing (C-DAC) at Thiruvanthapuram. "The C-DAC software called 'True Back' will be on a floppy carried by Police teams to 'freeze' the contents of any PC suspected of having been used in a Cyber Crime." *28B This process will protect both the Police and the accused from being falsely implicated for inserting material by anyone other than the accused.

SEARCH AND SEIZURE

Searching the suspected computer or computer system, the place and the person related to the machine may also be searched to collect data, materials and evidence. And the LEA can seize a no. of hardware and software - materials as well.

The Law of search and seizure in real world is that the search must be according to law – otherwise any recovery if made is to be returned –

(*) Momgudi V State AIR 1971 Mad 275.
(*) Sundaram & Co. V State AIR 1972 Mad 313.
(*) Khalil Vs State – 1976 Cr. LJ465 (All)

"Investigation of Cyber Crimes often requires collecting and evaluating data stored in some systems. In a transnational computer crime the data may be staled in a system located in another country." *29 In case of foreign country search, the assistance of counterpart is a barrier to the free and quick search of crime related informations.

A group of computer forensic experts have born form computer professionals to conduct searches “In fact within the professions of information security law enforcement and even accounting, there have emerged cyber sleuths, computer forensic experts who specialize in electronic discovery through examination of files, disks, Zip disk, backup tapes and hard drives. This also involves reconstructing communications and data that are one systems or transmitted through ISPs. The forensic examination process starts with making a duplicate image of the storage media under scrutiny and then conducting a complete search for specific words, files or documents.”*30

The US Department of Justice (DOJ) has issued guidelines on the subject of searching and seizing computers.

- www.usdoj.gov/criminal/cybercrime/searching.html
- www.edu.gov/cybercrime/searching.html
- www.technology.org/forensics.html
- www.fbi.gov/cib/nci/guidelines.html
- www.education.gov/cybercrime/searching.html

---

28B * Sup---13-----------------------------2004------------------------p-185
29 * Sup---13-----------------------------2004------------------------p-117
30 * Sup---8-----------------------------2001------------------------p-325
Evidence plays the crucial role in determining the criminal liability of the accused as it establishes the link between the offence committed and the accused person. "The prosecution must adduce prima facie evidence of the accused's guilt for otherwise there is no case to answer and the judge directs an acquittal; this means only that the prosecution must adduce sufficient evidence of the actus reus and mens rea mentioned in the definition of the offence charged. It is not necessary to negative every special defense that might be available to the accused". However it is observed in various cases that the nature and scope of evidence—everything depends upon the particular fact situation of an individual case. In the trial under IT Act—crimes the basic rules principles and guidelines are taken from the Indian Evidence Act—1872 which has been duly accommodated to deal with electronic evidence through necessary modifications and amendments. (Amendment of Act 1 of 1872).

The IT Act—has provided all the relevant changes in the second schedule by virtue of S/92—IT Act.

The section /3 as amended has defined evidence as—'Evidence' means and includes—
(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under enquiry; such statements are called oral evidence
(2) all documents including electronic records produced for the inspection of the Court;
Such documents are called documentary evidence.

Similarly the necessary changes and additions have been made in many other sections such as S/17,22A,34,35,39,47A,59,65A,65B, 67A,81A,85A,85B,85C,88A,90A,131. of the Indian Evidence Act.

31 * Cross & Jones—Introduction to criminal law—1976---Butterwoth & Co.----- -p-54
The new provisions are:

S/22A – when oral admission as to contents of electronic records are relevant.

47A – Opinion as to digital signature when relevant.

65A – Special provisions as to evidence relating to electronic records.

65B – Admissibility of electronic record (the electronic record will be admitted as genuine if it is taken form a computer (1) which is under regular use, store process etc. (2)Computer was not out of order, (3) a certificate by responsible officer describing the machine.

67A – Proof as to digital signature.

73A – Proof as to verification of digital signature

81A – Presumption as to Gazettes in electronic forms

85B – Presumption as to electronic records and digital signatures.

85C – Presumption as to Digital Signature messages.

88A – Presumption as to electronic messages

90A – Presumption as to electronic records five years old.


The problem of electronic record is that it can’t retained 15 years or more beyond which it becomes unusable fade and hence deformed “Digital is a problem. Digital storage media-floppies, compact discs, whatever – don’t have a long life span. A few decades at most. Digital storage is an all or nothing proposition once the Zero’s and One’s that make up the digital record start to break down, the entire disc or tape becomes unreadable.”*32

Material evidences can be recovered sometimes from the computer used by the victim of traditional or computer related offences. “In June 1997, Senator Charles Grassey told of an 11 years old boy in the Denver area who Committed suicide after being sexually molested. The boy had ---- a personal organizer which might contain information about the man molested him.”*33 But the boy applied encryption to materials kept recorded. Therein. And “the Police had been unable to crack the password. The investigation had been on held since February 1996.***34 Encryption of texts or search materials is not a major problem to the investigators. Because they can recover the key to the encrypted materials by consent, or find it on disk, or by cracking the system in some way – such as by guessing a password or exploiting a weakness in the overall system.

"Alternatively they used other evidence such as printed copies of encrypted documents other paper documents, unencrypted conversations and files, witnesses, and information acquired through other, more intrusive surveillance technologies such as bugs we emphasize, however that these were cases involving Computer – searches and seizures, not wire taps".* 35 The UN Model Law provides for legal recognition and admissibility of electronic record. The electronic record may be used as a document if it satisfies two tests U/A – 13. "The twin tests are (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as a data message or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.... Digital signatures can also be used to ensure the integrity of messages or information – Art – 8(1)(a) b"

* 36

The problem as to computer record so far has been that it is considered as hearsay evidence not direct. The exclusion of hearsay evidence in all the common law countries stands as rule. S/60 – oral evidence must be direct (Indian Evidence Act – 1872). So Computer records or printouts are losing ground to stand as direct evidence.

Case: Monotype Corp. Inc

Vs

International Typeface Corp

43.F.3d.443 (9th Cir).

In this case involving Internet evidence --- on e-mail message, Court in 1994 held – "E-mail is not a regular, systematic record meeting the foundational requirements of the business records exception". *37

But in another case:

(*) US Vs Catabran (9th Cir 1988) – The Court held that printouts of accounting and other book keeping records are admissible as business records also.

Also (**) Quality Auto Serv.

Vs

Fiesta Lincoln – Mercury Dodge. (Tex App – 1997)

(**) US V Kim – (D1 Cir 1979).

However better recognition came in Armstrong V Executive Office of the President where the Court held that ‘government e-mail is a record as per the Federal Records Act’ and it is in sufficient for the Government only to preserve a print out’. In UK also – the hearsay rule is- an established rule so far -

Taper V Reginam – 1952 All ER 449
Meyers V DPP 1964 All ER 877
RV Patel 1981 All ER 94.

35 * Sup – 33 --------------2000------------------------ p -115
36*Sup ------7----------------2001------------------------p---76
37*Sup------7----------------2001------------------------p---86
But UK considers the computer-generated evidence as a different class of evidence – so the traditional rule of hearsay is not directly applied hereto.


The question was whether expert evidence relying on a machine’s printout amounted to hearsay where printout was not exhibited and accuracy not challenged. The Court did not like to apply the hearsay rule to the computer evidence. The position further was clarified in –


Mr. Shepherd was charged with shop-lifting and the contended that the receipt was thrown away. The prosecution relied upon the Store’s computer records. The Court then applied certification test of S/69 of UK police and Criminal Evidence Act 1984.

“First there must be no reasonable ground for believing that the statement is in accurate because of improper misuse of the computer. Second, the Computer must have been operating properly at all; material times or at least the part that was not operating properly must not have effected the production of the document or the accuracy of the contents’. 38 And as to the proper functioning of the computer, a written certificate may be taken from a responsible officer having control over the machine. And the officer may be asked to stand the examination in chief and also cross exam when an expert testimony may not be required.

And thus UK has clarified the position as to computer evidence. The computer generated documentary evidence has been of three types.

(1) Real evidence – as evidence of a tangible nature from which the tribunal of fact can derive information by using its own senses. Here in electronic issue – this part will be the calculations or analysis that are generated by the computer itself through the running of software and receipt of information form other devices as built in clocks remote sensors. So when a bank computer automatically calculates the charges based upon tariff, the transactions on the account and the daily cleared credit balance – this calculation is a piece of real evidence such other is voice spectrographic.

(2) Hearsay evidence of Computer – the records or documents when produced by the computer as simple copies of information supplied by human beings – Cheques drawn and paying-in-slips credited to a bank account are hearsay evidence. And hence has less value.

(3) Derived evidence – When any record or document is created combining some real evidence with the information supplied form outside by human individual. One such is a daily balance column of a bank statement – as it is derived from automatically generated bank charges (real evidence) and cheque entries (hearsay evidence).

38* Sup ---7----------------------------- 2001----------------------------- p-63
Case: R Vs. Vandenberghe (BCCA 1976). It is observed that record prepared in the course of business provides strong assurance as to integrity and reliability and admissibility.


The accused used to send porn files to bulletin boards using a code name. The records taken form his computer were challenged to be hearsay one and hence - inadmissible. Court however rejecting the contention, took the materials as circumstantial evidence.

Case: R Vs. Weir A. J. 1998

The issue was user log and – email message supplied by ISP to be admissible or not. The court held the use of unseen procedure by itself can’t take away the reliability of the content as in blood test, photo Radar etc. The source giving out print copies is safe, if so kept, and hence reliable.

“Thus a positive judicial attitude, coupled with an effort to create a ‘Law of Electronic Evidence’ has ensured that Canada is in the lead in the development of such jurisprudence and India would do well to take note of Canadian progress in the Internet evidence area”. *39

In India S/60 – provides for oral evidence to be direct and thereby excludes indirect hearsay evidence – S/32 provides some exceptions to the above hearsay rule – where the person can’t be called in to depose in the Court. The exception U/s. 32(2) – when it relates to; or is made in course of business and kept in the books in ordinary course of business.

And also the provision U/s.34 relating to Entries in books of account including those maintained in an electronic form when relevant. So these two provisions S/32(2) and S/34 may provide sufficient ground to admit computer evidence in the judicial proceedings. “Thus there is no difficulty in admitting electronic evidence in India, and any arguments as to hearsay will not stand unless there are compelling reasons such as the electronic record under examination indeed falling into the hearsay category”. * 40 The author believes that electronic evidence does not demand any change to the rules on hearsay.

Case:

Ishwar Das Vs. Sohanlal – AIR 2000 SC 426 Held – Entries in account books regularly kept in the course of business are admissible though they by themselves can’t create any liability.

Dharam Chand Joshi

V

Satya Narayan Bazaz AIR 1993 Gan 35.

The problem of electronic evidence is new to the present legal system – as the entire process of collection preservation and then production of the e-evidence is new and complicated subject. The digital records may be seized as evidence through Computer forensics, Traffic Analysis, Evidence of Intrusion, Password recovery of Key

39*Sup ---7-----------------------------2001-------------------------------p-90
40*Sup---7-------------------------------2001-------------------------------p-91
(encryption) recovery. But the record so derived need to be protected in a lawful manner to keep it away from tampering in all possible manner as the digital record may suffer traceless tampering.


The Chain of custody of e-evidence-

4.1 – Chain of Custody

- You should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it.

The following need to be documented:

- Where, when and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.)

If possible commonly used media (rather than obscure storage media) should be used for archiving. Access to evidence should be extremely restricted and should be already documented. It should be possible to detect unauthorized access”.*41 And standard tools are to be sued like a program for examining processes (e.g. ps), program for examining system state (like – showrev, if config, netstat, arp) a program for doing bit to bit copies (like Safe Back, dd), program for generating checksums and signatures (eg.shalsum…), programs for generating core images and for examining them (eg.gocore,gdb), script to automate evidence collection (eg. Coroner’s Tool Kit FAR 1999) etc.

The UK Police Officers’ Association provided a set of rules on the collection of computer evidence.

(1) “No action taken by the Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court.

(2) In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions.

(3) An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

(4) “The Officer in charge of the case is responsible for ensuring that the law and these principles are adhered to. This applies to the possession of and access to information contained in a computer. They must be satisfied that anyone accessing the computer or any use of a copying device, complies with these laws and principles”.*42 The Indian Evidence Act 1872 in the newly inserted part S/22A – provides for oral admission as to contents of electronic record in case of a question as to genuineness of a record in digital form.

*41 Sup-13------------------------2004------------------------P-971
*42 Sup--13------------------------2004------------------------P-178
The IT Act provides for interception of data by the controller in the interest of national security and also for compelling the person concerned to assist and help decrypt the messages u/s-69. The IT Act provides a positive duty to the ISP to take all necessary steps to keep away from offensive activities u/s69. And the guideline for ISP issued by GOI has specifically required the ISP to setup monitoring system at it's own cost with one exclusive telephone line and to assist with the LEA to track and trace, to intercept any specified data stream for the purposes of crime control.

And all these data so collected are preserved to for analysis and production to the court of law.
Trial of the accused is the final but vital part of the Legal venture to deal with the crime. And the law of trial in Common Law counties requires the prosecution to establish its case adducting more than sufficient evidence, this being accusatorial and adversarial system.

The rule of criminal law further requires that the prosecution has to maintain a higher minimum proof to hold the accused liable for the offence charged cyber crime being a part of the crime generally, the rules of criminal law equally apply in the trial of cyber crime also.

- Queen V Ahmed Ally (11 W R CR 27)
  Normal J. Observed—"Every criminal charge involves two things, first, that a crime has been committed; and secondly, that the accused is the author of it. It is almost a universal rule that crime is not to be presumed". * 43

The criminal trial requires a higher degree of evendential support than in civil cases. 'The graver the crime the clearer and the plainer ought to be the proof of it.

Case:- R V INGS. 33 St. Tr. 1135.

The reasonable doubt in criminal trial exposes the prosecution to failure — as the maxim goes — 'it is better that ten guilty men should escape than that one innocent man should suffer'.

Case: (*) Sara Hobson.
  (*) R V Sterne (Sum Ass 1843 M.S.)
  The evidence must be entirely free from any doubt. Case - Nibaran Chandra Roy — as -king-
  Empeoror — 11 CWN 1085

Case:- Reg V Madhab Chandra (21 WR Cr.13)
Series of motivated conclusions cannot be framed to victimize the accused in absence of clear legal provision is injustice.
Case:- R – Vs Bond (113 & Std. 390)
The criminal provision can’t be extended by construction.

Empress V Kola Lalang (8 Cal. 214)

In the light of established legal rules and universal principles the legal control of cyber crimes has been in action in different countries.

The rights of the accused, the danger of false prosecution, perjury, illegal authoritative power of the government, excessive search and seizure, invasion into privacy and other human rights issues etc. come to the process of law – enforcement, prosecution, trial and penalty.

“Historically in the United States, a great deal of value has been placed on an individuals privacy from government intrusion (embodied in the fourth amendment)

And more generally on an individual’s right to be left alone (embodied in such judicial decisions recognizing the right to marry without regard to race and the right to control procreation etc”.

The search of the home of an attorney was excessive and the warrant did not specify the crimes for which the search was necessary. The Court agreed with the defendant as to violation of the 4th Amendment right.

US V Morries – US 817 (1991) worm was released by the accused who discovered loopholes in computer programs. These holes actually allowed his worms to make special and unauthorized access route into others’ computers. He already had access as a senior student to the Computer system at Carnell, Harvard and Barkeley, all being on – line. He was found guilty of unauthorized access, not being merely exceeding scope of authority.

(*) US V. Czubinsky (1st Cir 1997).

The defendant, and employee of a tax management Co accessed files without authority. The prosecution failed to prove his guilty mind or any injury – corpus delicti.


One Suhas Shetty (31 year) entered the name, phone number and a soliciting message of a lady into various adult websites of the Internet. Upon a complaint, police tracked and traced the accused in an our Internet café in Mumbai, using the address of the ISP. The court held his liable for 5 years imprisonment – 2yr. under IT Act S/67, 2 yr. for forgery U.s-465 IPC and 1 yr. for outraging modesty of a woman u/s – 509 IPC. The problem of prosecution trial and sentencing an accused of a cyber crime is complicated in the sense that Actus delicti (the offense, effect of offense) can’t be established as in the case of real space of crimes. The virtual presence, taking away copies of information installing Trojan Sniffer etc. are different than real space incidents.

A teen ager (16 Yr) of Pondicherry carried on e-mail bombing against one UK based media Co. for long three days in Mar. 2002. The CBI - CCIC upon request by UK- police, tracked and traced the accused and sized the computer with the e-mail programme.

44*Sup-8-----------------------------2001-----------------------------P-323
The problem of linking the Actus Reus and the injury with the accused can't be made without construction of jurisdiction in Cyber space — kind of judicial adventure. The IT Act provides for penalty in the form of imprisonment and or fine in case of violation of the Act and does not provide for community service or house arrest or the like, in suitable cases however the court is a liberty to chose probation, parole or other forms of control.

6.9 - VIOLATIONS OF HUMAN RIGHTS AND THE IT ACT

The cyber space is not much different place than the real space so far the threats to the H. Rts are concerned. The basic rights like speech and expression, privacy, dignity, freedom of communication, etc. Are facing attacks coming form different corners — individuals and powers, organized and remote.

In some respects, Cyber space is more vulnerable than the real world. More correctly the animal instinct finds greater opportunity here in Cyberspace to move and to act with much less restraint than real space.

"The new information technologies are breaking down the realms of what is private and what is public. Around the world, when individuals in private do acts that would result in possible criminal sanctions, there usually is little or no regulation of such activities. Examples include indulging in various forms of obscenity, expressing racial or ethnic hatred, through idle — conversation, breaching the privacy of other individuals. If they are regulated or stopped, it affects the right to freedom of expression. If allowed to continue it may affect some other freedoms of some other group of people. How to balance these conflicting interest is posing a problem from governments as well as human rights organizations".

The right associated with the freedom of speech and expression has tree risk zones in the IT Act.

1) Interception and monitoring by the ISP — Monitoring Centre — The Government of India has issued on e guideline for ISPs — and asked the ISP to install monitoring device to be used by the law enforcement as and when necessary.

2) Encryption key has been limited to 40 bit length by the same ISP guideline and has required that for higher key length — permission of Telecom Authority is required.

3) The provision U/s -67 – of the IT Act provides for obscene materials in cyber space. And the obscenity has remained as issue with no clear definition and precise concept for universal application. Moreover the rule of the freedom at the source also finds some difficulty in this provision.

45* Sup-13---------------------------------2004-------------------------------------1* 241
The freedom to use the Internet in any manner a man likes - is also causing concern to other especially to the women who are very often the victim of cyber stalking, unsolicited e-mails etc.

State Vs. Suhas Shettey – 2004

One Suhas Shetty (31 Years) of Chennai put up the name of a woman, her phone number along with a soliciting indecent message in numerous sites of the space. This embarrassment is a serious invasion into the personal life of a woman. The man was tackled and prosecuted and punished by Mumbai law enforcement agencies in November - 2004. The question of privacy in communication has been issue of great debate at international level. The IT Act has to a great extent encroached into this private area of individuals.

S/69 of the Act provides that the Controller can intercept any communication line without warrant and also he can ask an ISP or an agency concerned to decrypt messages.

"S/69 - Directions of Controller to a subscriber to extend facilities to decrypt information – (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the states friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offences, for reasons to be recorded in writing, by order direct any agency of the government to intercept any information transmitted through any computer resource". Thus the privacy through encryption is not safe during private communications.

6.10. - VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS AND THE IT ACT

"The protection of intellectual property on the Internet remains a grey area with the Information Technology Act – 2000, not addressing the issue of trademarks on the internet". *46

The intellectual property especially copyright, trademark, industrial know how etc. are very serious issues in Cyberspace. The new technologies in the information and communication systems are at the root of these problems. Pirated software, music files (MP3, Napster) domain name reservation etc. are the burning issues to day.

Ticket master Corp – Vs- Microsoft Corp.------- on linking websites.

The issues of framing, hyper linking etc. are also common problems. " Perhaps the most visible impact of the Internet on how organizations manage their IP has been associated with the threat that the Internet has brought into place. Particularly relevant to copyright how organizations have tried, succeeded and failed to defend their IP in Cyber space has been on e the most prominent IP issues over the past few years. The three core areas of impact for this have been in the software, music and, to a lesser extent book publishing industries". * 47 Also in India. "New study sees piracy at 70% and rising – software piracy in the country rose to 70% in 2001-02 compared to 63% in 2000-01 according to Business Software Alliance (BSA). It is surprising that piracy is rising in India.

46*Sup-24------------------------2001-----------------------------------P-151
despite the steps taken by the government. Policing has been strict in recent times". *48

The other form of IP right violations in India has been the domain name issues. The Domain Name Dispute Resolution Policy of ICANN has provided for the proper dispute management on domain names. Sometimes NSI also decides the domain name disputes. India has a body - under CNNIC (India’s Internet Administration Body) to deal with domain name - dispute. One dispute was however decided by Delhi Court - Yahoo Inc.-Vs-Akash Arora & anr.78(1999)

Delhi Law Times—285.

One Akash Arora registered his website as Yahooindia.com resembling to the media Co-Yahoo. Yahoo sued Akash Arora praying for injunction against the defendant. The Delhi Court rejected the contentions of the Defendant and allowed injunction.

Case: (*) Card Service International Inc
VS
MC Gee 42 USPQ2d 1850
(*) Jesus VS Srpds1u – 46 USPA2d 1652.

"In India, the court ruled in favour of the trade mark right of US based Yahoo Inc; against a local company, which had registered yahooindia.com The Court found that yahooindia was intentional effort to trade on the fame of the Yahoo trade mark". *49 [Yahoo Inc. Vs Akash Arora 1999(2) AD (Delhi) 229”.

6.11- OBSERVATIONS FROM QUESTIONNAIRE
Some valuable materials through questionnaire have been collected. It has been observed by some of the respondents that new type of harassment and embarrassment for innocent persons exploiting the Internet may have become very easy for motivated peoples. One such common mode of harassing a woman is to put the name of one lady with her contact number in the internet for display-mentioning her to be a call girl. And then as a result, unsolicited silly offers begin to flow to her, taking her for a call girl. It has also been observe that a net technology is now used (IBM- Laptop) to make the thumb impression as pass word to open the machine to protect privacy. Some also observe that the software piracy has become very wide spread in our country now. It has also been observe that the police personnel must be trained and properly educated to cope with the new high-tech crimes and to make a quick response. It is also suggested that the system of super user, log files, check pointing etc. way be helpful as security measures. The role of ISP has been observed by some of them as vital for police investigations, monitoring etc. The use of virus scanner fire walls etc. has also been suggested by many respondents.

It has also been observed that different spy softwares may be used to locate/trace the activities of employees/children using the computer. It is also suggested that software SPECTROSOFT -may be useful for Internet Monitoring. The sources given-

1. www.ics-iii.com (Intelligent Computer Solution)
2. high-tech-crime institute.com-www.htciat.labtech.com
3. Cyber Research Institute
4. Spector, e Blaster etc. different Internet Monitoring Softwars.

*48* The States man ---------- Kol---------24.01.2003-----------------p-11
*49 * Sun -24------------------------2001-------------------------------n-150